

EU policy update

6th Joint Data Exchange and Cybersecurity workshop

Felipe Castro

DG ENERGY unit F4: Energy security and safety

15 October 2026

Recent updates on cybersecurity in the energy sector

- Preparative Study for the Development of a Delegated Act/Policy Initiatives on Oil, Gas and Hydrogen Cybersecurity
- Smart Energy Expert Group (SEEG)
- Cybersecurity Network Code for cross-border electricity flows
- Other relevant initiatives:
 - Risk assessment related to wind and solar energy
 - Review energy security framework



• MARCH 2026

- Preparative Study for the Development of a Delegated Act/Policy Initiatives on Oil, Gas and Hydrogen Cybersecurity

Final Presentation

outwit complexity™

#	Content
---	---------

- | | |
|---|-------------------------|
| 1 | Objectives |
| 2 | Methodology |
| 3 | Analysis |
| 4 | Key Findings |
| 5 | Overall Recommendations |

Objectives

Core Objective

Key Objective

Create a common understanding of cyber risks, in the gas, hydrogen and oil sectors, identification of existing regulatory gaps and analysis of needs to mitigate these risks, including an estimation of implementation resources and operational costs of respective measures to address those risks.

Context of this study

- This study was undertaken to support the European Commission’s consideration of delegated or other policy initiatives on cybersecurity in the gas, hydrogen and oil sub-sectors.
- These sub-sectors form part of Europe’s critical energy infrastructure and depend on increasingly digital, connected and interdependent operational environments.
- Their industrial control systems, supervisory systems, communications networks, metering systems, remote access arrangements and enterprise platforms are essential for safe operation, commercial continuity and security of supply.
- As these systems become more digitalized, their exposure to cyber threats also increases.

Why does this study and baseline understanding matter?

- Gas, hydrogen and oil systems are increasingly digitalized and interconnected.
- Cyber incidents in these sub-sectors can affect safety, the environment, operational continuity and security of supply.
- The study therefore examines both the policy landscape and the operational pathways through which cyber risk materializes.

Key Tasks in the study with expected activities and outcomes

Tasks	Expected activities and outcomes
1 Legislative and Policy Landscape	Map the current legislative and policy landscape across the EU and comparable frameworks, identifying how cybersecurity requirements for the sub-sectors are currently expressed and where important differences remain.
2 Digital System and Data Flows	Describe digital systems and data flows that underpin these sub-sectors, identifying where operational dependencies and exposure points are concentrated.
3 Risk Assessment Methodology	Develop and apply a risk assessment methodology suitable for the specific sub-sectors and the industrial environments in scope, applicable to the evidence collected through the assessment.
4 Threat scenarios and mitigations	Identified the highest-priority cyber threat scenarios, the gaps that make those scenarios plausible, and the measures most likely to mitigate them
5 Overarching findings and recommendations	Assess the likely implementation and operational effort associated with stronger cyber resilience and translated the results into recommendations for the EU, Member States and operators.

System Description, using Purdue Enterprise Reference Architecture (PERA) (*) levels

Levels 4/5: Enterprise and Business Networks: This layer comprises the IT infrastructure that includes business applications and internet connectivity. This highest level represents the enterprise IT systems that support broader business functions and connect to external networks. Examples include Enterprise Resource Planning (ERP) software, databases, and email servers.

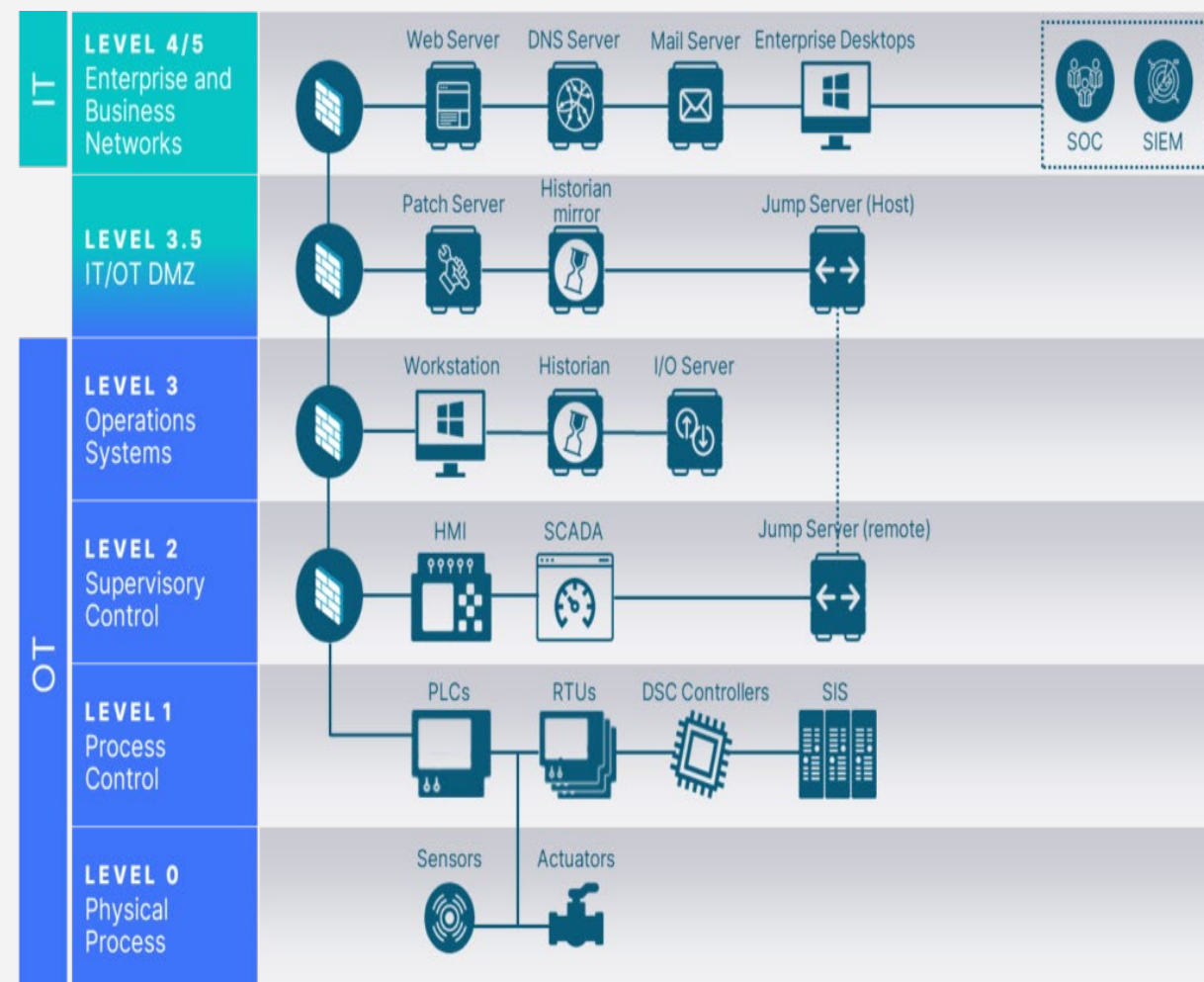
Level 3.5: Industrial Demilitarized Zone (iDMZ) for IT and OT: This level acts as a secure buffer between the ICS/OT network and external networks. It often contains security devices such as firewalls and Intrusion Prevention Systems (IPS), as well as servers.

Level 3: Operations: This layer typically includes Manufacturing Execution Systems (MES) and historians. It manages and optimizes production processes and can include systems for batch management, maintenance, and plant performance management.

Level 2: Supervisory Control: This layer incorporates SCADA (Supervisory Control and Data Acquisition) systems and Human-Machine Interfaces (HMIs). It aggregates data from controllers for process monitoring and control, allowing operators to oversee and manage the industrial process.

Level 1: Basic Process Control: This layer houses controllers and Programmable Logic Controllers (PLCs) responsible for automating individual processes. It translates sensor data into actionable commands to control the physical process. Other devices in this layer include Remote Terminal Units (RTUs) and Intelligent Electronic Devices (IEDs).

Level 0 Physical Process: This is the foundational layer, encompassing the actual physical processes and equipment that produce goods or deliver services. It includes devices like sensors, actuators, valves, motors, pumps, and field devices that directly interact with the physical world.



Key Threat Scenario's by PERA Level (1 of 2)

PERA Level	Threat Vector description	Risk Ranking*			Measures Mitigating Risk
		Likelihood	Impact	Overall	
4/5	Enterprise ransomware causing operational shutdown or delay.	Amber	Red	Red	- Segment enterprise-OT dependencies - Resilient recovery for business platforms - Business-continuity procedures - Access hardening - Threat prevention and detection - Vulnerability and posture management - Third Party risk controls - Crisis management and communications - Residual Risk: Amber
4/5	Credential theft and remote access abuse enabling compromise of refinery and terminal operations	Red	Red	Red	- Phishing-resistant authentication - Privileged access management (PAM) - Conditional access and device posture - Identity and domain separation - Controlled OT access path - Monitoring, detection; process controls / dual custody - Hardening and Hygiene - Residual Risk: Low
3.5	Historian bridge compromise and authenticated pivot into OT systems.	Amber	Red	Red	- Eliminate dual-homed designs - Separate identities and trust domains - Restrict administration and scope - Continuous monitoring and anomaly detection - Data flow governance - Hardening and resilience - Residual Risk: Low

Key Threat Scenario's by PERA Level (2 of 2)

PERA Level	Threat Vector description	Risk Ranking*			Measures Mitigating Risk
		Likelihood	Impact	Overall	
3.5	Compromised remote access gateways or jump hosts connecting vendors and OT assets.	Red	Red	Red	- Dedicated, monitored OT access gateways - Protocol break/translation layer - Vendor access brokering and PAM - Continuous monitoring of jump hosts - Offline/emergency access procedures - Patch and configuration assurance - Network segmentation and rate limiting - Residual Risk: Amber
3	Ransomware or Operational Technology Lockout leading to Loss of View and Loss of Central Coordination.	Amber	Red	Red	- Operational segmentation and isolation - Resilience by design - Passive network monitoring and anomaly detection - Incident response rehearsals - Residual Risk: Low
2	Compromise of an EWS or HMI through stolen or phished credentials, abuse of remote access gateways or vendor support sessions, or lateral movement from the IT network across the iDMZ.	Amber	Red	Red	- Network segregation and isolation - Access control and session governance - Configuration and change control - Monitoring and all-listing - Residual Risk: Low

Summary of Key Findings

Key Findings

1 Regulatory landscape is uneven

The study found a broad common policy direction through NIS2, but uneven national transposition, implementation and sector specific guidance.

Stakeholders reported duplication and administrative burden where NIS2 obligations overlap with existing standards and practices.

The core issue is therefore not a lack of frameworks, but insufficient coherence and operational translation across them.

2 Sub-sectors share common digital architecture

Oil, gas and hydrogen operations rely on layered architectures that connect field devices, controllers, supervisory systems, historians, industrial DMZ functions and enterprise platforms.

Across these sub-sectors, a relatively small number of bridging systems concentrate operational and cyber exposure.

These bridging systems include engineering workstations, HMIs, remote access gateways, jump hosts, historians and industrial DMZ services.

3 Main attack pathway runs from IT to OT

The study found that the most plausible and highest-priority attack pathway starts in enterprise IT or trusted external access and then moves toward OT.

Incomplete IT/OT separation, weak identity segregation, insecure remote access and poorly governed data exchange increase the chance that an IT incident becomes an operational event.

Smaller operators and newer entrants may be more exposed where resources and supplier leverage are limited.

4 Small number of threats drive most risk

Six priority threat scenarios were identified: engineering workstation/HMI compromise, OT lockout, compromised remote access gateways, historian-based pivoting into OT, credential theft, and enterprise ransomware causing operational shutdown.

These scenarios differ in mechanism, but all point to structurally sensitive chokepoints at Levels 2, 3, 3.5 and 4/5.

The operational consequences can include loss of visibility, unsafe control changes, degraded coordination, supply disruption and commercial loss.

5 Resilience is feasible, but must be proportionate

Stronger resilience is feasible, but effort varies with system complexity, number of sites, vendor pathways and operational interdependencies.

The largest uplift is generally required at Levels 3, 3.5 and 4/5, where monitoring, remote access governance, privileged access management, backup and recovery capabilities must be strengthened.

The report therefore supports proportionate baselines rather than one uniform compliance burden for all operators

Overarching Recommendations

System-level objectives and tactical technical actions for sector operators, member states, and at the EU level

EU-Level Action

- The EU should establish an outcome-based OT baseline that can be recognised across Member States and mapped to PERA levels.
- NIS2 should remain the overarching legal anchor, while IEC 62443 should serve as the principal OT-specific technical reference.
- EU-level action should also strengthen common incident playbooks, shared incident data and cross-border exercises.

Member State Action

- Member States should complete and operationalise NIS2 implementation in ways that reduce fragmentation rather than create additional duplication.
- National guidance should clarify how legal requirements translate into OT security outcomes for the oil, gas and hydrogen sub-sectors.
- Competent authorities should track progress through a small set of practical indicators, including implementation completeness, playbook adoption, exercise participation and reduced audit overlap.

Sector / Industry-led Actions

- Operators should build a current-state map of assets, data flows, interfaces, identities and decision rights across the IT/OT boundary.
- They should prioritise brokered and monitored remote access, stronger identity and privileged access controls, tighter historian and industrial DMZ governance, and tested recovery capability.
- Supplier assurance should be strengthened through named accounts, secure update paths, session recording and better evidence from vendors.

Smart Energy Expert Group (SEEG)

Status update



The Smart Energy Expert Group (SEEG)

- The Smart Energy Expert Group replaces the Smart Grids Task Force.
- It will advise the Commission on initiatives and actions to coordinate and accelerate the digital and sustainable transformation of the EU's energy system, namely on the development and deployment of smart energy solutions, cybersecurity and consumers empowerment and protection.
- The Commission has established 3 subgroups under the SEEG to cover:
 - Data for Energy (D4E)
 - Consumer Empowerment and Protection
 - Cybersecurity



Smart Energy Expert Group (SEEG)

Work programme - Topics for research:

1. Recommendations to address cybersecurity risks in Photovoltaic. Report published in October 2026 - [Critical infrastructure and cybersecurity](#)
2. Existing EU legislation and standards in the energy sector. Report published in September 2026 - [Critical infrastructure and cybersecurity](#)
3. Requirements of a reference architecture for energy grids
4. Cybersecurity Information Exchange in the European Energy Sector

Network code on cybersecurity (NCCS)

Status update



What is the Network Code on cybersecurity?

- Delegated Act of **Electricity Regulation (EU) 2019/943**, Article 59 (2).
- Foresees **sector-specific rules** for cyber security aspects of cross-border electricity flows, on common minimum requirements, planning, monitoring, reporting and crisis management.
- Applies only to **Electricity**. Inside, the scope is limited to entities with impact on **cross-border** electricity flows
- The **risk assessment** will identify which entities are most relevant and what **security measures** they need to apply. **They will be very specific, looking at the industrial processes involved in the x-border flows of electricity.**
- **Complementing and building upon NIS2** to include sector-specific cybersecurity requirements, notably **involving both key stakeholders in electricity and cybersecurity** governance frameworks.
- It provides more **precise instructions and procedures**, leveraging existing electricity mechanisms to prevent and react to electricity incidents and streamlining the communication to cybersecurity authorities once a cybersecurity root cause is identified.
- Designed by electricity **stakeholders** together with cybersecurity **experts**, for the **electricity sector**.



Key elements in the NCCS architecture

- Definition of a **list of entities that play a role** in the NCCS, either actively applying risk management measures for their electricity processes, or by playing supervisory/advisory roles
- Definition of **National Competent Authorities** for the purposes of this Regulation (NCCS-NCA), including mutual cooperation
- Procedures to **develop and adopt Terms, Conditions and Methodologies** to implement the different obligations
- Execution of risk assessments and implementation of controls
- Definition of **rules for public consultations**
- Procedures for **monitoring, supervision and enforcement**



State of play for some key deliverables

- Cybersecurity risk assessment methodologies: approved by All TSOs and DSO Entity Board and joint decision reached by Competent Authorities in October 2026
- Cyber-attack Classification Scale Methodology: approved by All TSOs and DSO Entity Board and joint decision reached by Competent Authorities in October 2026
- Recommended provisional electricity cybersecurity impact index ('ECII'): published
- Recommended provisional list of European and international standards and controls: published
- Guide on benchmarking the costs and effectiveness of cybersecurity investments: issued by ACER
- Procurement recommendation for substation automation systems for high voltage grids



Key achievements

- Development of methodologies: joint decision for two methodologies. Readiness to start risk assessment after communication of final version.
- Art 4. Designation of CAs:
 - 15 notifications and 5 indicated as pending national legislative procedure
 - possible action by the Commission for remaining designations.
- Initiative to prepare rule of procedure for approval, in line with the key learnings extracted from ACER survey.
 - Inspire from existing mechanisms like the one existing at the Energy Regulators Forum for other network codes.
 - All CAs should explicitly approve the procedure for future methodologies and reviews
- Progress in other deliverables: ACER guidelines, Procurement recommendations, etc.



EU cybersecurity risk identification and scenarios for the wind & solar power infrastructure

Status update

Context of the exercises

- Cybersecurity risks for electricity security and safety of supply:
 - Looking at incidents and crisis stemming from renewable generation
 - cybersecurity as one of the root causes for electricity incidents.
- Risk preparedness regulation 2019/941: Art 5 includes malicious (cyber)attacks as part of the Methodology for identifying regional electricity crisis scenarios. Gas security of supply also requires cyberattacks as part of security risks.
- Wind Action Plan (2023): Tackle cybersecurity risks in wind energy installations and infrastructure
- Economic Security Strategy (2025): Limit cyber-vulnerabilities in critical infrastructure (ie, solar inverters)
- Strategic Roadmap for Digitalisation and AI in Energy Sector (2026): Risk assessment of solar installations

Objectives for both assessments

Objectives of the Risk Assessment:

- map digital components and processes that could be used maliciously to affect the operation of the wind and solar installations
- priority is given to phases where digital processes are likely to be more pervasive, like the design of installations (Construction and installation), operations and maintenance
- reuse, as much as possible, Commission methodologies, in particular the EU Methodology for Union-level Cybersecurity Risk Assessments sponsored by the NIS Cooperation Group

Relevant players for the risk assessment

European Commission is reaching out to key actors in the industry, with support from Wind Europe, SolarPower Europe, the European Solar Manufacturing Council (ESMC) and other bodies and organizations, including European and National authorities. For example:

Industry:

- Wind Europe
- GWEC (Global Wind Energy Council)
- SolarPower Europe
- European Solar Manufacturing Council (ESMC)
- ENTSO-E
- the EU DSO entity,
- National TSOs/DSOs
- Manufacturers, integrators, operators, etc

Authorities:

- ACER and National Regulatory Authorities
- NIS Cooperation Group
- EIB
- EBRD

Commission:

- DG ENER
- DG CNECT
- DG JRC
- ENISA

Expert Groups:

- Smart Energy Expert Group



Cybersecurity in the Security of Supply framework

Status update



Areas for improvement

- A more efficient the decision-making process for Terms, Conditions and Methodologies in the Network Code for cybersecurity. We need to explore agreed procedures in case of non-response or disagreements among the Competent Authorities (similar to what happens in other Network Codes)
- Grid operators need a better understanding of the cybersecurity risks introduced by energy systems connected to their grid connection points (currently outside of the scope of the Network Code on cybersecurity).



Thank you



© European Union 2025

Unless otherwise noted the reuse of this presentation is authorised under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license. For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.

