DSO ENTITY
DSOs FOR EUROPE

Strengthening the resilience of the EU energy system: The important role of DSOs

February 2026

Table of Contents

Acknowledgements:

This report was developed by DSO Entity members from the Country Expert Group (CEG) with the kind support and guidance from members of the Expert Group Cybersecurity (EG CS) and other relevant experts. DSO Entity thanks all involved members and colleagues for their inputs and support.

List of abbreviations

ACER Agency for the Cooperation of Energy Regulators

ARERA Italian Regulatory Authority for Energy, Networks and Environment

BCM Business Continuity Management

BESS Battery Energy System Storage

CEG Country Expert Group

DER Decentralised Energy Sources

DNDP Distribution Network Development Plan

DRES Distributed Renewable Energy Systems

DSO Distribution System Operator

EC European Commission

EMD Electricity Market Design

ENISA European Agency for Cybersecurity

EU European Union

EV Electric Vehicle

FIRE Electricity Rapid Intervention Force

GW Gigawatt

ICS Incident Classification Scale

INI European Parliament Own-Initiative Report

LV Low voltage

MV Medium voltage

NC Network Code

NC CS Network Code on Cybersecurity

NECP National Energy and Climate Plan

OEM Original Equipment Manufacturer

PCI Project of Common Interest

PV Photovoltaic

RED Renewable Energy Directive

RES Renewable Energy Sources

RfG Requirements for Generators

SSD Stredoslovenská distribučná

TCM Terms, Conditions and Methodologies

TSO Transmission System Operator

VSD Východoslovenská distribučná

ZSD Západoslovenská distribučná

Executive Summary

As the most integrated network in the world[1], European electricity grids are a core component of the European Union (EU)'s energy security. **This report demonstrates the key role and increasing relevance of Distribution System Operators (DSOs) for a resilient European energy system**. With the transformation of the energy system, distribution network operators have developed into active DSOs with greater responsibilities in strengthening system resilience and energy reliability in coordination with Transmission System Operators (TSOs). By integrating 70% of renewables and connecting Decentralised Energy Sources (DER) like Electric Vehicles (EV) and heat pumps, **DSOs play a growing role in enhancing the EU's energy independence and in collaborating with TSOs to ensure security of supply by reinforcing system resilience**, i.e. the ability to prevent, respond to and recover from disruptions while maintaining balanced and reliable operation.

Furthermore, beyond physical security of supply, DSOs are increasingly relevant for designing and implementing **measures to face growing external challenges in cybersecurity and climate adaptation**. Their role should be further understood in light of the evolving EU resilience framework, notably the Directive on the security of Network and Information System (2022/2555/EU, NIS2), the Resilience of Critical Energy Entities Directive (2022/2557/EU, CER Directive) and the Network Code on Cybersecurity of the electricity sector (2024/1366/EU, NC CS), that **shift the EU energy security from a pure security of supply focus to an all-hazard approach**. In a more unstable geopolitical environment, resilient distribution grid operations and security measures are hence key to protect grid infrastructure against physical and cyber-attacks, the latest having doubled between 2020 and 2022 in the power sector[2]. DSOs also face more frequent extreme-weather events which have already caused over EUR 145 billion in economic losses across the EU[3]. To respond effectively to such events, it is essential to have secure, affordable, and available supply chain equipment to reinforce grid infrastructure and react to emergency scenarios. The report therefore adopts a strategic approach, shedding light on the challenges to the resilience of the EU's energy system and the role of DSOs in addressing them.

This report builds on the Technical Vision[4] published in January 2025 and was developed in parallel with the ongoing reflection led by DSO Entity's ad-hoc expert group on the Iberian Peninsula incident of April 2025.

In a nutshell, the report addresses the following aspects:

- It underlines the need to follow **a broader and more forward-looking perspective focusing more closely on resilience** (also in economic regulation) to enhance the EU's energy security in the long term, especially in connection with the role of electricity grids.
- It sheds light on **how distribution grids are increasingly relevant for the resilience of the EU's energy system**.

[1] European Commission (COM/2025/79): *Action Plan on Affordable Energy Prices, p.3.*
[2] Eurelectric (2025): *Cybersecurity in the power sector*. Available online.
[3] Eurelectric, op.cit.
[4] DSO Entity (2025): Technical Vision. Available online.

DSO Entity | Rue Belliard, 35 – 1040 Brussels BE
www.eudsoentity.eu | info@eudsoentity.eu

- It demonstrates the increasing **responsibilities of DSOs in maintaining system stability** and reliable energy in coordination with TSOs in a changing energy system.
- It highlights **how DSOs need to adapt to new external challenges through an all-hazard approach** by actively strengthening cybersecurity and developing climate adaptation measures.

Eventually, in the context of the EU-level discussion on what is needed for an adapted energy security architecture, the report underlines that **sufficient investments in increasing grid resilience are a non-regret option and an adapted and forward-looking regulatory framework is hence needed** to set the right conditions through an anticipatory investment approach. The report also stresses how essential the **effective implementation of existing EU regulations** is to strengthen resilience and prevent delays in the decarbonisation process. Given the increasing relevance of DSOs for system resilience, the report finally underlines the **importance of a true TSO-DSO cooperation to ensure a system-of-systems approach also for energy security** and how a stronger involvement of DSO Entity should be considered at the EU level when assessing pan-EU security incidents.

Methodology

The report is based on a qualitative analysis of information collected through a structured survey distributed to national expert representatives of DSO Entity's Country Expert Group (CEG)[5]. The CEG started working on the topics of energy security and resilience in February 2025; hence contributing to the implementation of DSO Entity's Knowledge Sharing Strategy 2025. The survey was conducted within the CEG between September and November 2025 and gathered 23 DSO respondents who completed the questionnaire through their country's perspective.

The methodology involved:

- Collecting feedback from DSO national representatives via a structured questionnaire.
- Analysing responses of DSO respondents to classify most critical challenges for the European grid resilience in the EU Member States.
- Mapping specific national security challenges and identifying commonalities across Member States to determine security threats for the overall EU energy system.
- Compiling good practices from DSOs respondents to show the relevance of distribution grids for the resilience of the EU energy system and DSOs' engagement in addressing ongoing challenges.

The analysis of the survey resulted in different graphics displayed across the report. Practices collected through the survey were also summarised and integrated in the report. This approach provides a representative overview of the most critical challenges to grid resilience in the EU, while also capturing country-specific obstacles.

[5] DSO Entity's Country Expert Group (CEG) is composed of DSO representatives from EU Member States appointed by their respective countries. The members provide expertise from their respective countries through a national perspective, including data and good practices.

DSO Entity | Rue Belliard, 35 – 1040 Brussels BE
www.eudsoentity.eu | info@eudsoentity.eu

1. Introduction to energy security, resilience and electricity grids

The Iberian blackout of 28 April 2025 and its repercussions underlined the **importance of resilient and robust energy infrastructure for the security of the EU energy system**. However, when addressing security of supply, the focus is often on how to ensure that demand and supply remain always stable (resource adequacy), which in day-to-day operations is the responsibility of TSOs; and hence dismisses other relevant aspects for which the distribution level is key.

In light of a changing security paradigm, **a broader and forward-looking perspective focusing more closely on resilience** is needed to cover existing and emerging challenges to the EU's energy security and to sufficiently consider the relevance of distribution grids. DSOs' evolving role in ensuring resilience must be further assessed within the EU's resilience framework set in the NIS2 Directive (2022/2555/EU, NIS2) and the Critical Energy Resilience Directive (2022/2557/EU, CER Directive) and complemented by the Network Code on Cybersecurity for the electricity sector (2024/1366/EU, NC CS). For the first time, horizontal, binding resilience and risk-management obligations were established for critical energy entities, including DSOs; but details still need to be sorted out in national implementation activities in which DSOs should be involved from the very beginning. The shift from a pure energy security focus to an all-hazard approach is reflected in DSOs' resilience investment, contingency planning and grid reinforcement which are increasingly embedded in risk-based assessments. The objective of this paper is therefore to provide a comprehensive perspective of the topic in connection with distribution grids by focusing on key strategic aspects.

To show the relevance of electricity distribution grids for the overall EU's energy security, it is important to clarify:

- The differentiation but also the link between energy security and resilience.
- The relevance of grid resilience.

1.1 Resilience vs. energy security

Energy security is one of the three core objectives of the EU's energy policy. Mentions of the **resilience of energy infrastructure have become more prevalent in the latest EU initiatives** such as the Affordable Energy Action Plan[6]. While at the same time intrinsically linked and even complementary, energy security and resilience are to be distinguished:

- **Energy security** refers to the availability and reliability of an adequate supply of energy at a reasonable cost. Beyond physical and pricing aspects, it also encompasses sustainable and geopolitical dimensions. These dimensions have become more important these last years in the context of the energy transition induced by the setting

[6] European Commission (COM/2025/79): *Action Plan for Affordable Energy*. Available online. European Parliament (2024): *Report on Security of Energy Supply*. Available online. Polish Presidency of the Council of the European Union (2025): *Programme of Presidency*. Available online. Polish Presidency of the Council of the European Union (2025, 26 March): *High-Level Grid Conference on Electricity Grids*. Available online.

DSO Entity | Rue Belliard, 35 – 1040 Brussels BE
www.eudsoentity.eu | info@eudsoentity.eu

of EU's energy targets, and the increasingly tense geopolitical environment. Though it also encompasses it, this dimension is larger than security of supply only.

- **Resilience** in contrast means '*the ability to avoid, prepare for, minimise, adapt to, and recover* [within a reasonable timeframe] *from anticipated and unanticipated energy disruptions in order to ensure energy availability and reliability*'[7]. It is strongly connected to the capacity to maintain energy supply even in time of disruptions regardless of their cause or area of occurrence, which can include extreme weather events, cyberattacks, or other unforeseen circumstances anywhere across the overall system. Therefore, resilience **follows a more forward-looking approach that contributes to enhancing the EU's overall energy security**.

	Physical Security	Security of Supply	Cybersecurity
Risks	Physical, malicious attacks, sabotage Military attacks, hybrid threats Impact of climate-related events	Energy dependency towards foreign energy supplies, Renewable Energy Sources (RES) variability, intermittent and bidirectional energy flows	Cyberattacks
Grid resilience	• Critical infrastructure • Protection and grid reinforcement • Risk preparedness, crisis and business management, readiness • Climate resilience • Cybersecurity standards and measures		

Table 1: Energy security and grid resilience.

1.2 Resilience and electricity grids

*"The resilience of energy systems, understood as the ability to anticipate, withstand, adapt to, and quickly recover from possible disruptions, **is now a strategic imperative**".*

Own-initiative report (INI) from the European Parliament on the security of energy supply in the EU (30.06.2025).

Resilience covers mitigation measures and adaptation strategies implemented to prevent and be prepared to respond to potential threats or other unforeseen events. In this respect, grid operators play a key role in guaranteeing energy availability and reliability when ensuring that "the lights stay on", i.e., electricity demand and supply always remain balanced. Yet, the changing energy system, becoming increasingly decentralised, digitalised and decarbonised, as well as the growing threats to the security and safety of the European grid infrastructure, have shown that the **relevance of grids is no longer only limited to this sole physical security of supply aspects**. **Grids are increasingly impacted by other challenges** resulting from the integration of renewable and DER into the power network but also from external emerging challenges that expose their vulnerabilities. To address these challenges, grids need to become more resilient in design and adopt an all-hazard approach to tackle natural hazards (e.g. extreme weather, climate impacts), accidental hazards (e.g. technical failures) and human-induced threats (e.g. sabotage).

[7] Cornell University. (s.f.): *Definitions – U.S. Code*. Legal Information Institute. Available online.

1.3 Targeted approach to resilience focusing on strategic aspects for distribution grids

This report focuses on the resilience of distribution grids. It reflects on core and non-exhaustive strategic aspects that are key to enhancing the EU's overall energy security, and for which distribution grids are becoming increasingly relevant[8].

It sheds light on the relevance of DSOs for the EU's system resilience when facing the following challenges:

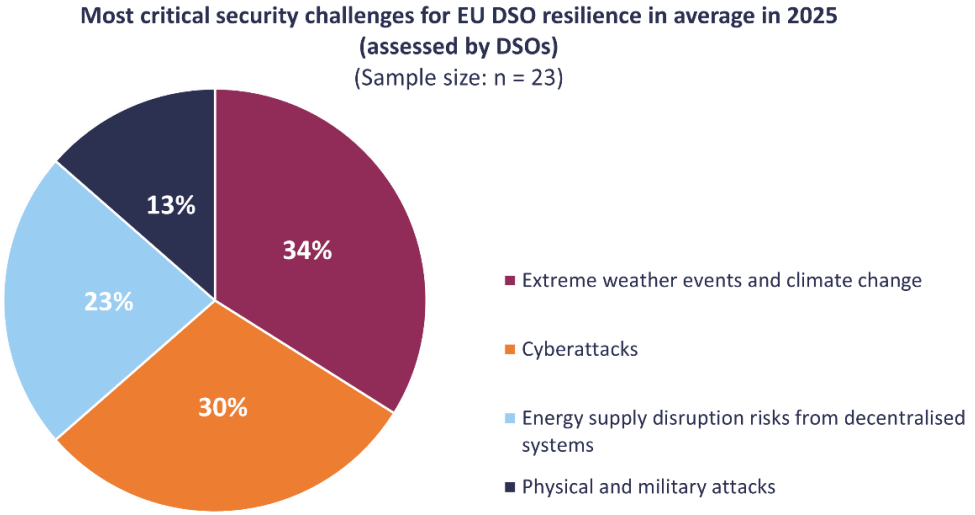
- **Internal challenges**: Grid stability; DER connection to the grid and related effects on the EU's energy independence.
- **External challenges**: Threats to system management covering climate adaptation and cybersecurity.

The second chapter elaborates on the growing relevance of DSOs for the resilience of the EU's energy system and on the challenges mentioned above.

[8] For the purposes of this paper, a targeted approach has been adopted, focusing on selected key strategic aspects of resilience that are relevant to distribution grids. Consequently, not all dimensions of resilience are covered; topics such as supply interruptions, system recovery after disruption or joint preparedness measures will not be addressed directly. Nevertheless, these subjects may be mentioned or partially considered in the context of other discussions.

2. The relevance of DSOs for a resilient EU energy system

Grids are essential to ensure a well-functioning, secure and stable energy system, and their resilience is a key prerequisite for the EU's energy security. In recent years, the EU's energy system has undergone an unprecedented transformation, becoming more decentralised, decarbonised and digitalised. As a result, **DSOs that used to focus traditionally more on passive infrastructure management have developed** a more active management and operation of the distribution system **assuming greater roles and responsibilities in actively managing grid operations and bolstering the EU's energy system resilience**. European DSOs are progressively connecting growing volumes of RES and DER to their distribution networks. This transformation already necessitates a stronger, more complex system which together with other emerging challenges, increases system complexity and cyber vulnerability, requiring DSOs to simultaneously strengthen the physical infrastructure, its cybersecurity defenses and climate resilience to safeguard the operation of the increasingly decentralised and digitalised EU energy landscape. Recent energy crises and growing geopolitical tensions have further highlighted the urgent need to strengthen and protect energy infrastructure. The April 2025 blackout in the Iberian Peninsula that affected households, industries, telecoms and generators, etc. demonstrated the strategic importance of resilient grids for both modern society and the broader economy. To better address these challenges, the European Commission (EC) plans to revise the EU's energy security framework with the resilience of grid infrastructure as a pillar of future initiatives.



The infographic ranks the most critical security challenges identified by DSOs (n = 23) according to their priority in EU average. Threats were rated on a 4-to-1 scale, with 4 indicating the highest priority. Total points were summed and percentages calculated to reflect the EU average. The findings indicate that extreme weather is regarded as the most critical threat, followed by cyberattacks, disruption of energy supply from an increasingly decentralised energy system, and, lastly, physical or military attacks.

Figure 1: Most critical security challenges for EU DSO resilience in average in 2025 (assessed by DSOs). Data based on a survey conducted in DSO Entity's CEG in 2025.

DSO Entity | Rue Belliard, 35 – 1040 Brussels BE
www.eudsoentity.eu | info@eudsoentity.eu

2.1 The energy system is changing, and the role of DSOs in active system management is increasing

1) As the largest integrators of renewables, DSOs contribute to enhancing the EU's energy independence and need to manage intermittent energy flows

The energy system is undergoing an unprecedented change driven by the decentralisation and decarbonisation of power generation, the digitalisation of services and processes, and the electrification of consumption. The Green Deal and Fit for 55 targets have accelerated this transformation in Europe; and efforts to cut dependency on Russian energy imports were further intensified following the outbreak of the war in Ukraine. As energy independence and diversification lie at the core of the EU's strategy to strengthen its security of supply, the accelerated deployment of homegrown renewables needs to be supported by resilient grid infrastructure.

As the technical enablers of this transition, DSOs play a key role in enhancing the EU's energy independence by integrating most of the Distributed Renewable Energy Systems (DRES), both supply and demand. DSOs connect 70% of the new EU's RES capacity to the distribution grid, among which the 600 Gigawatt (GW) target of solar capacity by 2030[9]. Already 338 GW of solar Photovoltaic (PV) capacity was installed in the EU in 2024 with 38 GW of newly installed rooftop solar PV connected to the DSO grid[10] (compared to 1.4 GW of newly installed offshore wind capacity[11]) (see Figure 2).

Furthermore, DSOs also connect high volumes of DER with the roll-out of EVs and heat pumps. At the same time, the energy system of the future, that increasingly relies on intermittent and bidirectional energy flows, requires different management with a growing need for flexibility through storage and demand response. As the largest integrators of RES, DSOs therefore need to be more robust, reliable and resilient to maintain the stability of the power supply.

[9] European Commission (COM/2022/221): EU Solar Strategy, p.1. Available online.
[10] SolarPowerEurope (2025): *EU Market Outlook for Solar Power 2024-2028*. Available online.
[11] WindEurope (2025): *2024 Statistics & the outlook for 2025-2030*. Available online.

DSO Entity | Rue Belliard, 35 – 1040 Brussels BE
www.eudsoentity.eu | info@eudsoentity.eu

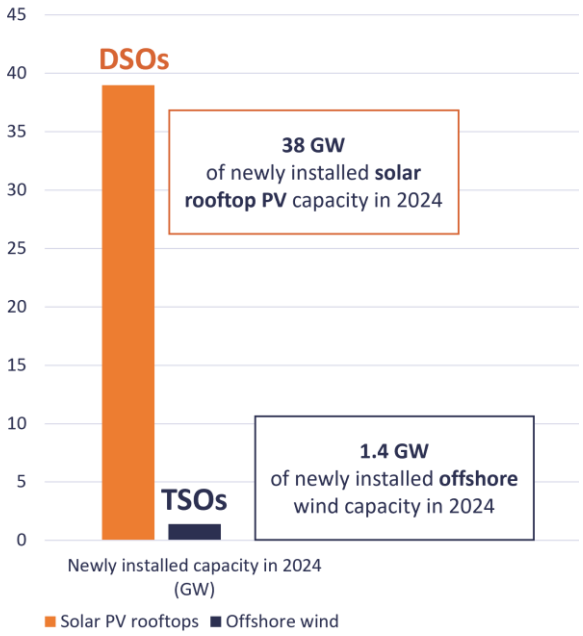


Figure 2: Newly installed capacity in rooftop solar PV and offshore wind in the EU in 2024. Data from Wind Europe and SolarPower Europe (2025)[12].

2) Through active system management, DSOs play a greater role in grid stability in coordination with TSOs

Traditionally, TSOs have been responsible for maintaining grid stability by balancing generation and consumption levels to meet demand, preventing fluctuations in frequency and disruption in energy supply. Meanwhile, the mission of distribution grid operators has historically been to provide the grid infrastructure that is used to deliver energy to end-users, maintain network quality and continuity of supply, and ensure network efficiency by investing in and maintaining the network to accommodate new consumption connections. In today's interconnected system, the role of the distribution level has however gained significance. While TSOs remain responsible for the physical security of supply (balancing), **DSOs are in charge of a growing portfolio of activities,** i.e., integrating growing volumes of RES and DER, empowering customers through flexibility services or energy sharing solutions, and ensuring reliable electricity supply through a more active system management.

In a nutshell, **DSOs play a growing role in managing system stability** in coordination with TSOs as further demonstrated below.

A) The role of DSOs and grid forming capabilities in strengthening system stability

DSOs have gained new competencies, including anticipating and responding to fluctuations in demand and supply, while effectively managing the intermittent and bi-directional energy flows. Traditionally, grid stability depended on synchronous generators that naturally provided inertia and voltage and frequency references. But, in an increasingly renewable-dominated energy

[12] WindEurope (2025): *2024 Statistics & the outlook for 2025-2030.* Available online; SolarPowerEurope (2025): *EU Market Outlook for Solar Power 2024-2028*. Available online.

system, fossil fuels are replaced by inverter-based resources (like solar PVs, batteries, wind). This is where the capabilities of inverters, including grid forming, will play a key role. Though they can present some technical challenges, they can also enable part of the system to operate in an island mode, disconnected from the main power system when needed.

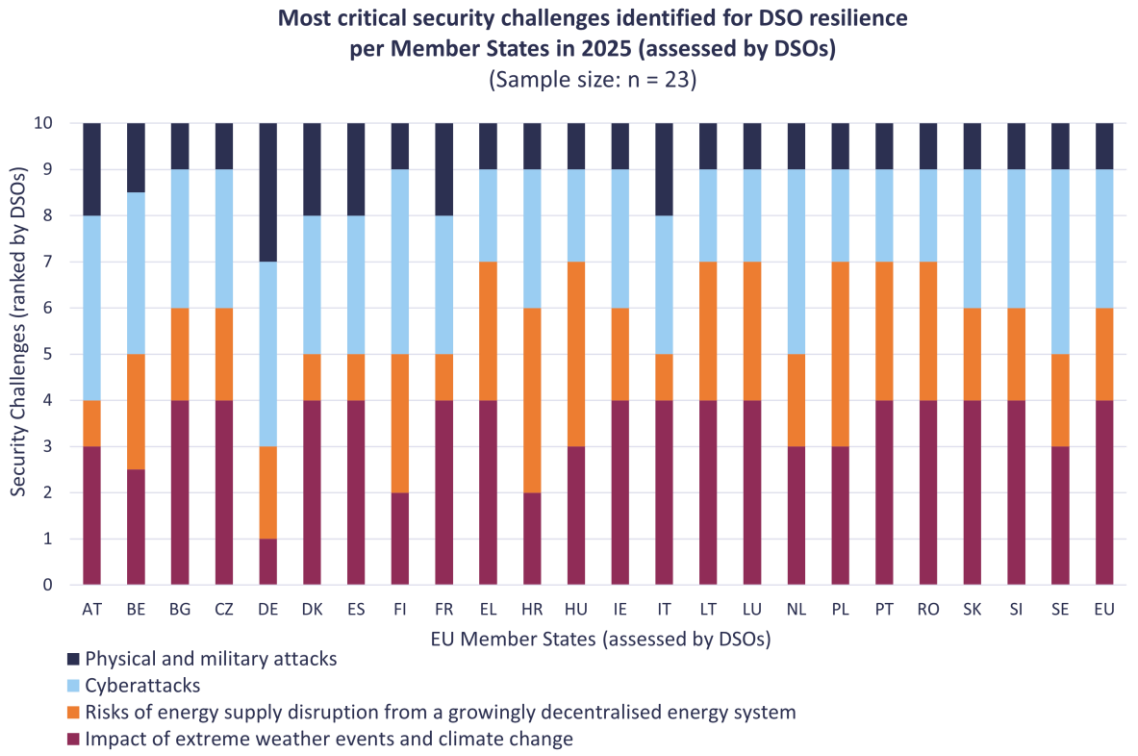
In brief, grid forming contributes more concretely to strengthening system stability and resilience by:

- **Emulating inertia and thus ensuring power quality** by resisting frequency changes and operating like a virtual synchronous machine.
- **Creating and maintaining voltage and frequency references**, essential for islanded microgrids by providing congestion relief and local grid stability.
- **Enhancing system resilience with black start capability** that enables power restoration after major power outages by re-energising itself after a blackout and being later reconnected to the main grid in case of islanded grids.

B) The role of digitalisation to enhance grid observability over the distribution network

DSOs are taking on a more dynamic role, enhancing **grid observability over the distribution network through smart systems and active-system-management capabilities**. Upgrading the grid with digital technologies enhances monitoring, communication, and eventually control capabilities that support grid operation and maintenance. Automation and other smart grid functionalities help DSOs identify faults early, improve reliability, and enable quicker, safer and more efficient fault corrections. By deploying smart meters and advanced digital technologies, DSOs can access near-real-time consumption data, enhancing network observability and monitoring of the state of the grid while supporting local supply-demand balancing in coordination with TSOs. DSOs also actively **interact with grid users providing responsiveness to changing demands and flexibility services** which are critical for congestion management and system stability.

Since the vast majority of flexible assets are connected to the distribution networks, DSOs play a pivotal role in supporting smooth operation over all voltage levels, alongside TSOs who are ultimately responsible for balancing. This collaborative approach enhances the overall system security within an integrated system-of-systems, though such interconnected systems also constitute an additional attack vector in terms of cybersecurity (malfunctioning of system, manipulated data, etc.).



The infographic ranks the security challenges faced by DSOs by priority in each country as identified by DSO respondents (n=23). Threats were prioritised on a 4-to-1 scale, with 4 indicating the highest priority, and total points were summed to assess overall significance. It shows the growing grid concerns across EU Member States over the risks posed by external challenges like cyberattacks or extreme-weather events.

Figure 3: Most critical security challenges identified for DSO resilience per Member States in 2025 (data based on a survey conducted in DSO Entity's CEG in 2025).

2.2 The key role of DSOs in enhancing the resilience of the EU's energy system against emerging external challenges

External challenges, such as cybersecurity and the impact of climate change, also increasingly affect DSOs' business and operation landscape and long-term strategy. Distribution grid planning increasingly needs to address multiple, simultaneous and cascading risks. The NIS2 Directive and the CER Directive for the first time introduced entity-level (i.e. DSO company or other actors) risk assessments for critical infrastructure based on an all-hazard approach. It shows the need to move beyond a narrow focus on physical security of supply towards integrated, risk-based decision-making encompassing cyber, physical, climate and hybrid threats, and that must eventually also include suppliers. In this context, DSOs are key, playing an increasingly essential role in enhancing grid preparedness to provide seamless energy supply during extreme climate events and prevent, prepare and react to cyberattacks, as explained below.

DSO Entity | Rue Belliard, 35 – 1040 Brussels BE
www.eudsoentity.eu | info@eudsoentity.eu

1) Cybersecurity challenge: The role of DSOs in tackling cyber-threats against EU energy infrastructure

EU energy infrastructure is facing growing cybersecurity threats

The increasing use of smart appliances, along with the deployment of RES and DERs, introduces additional points of communication in the DSO system as well as connectivity among DSOs, TSOs, aggregators, customers, Original Equipment Manufacturers (OEMs), and other stakeholders, with growing **risks of security vulnerabilities and cyberattacks against energy infrastructure**. DSOs therefore need to implement robust cybersecurity measures, monitor grid performance, but also coordinate with stakeholders and suppliers to ensure a unified defense against cyberthreats. With smarter grids, **DSOs are also responsible for protecting customers' sensitive information and personal data that they process against cyberattacks** while providing them with reliable and uninterrupted energy services. Furthermore, the **cybersecurity workforce shortage** also presents another challenge for DSOs. In the EU, a 299.000 shortage of cybersecurity professionals is estimated with 81% of companies considering their difficulties in hiring cybersecurity staff as a big risk for potential attacks[13].

All these challenges are further reinforced by the evolving nature of cyberthreats but also by the unstable geopolitical context and the security threat posed by Russia. These last years, the EU has experienced a rise in cyber-attacks with 200 cybersecurity incidents reported in the energy sector out of a total of 1.276 (15% of total; mainly due to system failures and malicious actions). This makes energy the second most impacted sector by cyberattacks according to the European Agency for Cybersecurity (ENISA)[14]. While no official aggregated data are available due to their sensitive nature, ENISA reports confirm that disruptive attacks have doubled in recent months with many traced backs to Russian backed groups or Russian threat actors.

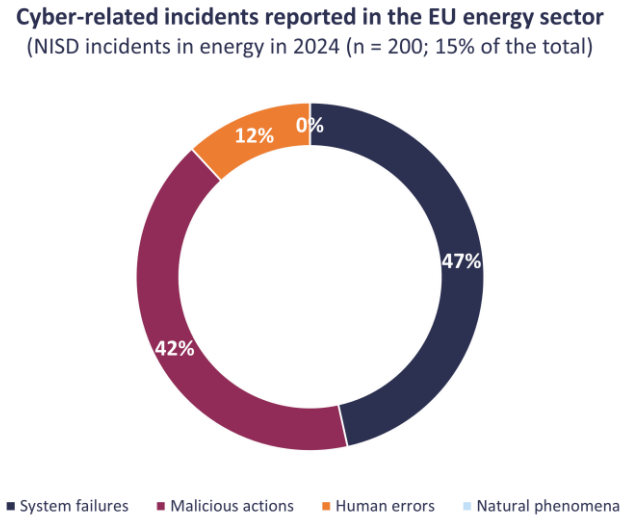


Figure 4: Cyber-related incidents reported in the EU energy sector. Data from the EC's 2024 Annual Report on the NIS Directive Security incidents[15].

[13] European Commission (2025). *EU Cybersecurity Skills Academy*. Available online.
[14] European Commission (2025): *2024 Annual Report on the NIS Directive Security incidents* (p.44). Available online.
[15] European Commission, op.cit.

How DSOs enhance EU cybersecurity

Cybersecurity is a cornerstone of the EU's energy security and **DSOs play a key role in implementing the EU cyber legislation**. Several DSOs are listed among the critical entities covered by the CER Directive (2022/2557/EU) and the NIS2 (2022/2555/EU). This EU horizontal legislation is further supported by the **NC CS** (2024/1366/EU)[16] developed by DSO Entity and ENTSO-E to ensure a unified approach to cyber-risk management (see box below). According to DSO Entity's estimates, around 100 DSOs are listed as critical-impact or high-impact entities under the NC CS. The NC CS needs to interact seamlessly with the NIS2, the CER Directive and the rest of the horizontal cybersecurity framework to ensure consistency across all provisions (i.e. definition and thresholds fit).

Network Code on Cybersecurity for the electricity sector (2024/1366/EU, NC CS): A major step in strengthening the cyber resilience of critical energy infrastructure

The NC CS entered into force on 13 June 2024 and provides:

- European rules on cyber-risk assessment, common minimum requirements, cybersecurity certification of products and services as well as monitoring, reporting and crisis management in the electricity sector.

- Clear definition of the roles and responsibilities of each stakeholder. It also identifies the entities that perform digitalised processes with a critical or high impact in cross-border electricity flows, their cybersecurity risks and the subsequent necessary mitigation measures.

Following up on the development of the NC CS, DSO Entity and ENTSO-E are jointly developing terms, conditions and methodologies (TCMs) to support its implementation. Two TCMs have already been delivered to the national regulatory authorities on the risk assessment methodology and the cyber-attacks classification scale methodology, and four others are under development.

Furthermore, **DSOs develop risk assessments, crisis management plans and business continuity plans to enhance preparedness for cyber-attacks**. Through Business Continuity Management (BCM), DSOs strengthen their operational reliability and capacity to respond when incidents occur (also against other types of incidents than cyber incidents caused by climate change). It contributes to enhancing system resilience by ensuring the maintenance of DSOs' critical business functions, minimising disruptions that can affect vital assets, and resuming operations with minimal impact. Continuous adaptation is furthermore essential as new methods are constantly developed by cyber-attackers. DSOs are thus continuously learning, enhancing staff skills and strengthening cybersecurity strategies through a proactive approach to safeguard operations and customer data (see practice below).

[16] European Commission (2024): *Regulation on cybersecurity rules for cross-border electricity flows*. Available online.

Portugal: Strengthening cyber skills via internal company's awareness programs and training

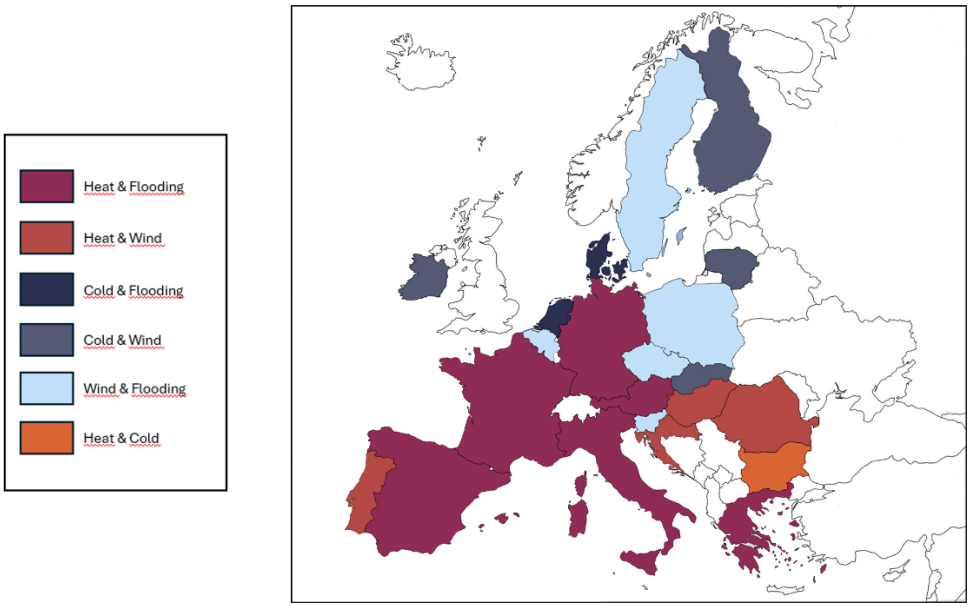
The Portuguese DSO, E-REDES, has established an internal comprehensive program to embed cybersecurity into its organisational culture, encompassing all staff, specialists, management, and external collaborators. The program integrates mandatory annual training, simulations (e.g., CiberPerseau, CMX), e-learning modules (e.g., phishing quiz), and targeted workshops. Continuous communication through daily updates, a dedicated cybersecurity intranet, and the 'Cybersecure' vulnerability reporting channel, reinforces engagement and awareness across the DSO company. Collectively, these measures strengthen ongoing cybersecurity vigilance, operational resilience, and secure management of critical energy infrastructure.

2) Environmental challenges: How DSOs adapt to the impact of climate change and extreme weather

Climate change and extreme weather: Growing challenges for grids

2024 marked the warmest year on record globally with average temperature exceeding 1.5°C above the pre-industrial level[17]. In Europe, temperatures are expected to rise faster than the global average[18] and countries are already experiencing more frequent extreme-weather events caused by climate change from heatwaves and wildfires to droughts and floods. As illustrations, wildfires burnt more than 1 million hectares of land in the EU at the end of the summer 2025[19]. Heavy flooding caused by storms also swept through Western, Central and Eastern Europe (e.g. Spain, France, Belgium, Slovakia, etc.) in 2023 and 2024. According to geographical characteristics, the nature and frequency of extreme-weather events vary across Europe, with each region facing specific climate-related exposure (see Figure 5) and hence require tailored resilience and adaptation measures.

[17] European Commission (2025): *EU Climate Action Progress Report 2025*. Available online .
[18] European Environment Agency (2025): *Global and European temperatures*. Available online.
[19] European Commission (2025): *EU Strategic Foresight Report*, p.9. Available online.



The map is based on data from a DSO Entity's survey conducted in 2025 within the CEG with responses from DSOs in 23 EU Member States (in color on the map). Respondents were asked to identify, out of five proposals, the two extreme weather events with the most critical impact on their distribution grids faced in their respective countries.

Results show that extreme heat and extreme cold are most frequently selected. Southern Europe, particularly the Mediterranean region, is most affected by extreme heat, including intense heatwaves and prolonged drought; while Northern Europe faces cold spells, snowfall and winter storms. Flooding and wind risks occur across Europe reflecting large-scale meteorological systems (European cyclones, Atlantic storms, etc.).

Figure 5: Extreme weather events impacting EU Member States in 2025 (data based on a survey conducted in DSO Entity's CEG in 2025).

Climate-related disasters can disrupt energy supply triggering cascading effects across all layers of society, with extreme-weather events responsible for EUR 12 billion annual economic losses on average in the EU[20]. Such events increasingly put a strain on DSOs that need to adapt their grid to prevent potential destruction of network equipment and subsequent power outages directly affecting customers. Furthermore, climate change can also have indirect effects on the grid and cause significant increases in demand, exacerbated by shifting consumption patterns, such as higher demand for air conditioning during heatwaves. The cumulative impact of climate change threatens both the reliability and affordability of energy supply for consumers. It is therefore essential to consider and increase wherever possible the physical security of field crews that are deployed in extreme weather conditions or their aftermaths.

At the distribution level, various power assets are exposed to specific risks:

- **Overhead power lines** and their pylons are affected by strong winds, flash floods and falling trees, as well as by ice sleeves with potential effects on bare power-line conductors.
- **Substations** may sustain potential flood damage, if inadequately protected.
- Even **cables** may be disrupted by avalanches caused by smelting glaciers or floods.

[20] European Commission (2021): *Forging a climate-resilient Europe - the new EU Strategy on Adaptation to Climate Change*. Available online.

DSOs' climate adaptation measures: How to safeguard grids against extreme-weather events

DSOs are evolving into resilience actors implementing comprehensive adaptation measures and internal resilience strategies to mitigate the impact of extreme-weather events and ensure the continuity of energy supply. In line with the CER Directive (2022/2557/EU), they play a **key role as critical entities in conducting risk assessments** covering notably climate risks, business continuity management and rapid recovery, as well as related physical security investments. **DSOs invest in enhancing the physical resilience of grids by strengthening and adapting assets to climate-specific risks**. To do so, DSOs, aiming at efficient investment and operations, need regulatory systems that adapt fast to rising costs by adjusting CAPEX and OPEX when and if necessary. For instance: DSOs bury overhead lines in flood-prone areas, design waterproofing substations, upgrade equipment like heat resistant cables, better select installation sites with less exposure, improve vegetation management, and increase the automation of medium-voltage (MV) network and remotely controlled equipment to fasten fault detection and restoration. For this, DSOs must ensure that the necessary equipment is secure, affordable, and readily available. This may require an increase in EU production capacity to enable the entire value chain to respond effectively to climate-related events. In the future, this could potentially be extended to enhanced DSO cooperation during crisis situations, allowing system operators to provide mutual support through the sharing of spare equipment, where permitted by regulatory frameworks and sufficient alignment of technical specifications.

In parallel, DSOs strengthen **monitoring, emergency management and real-time responsiveness** through real-time grid data analysis, flexibility services and grid forming capabilities to reduce power outages and accelerate recovery times for customers. The use of **digital tools such as weather forecasting and alert systems** also enables DSOs to better predict potential climate hazards and enhance grid preparedness (see practices below). Data are used in long-term resilience strategies like contingency, crisis management, and business continuity plans ensuring rapid restoration and operation reliability. Regular exercises to train the necessary capabilities of analysis and reaction are also becoming increasingly important.

The benefits of using advanced data-driven tools to adapt to climate change impact

Good practices in several Member States showcase the growing deployment of advanced climate-risk and multi-risk tools to identify threats, anticipate impacts, and guide prevention, protection, and restoration across the power system. In **Portugal**, the DSO E-REDES developed a tool, as part of an internal adaptation strategy, that integrates climate downscaling, geographical mapping and AI-based models. It contributes to assessing asset vulnerability, prioritising investments, and designing adaptation measures enabling data-driven local decisions. In **Greece**, the EU-funded R2D2 initiative under Horizon Europe, through its demonstration led by the DSO HEDNO, provides a comprehensive multi-risk framework covering climate extremes and cybersecurity via four dedicated tools (i.e., C3PO, IRIS, PRECOG, and EMMA). These tools support the assessment of risks and vulnerabilities of critical infrastructure against potential threats (e.g. climate incidents, cybersecurity threats and potential causes of power outages), prevention and restoration across the energy value chain. It therefore strengthens the security of critical network components and enables the deployment of predictive maintenance capabilities. In **Slovakia**, a real-time, data-sharing platform called Meteodata is being developed under the Project of Common Interest (PCI)

Selena project and integrates information among DSOs, fostering coordination and collaborative resilience planning to anticipate and mitigate risks from extreme weather. In **Spain,** the DSO i-DE deploys a predictive, computer-based system anticipating disruptive events, hence contributing to enhancing preparedness and informed decision-making.

Greece: Coordinated and cross-sector approach to climate adaptation

Greece strengthens system resilience through a coordinated, multi-level approach to climate adaptation and disaster management supported by guidance from the National Mechanism for Crisis and Risk Management. The General Civil Protection Plan "XENOKRATIS" ensures coordination among critical infrastructure operators including TSO and DSO, ministries, electricity network operators (the Greek TSO IPTO and DSO HEDNO), and Forest Firefighting Units, while hazard-specific sub-plans for floods, wildfires, snowfalls, and earthquakes are reinforced through regular exercises. Preparedness measures are complemented by large-scale simulations like THESEUS 2024 and MINOAS 2024, which strengthen cross-sector coordination and emergency readiness. When incidents occur, DSOs work closely with authorities to conduct damage assessments, prioritised restoration, and rapid deployment of technical teams.

Spain: Lessons learnt from DANA storm in October 2024 in Valencia: Preparedness, reaction and fast restoration of electricity supply[21]

In October 2024, the 'DANA storm' hit Valencia with daily rainfall of 400 l/m² and unprecedented hourly record of 185 l/ m², which caused severe disruption to the electricity distribution network leaving 180.000 customers without electricity. The Spanish DSO, i-DE mobilised around 500 people from Valencia and other regions to restore service and repair affected network installations. Half of the electricity supply was restored within 24 hours, 85% within 48 hours and 95% within 72 hours. It demonstrated the capacity of the grid to restore electricity in record time thanks to human and technical resources. Fast restoration was made possible by i-DE's anticipated preparation and investment in grid infrastructure, technology and digitalisation. Since 2023, i-DE collaborates with the start-up Wozalabs on the creation of an AI-enabled digital twin for long-term planning of overhead lines, integrating climate models, satellite imagery and historical fault data to identify areas at high exposure to future weather hazards. Following the DANA storm, i-DE reacted by further reinforcing and accelerating its resilience measures, investing EUR 100 million to redesign the distribution grid affected by the storm and make it more resilient and efficient. Launched in 2024, the Il Lumina Project combines design changes in assets with equipment of latest digitalisation standards. Expected to bring benefits to 650.000 customers, the initiative is due to be completed in 2026.

[21] Iberdrola (2025). "Iberdrola España invests €100 M to redesign the power grid affected by the severe weather event in Valencia". News. Available online.

3) DSOs are strengthening the physical protection of the grid infrastructure against potential attacks

Today European DSOs operate and manage over 10 million kms of cables and infrastructure out of the 11.3 million km of power network in Europe and connect more than 250 million customers, both households and businesses[22]. While it is impossible to physically safeguard all elements of such a vast infrastructure, it is also very apparent that in the context of geopolitical tensions, grid infrastructure also needs to further enhance its resilience against potential malicious physical attacks that threaten security of supply with potential impact on all parts of society. Under the CER Directive (2022/2557/EU), the NIS2 (2022/2555/EU, Art. 21) and the NC CS (2024/1366/EU, Art. 41), DSOs as other energy critical entities are required to carry out risk assessments and adopt technical, security and organisation measures to protect their infrastructure and especially its most critical elements against man-made threats. This includes the protection of assets against physical sabotage, intrusion and malicious attacks from any menaces including state actors, hybrid warfare actors, etc. To enhance the physical resilience of their grid, DSOs implement fencing, surveillance and intrusion detection (sometimes with drones), emergency response protocols in coordination with local authorities, TSOs and law enforcement. They also organise staff training and simulations to conduct stress tests and prepare teams for targeted physical attacks.

Slovakia: Increasing the physical protection of distribution grids and using new responses to face emerging threats

The Slovak DSOs Západoslovenská distribučná (ZSD), Stredoslovenská distribučná (SSD) and Východoslovenská distribučná (VSD)[23] enhance the protection of their substations and other critical assets against unauthorised entry. They implement perimeter security measures such as fencing, security staff, and surveillance, and increasingly deploy new security technologies such as radar-based protection systems. To address emerging threats such as those posed by unmanned aerial vehicles (drones), they develop innovative responses. For instance, the two Projects of Common Interest (PCI) Selena (involving all three Slovak DSOs above) and the Danube InGrid (involving ZSD, the Slovak TSO SEPS and the Hungarian DSO EED E.ON) will deploy a new generation of automatically operated substations as well as anti-drone protection systems designed to secure substations and grid lines against hostile or accidental incursions.

[22] According to a DSO Entity's survey, around 98% of industries are connected to the DSO grid in average in 2024.
[23] ZSD connect approximately 1.22 million customers, SSD 0.79 million and VSD 0.67 million.

3. Measures linked to grids to ensure reliable energy and resilient infrastructure

3.1 The need for a forward-looking regulatory framework to enhance grid resilience

The transformation of the energy system demands substantial investment in the renewal, expansion, and smartening of the distribution grid, where two-thirds of the total EU grid investment are needed[24]. As previously shown, DSOs need to strengthen grid resilience to adapt to increasingly complex challenges while maintaining reliable supply. **Investments are required to reinforce the grid against extreme weather, enhance cybersecurity, ensure enough capacity for new connections, and build technical skills**. Overall, general EUR 730 billion investments will be needed by 2040 for distribution grids[25], with EUR 33 billion specifically for resilience alone between 2020-2030 (a figure preceding the latest REPowerEU targets)[26]. Given the more frequent extreme-weather events (expected to keep occurring even under Paris Agreement's scenarios) and the other growing challenges, investments in grids are a non-regret option to ensure security of supply and energy independence in Europe.

To enable these investments, **regulatory frameworks need to adapt towards a more long-term, forward-looking and anticipatory approach**. Regulations should provide a predictable and supportive framework managing uncertainties linked to longer forecast periods and more complex planning considerations, such as the accelerated RES deployment or growing climate impacts. These frameworks will enable DSOs to make more efficient investment decisions via an anticipatory investment approach[27] already encouraged under the Electricity Market Design (EMD) reform[28]. The EC's guidance on anticipatory investments (COM 2025/3291/EU)[29] in fact identifies investment in grid resilience as potential anticipatory investments by listing: "**Developments to increase long-term system resilience**. For instance, this may include network **developments to increase climate resilience** (ensuring readiness for more adverse climatic years for example through structural reinforcement of lines).". Aligning these efforts with longer-term planning on the DSO side and strategic tools like Distribution Network Development Plans (DNDPs)[30], alongside resilience and contingency plans, will strengthen the resilience and adaptability of DSOs.

---

[24] "Around EUR 375-425 billion of investment in distribution grids is necessary by 2030. Overall, the Commission estimates that EUR 584 billion in investments7 are necessary for the electricity grids this decade."- see European Commission (2023). Communication COM (2023)757 "Grids,the missing link – An EU Action Plan for Grids" (p.2); See DSO Entity (2025). Let's Connect brochure.

[25] European Commission (2025). Communication COM (2025)1005: *European Grids Package*. Available online.

[26] Eurelectric (2021): *Connecting the dots: Distribution grid investment to power the energy transition.* Available online; *The Coming Storm*. Available online.

[27] DSO Entity (2025, February): *Anticipation investments – An initial regulatory discussion* report. Available online.

[28] European Parliament and Council of the European Union (2024): *Regulation (EU) 2024/1747 of 13 June 2024 amending Regulations (EU) 2019/942 and (EU) 2019/943 as regards improving the Union's electricity market design.* Available online.

[29] *European Commission* (2025): *Commission Notice on a guidance on anticipatory investments for developing forward-looking electricity networks*], OJ C 2025/3179, p.3. Available online.

[30] DNDPs provide robust long-term information and are already set in the Electricity Market Directive (2019/944/EU)[30]. Related provisions under Art. 32(3) and (4) need to be transposed to provide increasing visibility.

To wrap up, following measures should be supported:

- The swift implementation of the EC's Guidance on anticipatory investments.
- Further support for the implementation of the EMD reform with Art. 18(2) of the amending Regulation 2024/1747/EU to ensure forward-looking regulatory frameworks, adequate compensation and predictability about future earnings.

Italy: Foward-looking investments

In the Italian context, the management of emergencies within the electricity distribution network is governed by CEI Guide 0-17 and Italian Regulatory Authority for Energy, Networks and Environment (ARERA) Resolution 617/23. In accordance with these documents, each DSO is required to prepare and update **an emergency plan**, outlining the set of actions aimed at **reducing risks and mitigating the effects of emergency events on the electrical grid**. The Italian DSO, E-Distribuzione, in managing emergencies and critical events, has adopted a **structured and systematic approach based on four fundamental pillars (the "4R" approach): (1) Risk Prevention, (2) Readiness, (3) Response, and (4) Recovery.**

The 4R approach aims to make every phase of emergency management structural and continuous. While in the past the electrical system was required to ensure service continuity in the face of less intense and more predictable weather events, in recent years network operators started to deal with prolonged and widespread outages, with a significant impact on all types of users connected to the distribution network, whether energy consumers, generation plants, or prosumers.

The concept of "power system reliability" (that is, its ability to withstand single accidental faults, the so-called n-1 security) must therefore be expanded to include additional risk factors. The electrical grid must consequently be resilient, meaning capable of withstanding strong external stresses, such as extreme weather events, while limiting their effects both in terms of the number of users affected and the time required for service restoration. The "4R" approach is designed to make the emergency management process continuous, not limited solely to critical events.

Risk Prevention

This includes long-term preventive activities, such as:

- Maintenance interventions to reduce network vulnerability following exceptional events
- Grid development initiatives to reduce asset ageing—and therefore failure rates—and to install innovative and resilient technologies capable of better handling extreme weather events. More than **1 billion€ has been invested between 2017 and 2024** to increase network resilience. With ARERA Resolution 112/25, due to the increase in extreme events caused by climate change, the NRA has for the first time introduced the possibility of going beyond the current network fault rates and critical issues, also considering **prospective scenarios**.
  On this new framework, E-Distribuzione is investing roughly **3 € billion in 2025-2027** with a major Resilience Program.
- Structured checks of all procedures and preparations needed to manage emergencies, carried out as part of the "summer plan" (in preparation for summer-related issues) and the "winter plan" (in preparation for winter-related issues);
- Periodic emergency simulations involving all structures and personnel normally engaged in emergency management;

- Coordination with local and national institutions, formalised through the establishment and update of specific agreements and periodic meetings to share emergency management procedures;
- Updating and revising e-Distribuzione's Emergency Operational Plan.

Readiness

This includes activities carried out in the immediate lead-up to potential emergency events, such as:

- Declaration and management of alert status;
- Real-time monitoring of weather events and their impact on the network;
- Effective and continuous communication.

Response and Recovery

These include all activities carried out during the emergency, such as:

- Coordination of field workforce (both e-Distribuzione and third parties) to restore service to as many customers as possible in the shortest possible time;
- Establishment of dedicated units for emergency governance;
- Management of task forces (i.e., people, vehicles, and materials) mobilised from unaffected areas to impacted areas;
- Periodic updates of internal and external reporting;
- Preparation of the emergency report and execution of the post-emergency debriefing.

France: Integration of climate resilience in DNDP

The French DSO, Enedis, integrated internal climate adaptation measures and necessary investments in resilience in its DNDP. EUR 1 billion per year in network resilience and modernisation will need to be added to investment in grid reinforcement. It highlights that, in total, annual investments in Enedis' grid go from an average of EUR 4 billion (e.g., 4.4 billion in 2022) to consistently over EUR 5 billion per year.[31]

The climate adaptation measures laid down in the DNDP include:

- **Investment strategies steered towards climate risks**: Network reinforcement adapted to local climate risks (e.g., strengthening overhead lines against ice, heavy wind and tree falls; and reinforcing underground lines against flooding and heat waves). For instance, 20.000 km out of 48.000 km of overhead lines are planned for consolidation or burial by 2032.
- **Climate hazards plan ("plan aléas climatiques")**: A regularly updated preparedness plan based on: (1) mapping of weather-related risks depending on their occurrence probability; and network components' vulnerability; and (2) definition of targeted actions, security objectives, actions and prioritisation criteria.
- **Rapid power restoration**: A commitment to restore supply to 90% of affected customers within 48 hours, supported by the electricity rapid intervention force (FIRE) that can deploy 2.500 technicians and equipment within hours following a weather alert.

[31] Enedis (2025): *New Electric France 2027 and 2032: Enedis publishes the preliminary document for its future Distribution network Development Plan for electricity distribution*. Available with link for DNDP here.

Flood-risk management programme: A 3D flood-mapping tool targeting flooding risks in power vulnerable zones, especially in urban areas, and bringing together data on the DSO network and hydrographic geodata from flood scenarios.

Portugal: Coordination of climate resilience actions in the National Energy and Climate Plan (NECP)

Portugal's NECP 2021–2030 provides an integrated approach to climate adaptation. It integrates grid resilience and promotes measures such as converting overhead lines to underground networks in high-risk areas, investing in cyber-physical protected digital infrastructure, and enhancing grid observability and sensorisation. It also includes risk assessments, preventive and emergency plans, sectoral climate adaptation strategies, and flexible network planning that incorporates climate-proofing measures. Operational measures include strengthening transmission and distribution assets to withstand wind and flooding, deploying advanced monitoring and maintenance technologies, and developing contingency plans for rapid service restoration.

Investing in grid modernisation and climate-resilient infrastructure

Good practices can be found in several countries, demonstrating the long-term benefits of targeted investments in grid modernisation to enhance climate resilience. In **Sweden**, for instance, after the Storm Gudrun in 2005, the Krafttag programme weather-proofed over 96% of the MV network through systematic underground cabling, which proved cost-effective compared with alternatives such as insulated overhead lines. **Lithuania** has reinforced resilience by undergrounding aerial lines in forested areas, upgrading substations for robust operation, implementing automation at 10 kV points, and using mass outage prediction tools to enable rapid response. **Romania** focuses on modernising MV lines with insulated overhead cables, extending automation in primary substations, installing remotely controlled equipment in secondary substations, and strengthening communication networks with 4G and fiber-optic infrastructure. In **Germany**, after the devasting floods in the Arh Valley in 2021, several measures were implemented to make networks more resilient against flooding and heavy rainfall, such as using flood and heavy rain hazard maps to guide site selection, and ensuring flood-resistant construction (e.g., raised foundations, protective plinths). Furthermore, the DSO E.ON rolls out 450 MHz technology across its network to enable blackout-proof communication during emergencies, and several of its regional companies are testing and deploying suitable materials and components to withstand heatwaves.

3.2 Focus on the implementation of the existing cyber-related EU legislation

In an increasingly unstable geopolitical environment, the cybersecurity of critical infrastructure needs to be enhanced. Recent EU cyber-related legislation, together with the NC CS, provides a key framework to strengthen cyber-resilience. As the EC plans to revise the energy security framework, the **focus should be on the effective implementation of existing cyber legislation**.

DSOs need sufficient time to comply with recently adopted rules such as the NIS2 and the NC CS. In parallel, Member States should be supported in their implementation efforts. **In several countries, the implementation of the NC CS is delayed** due to the absence of nominated national competent authorities and the priority given to the transposition of the NIS2 (2022/2555/EU)[32]; and cooperation between the Agency for the Cooperation of Energy Regulators (ACER), ENISA and DSOs should be further enhanced. Compliance with these cybersecurity and resilience obligations also generate operational costs for DSOs and therefore **recognising the costs incurred by the preparation and future implementation for grid operators within the regulatory framework is important.**

Apart from the recognition of costs, another external factor can create additional pressure on grids when strengthening cybersecurity. Labour shortages mainly caused by the necessity to increase staff needed for the energy transition and the transformation of jobs due to the digitalisation of the sector (incl. cybersecurity), make upskilling and recruitment increasingly challenging. Continued support for the EU Cyber Skills Academy and similar initiatives (e.g., exchange of best practices) is thus key to **ensuring the development of adapted skills needed to enhance cyber-resilience**.

Slovakia, Czech Republic and Hungary: Joint PCI electricity smart grid project enhancing cybersecurity through cross-border cooperation

Through the electricity smart grid PCI Selena, Slovak, Hungarian and Czech DSOs jointly work to enhance and integrate considerations on energy security, efficiency and resilience in projects by cooperating on cybersecurity. The project establishes a **Cybersecurity & Resilience Cross-Border Centre** for testing and validating cybersecurity tools. It also promotes Cyber Threat Intelligence sharing via the Managed Security Service Provider (MSSP) platform and collaborates to collect and exchange meteorological data to secure the stability and safety of the grid from extreme weather events**.** The Selena project shows the importance of supporting DSOs in resilience projects and cross-border cooperation as cyber risks transcend national boundaries, require sharing of practices, and affect Europe's interconnected electricity systems.

Italy: Cybersecurity regulatory framework

Italy has established the **National Cybersecurity Perimeter (PSNC)**, a stringent regulatory framework managed by the **National Cybersecurity Agency (ACN)** being somehow a precursor of

[32] While the NIS2 is already in force and legally binding, the NC CS remains in a voluntary application phase until it becomes biding in 2027.

what is now available in the NIS2. This framework identifies major DSOs as strategic actors essential to national security, subjecting them to rigorous oversight beyond standard corporate compliance. This national legislation has one of its pillars focused on supply chain security that helped significantly secure DSO procurement processes, introducing state-level validation for core grid technology updates.

The Italian DSO, E-Distribuzione, is working on a funded project (GEMINI) to found innovative way to improve the resilience of the grid thanks to a better usage of the data already available or to gather new ones. One of GERMINI's project streams is focused on cybersecurity aiming at improving the monitoring of the security signals in the MV and LV substations, correlating huge amounts of data already available searching for early security warnings and securing communications with quantum edge cryptography.

Cyber skills and staffing initiatives supported by national governments and other collaborations

National governments play a central role in supporting initiatives that build cybersecurity skills and help prevent labour shortages. In **Poland**, the Ministry of Digital Affairs offers structured training for employees within the national cybersecurity system, ensuring a workforce capable of addressing evolving threats. Similarly, in **Greece**, government-backed initiatives such us the annual initiatives "Hellenic Cyber Security Team/European Cybersecurity Challenge" that engages young people to develop technical skills and strengthening the future emerging talents.

Alongside governmental efforts, collaboration between universities, the private sector and industry partners is equally important. In **Sweden**, industry-driven initiatives such as Energi-CERT and at the Royal Institute of Technology provide sector-wide cybersecurity support and practical training. In the **Czech Republic**, DSOs work with the Czech Technical University in Prague to create tailored testing environments that combine academic expertise with operational DSO challenges, while in **Greece** postgraduate programmes and professional certifications further enhance advanced skills on the field.

DSO Entity's contribution as platform of knowledge sharing and best practices exchange on BCM

DSO Entity offers a platform for European DSOs to share knowledge and exchange good practices including preparing and responding to cyber-attacks, assessing risks and managing crisis affecting energy reliability. In 2023, the first step was the setting up of a dedicated working group supporting DSOs on BCM by facilitating exchanges on lessons learnt, strategic approaches to managing business continuity risks, and periodic resilience exercises. Given the sensitivity of these topics, strict confidentiality clauses are enforced. The BCM working group has progressively taken on different workstreams, including the development of a common BCM template to help harmonise frameworks across companies and countries. Furthermore, DSO Entity's Expert Group Cybersecurity issues a dedicated newsletter to high- and critical-impact entities under the NC CS to raise awareness on provisions, support implementation and disseminate best practices.

3.3 Enhanced TSO-DSO cooperation and a more inclusive involvement of DSOs when assessing pan-European security incidents

As shown in the previous chapter, DSOs play an increasing role in maintaining system stability and energy reliability in coordination with TSOs. In the changing energy system, DSOs have a growing role in active system management and grid observability over local and regional grids among others, integrating growing volumes of RES and DER, and empowering consumers through flexible services. This demonstrates the **importance of TSO-DSO cooperation to ensure seamless energy supply**. As a result, **DSOs must be more closely involved as equal partners** to efficiently identify system capacity needs, continue safeguarding grid security and ensure reliable supply to customers in a system-of-system.

The Iberian Peninsula blackout of 28 April 2025

On 28 April 2025 at 12:33 CEST, the energy systems of Spain and Portugal (and for a limited period, small parts of France near the border with Spain) experienced a blackout that led millions of citizens, industries, generators, telecoms, etc. to lose access to electricity supply[33]. The blackout occurred after the electricity system became unstable with unusual fluctuations in voltages that led to the disconnection of the Iberian system from the rest of Europe. System operators in Portugal and Spain, together with neighboring countries, cooperated to restore power and almost all demand was met again on early 29 April. The incident demonstrated that in an interconnected and decarbonised energy system, security of supply depends on all parts of the system, and grid resilience and emergency protocols are key. It also sheds light on the **need for enhanced TSO-DSO cooperation when assessing the root-cause of such security** incidents to ensure the involvement of DSOs as essential parts of the system.

In charge of the process, ENTSO-E has been conducting investigation into the causes of the incident. While the first factual report was published on 3 October 2025, a more detailed report on the causes of the blackout is expected in Q1 2026 and will also include recommendations from ENTSO-E on how to improve the resilience of the EU's energy system. To ensure the DSOs' view and experience is considered, DSO Entity should be further involved in the process. At the moment, DSOs engagement is limited and DSO Entity decided on setting up an internal ad-hoc expert group to reflect on the incident and share learnings and potential recommendations from a DSO perspective. Through this ad-hoc expert group, DSO Entity was included in the development of ENTSO-E's report. Such involvement could be further guaranteed and formalised in the future in the occurrence of similar incidents.

The Incident Classification Scale (ICS) methodology

The ICS methodology provides a harmonised EU-level methodology to classify and report on incidents on a 0-3 scale in the electricity system. Such a classification refers among others to the severity of the incident impact, the extent of the disconnection, its significance from a system point of view and whether an expert investigation is needed. The ICS methodology is developed

[33] IEA (2025): "The Iberian blackout has highlighted the critical importance of electricity security" article. Available online.

by ENTSO-E as part of their obligations under the Electricity Market Regulation (2019/943/EU; Art. 30).

Given DSOs' growing role in the decentralised energy system and how they can be affected by the classified incidents, they should be **further involved in the ICS methodology especially for scale-2 or scale-3 incidents** (with scale 3 as the highest). For instance, in cooperation with DSO Entity, DSOs should be represented in the ICS Expert Panel with appointed representatives from affected and non-affected DSOs and should be among the stakeholders who shall receive internal investigation reports.

In brief, **DSO Entity and DSOs should be more closely involved in assessing pan-European security incidents** through a collaborative approach with intensified exchanges with ENTSO-E and ACER at the EU level and **true TSO-DSO cooperation at national level**.

3.4 Effective implementation of permitting provisions and timely adoption of the Network Code Requirement for Generators 2.0 to accelerate the RES deployment

Apart from the resilience measures above, further support is needed to ensure the integration of rapid renewable deployment and connection of new demands (e.g., EV roll-out, heat pumps, batteries). Grid build-out measures are needed as DSOs play an important role in increasing the EU's energy independence as the largest integrators of renewables. The EU has developed new provisions to speed up the transition to homegrown renewables by addressing permit-granting procedures and revising technical standards for grid connection. However, implementation and adoption are lagging behind which could delay the decarbonisation process, and further EU support is therefore needed.

Faster implementation of permitting provisions

At the distribution level, network (environmental and construction) permits can take up to 8 to 10 years for the medium- and high-voltage network. While the revised Renewable Energy Directive (2023/2413/EU, REDIII) and the RePowerEU set new provisions to simplify, streamline and accelerate permitting procedures, their implementation is slow in Member States. It is of utmost importance to ensure the **effective and fast transposition of the REDIII at national level**, especially **Art. 15e on dedicated grid infrastructure areas** (supported by EU guidance for Member States) and **Art. 16f introducing the principle of overring public interest** given their expected benefits for grids. Further, EU support could also bring further simplification and **generalise one-stop shops** beyond the scope of TEN-E Regulation (2022/869/EU, Art. 7-10). The simplification provided under the proposal of **new EU regulatory permitting framework as part of the Grids Package is welcome** in this regard. Especially the new authorisation system for DSO and TSO infrastructure projects under the EMD (2029/944/EU) is positive; as well as the measures extending the overriding public interest to electricity grids, shortening procedures notably with tacit approvals, setting digital one-stop shops, and exempting grid projects from certain environmental assessments. Yet, attention will need to be paid to the consistency of the provisions during the next steps of the legislative process. Indeed, the reopening of several key legislative files, only recently adopted and not yet transposed, could lead to a broader reopening

of the texts beyond the initial scope and increased complexity, hence further delaying implementation.

Timely adoption of the revised Network Code (NC) on Requirements for Generators (RfG 2.0)

With the growing penetration of RES and DER, system operators increasingly require grid forming capabilities and the existing EU framework thus needs to be revised to be fit for purpose. The original 2016 Network Code on RfG was designed when inverter-based resources were mostly grid-following and did not explicitly specify grid-forming functions. Updated technical RfG are therefore needed to connect new technologies to the grid, ensure secure and reliable grid operation and support RES integration. In 2022, the EC initiated the amendment process of the NC RfG, that was developed with an important TSO-DSO cooperation through ENTSO-E and DSO Entity. However, **the adoption of RfG 2.0 as a delegated act has been significantly delayed**, pending for more than 2 years since ACER's proposal to the EC in December 2023, and is now expected in H1 2026. **Timely adoption is essential to maintain system stability and avoid delays in renewable integration and higher system costs**.

Similarly, the adoption of the NC Demand Connection is very relevant for the roll-out of an increasing number of (inverter-connected) Battery Energy System Storage (BESS) and data centers in Europe. Both types of installations are entering the grid in large numbers and with considerable loads (per unit and in total). The EU must avoid a situation where loads that will be very relevant for the future behavior and stability of the energy system are deployed using a technical standard that can no longer be considered state-of-the art.

4. Conclusions

The report showed the relevance of DSOs for the resilience of the European energy system, highlighting their growing role and responsibilities in strengthening system stability and guaranteeing energy reliability in coordination with TSOs. They are also conducive in enhancing the EU's energy independence by integrating the growing volumes of renewable and DER into the network, notably with grid forming.

Furthermore, the report demonstrated that DSOs are key actors in protecting critical infrastructure against emerging external challenges, shifting from a pure security of supply focus to an all-hazard approach. Against the growing number of cyberattacks in the EU energy sector, DSOs heavily contribute as critical entities to implementing key EU cyber legislation and enhance DSO readiness for stress situations. DSOs are also significantly investing in grid modernisation, conducting risk assessments, and taking adaptation measures to prevent and react to more frequent extreme-weather events as well as quickly restore power in case of cascading energy supply disruptions and power outages. For this, they also need to be supported by a strong value chain supplying secure, affordable, and available equipment to reinforce grids and react to emergency situations.

Recommendations

To strengthen the resilience of the EU's energy system, the role of distribution grids should be further recognised and considered in view of the upcoming revision of the EU regulatory framework for energy security planned for 2026. The report underlined that an integrated and holistic approach is needed to ensure that the needs of DSOs are taken into consideration, and support is provided where needed at EU and national levels. It will be therefore important to 1) ensure an **adapted and forward-looking regulatory framework** providing the necessary conditions for sufficient grid investment in resilience (e.g., anticipatory investments), 2) support the **effective implementation of relevant existing legislation** and support Member States in their transposition efforts (e.g., cybersecurity, permitting), and 3) **follow a system-of-systems approach to energy security and resilience**. DSO Entity will play a key role in collaborating with the EC, ACER, and ENTSO-E to share DSO perspective.

In brief, the following measures should be considered at the EU level:

- **The swift implementation of the EC's guidance on anticipatory investments** (C/2025/3179/EU) **and related provisions in the Electricity Market Directive reform** (2024/1711/EU) to ensure forward-looking regulatory frameworks are in place for grids to invest in the resilience of their infrastructure.
- **Stronger focus on the effective implementation of existing EU legislation**: EU support in cybersecurity should concentrate on ensuring cyber legislation is transposed at national level, especially the Network Code Cybersecurity (2024/1366/EU) and providing the right conditions to system operators (i.e., cost recognition, support skills and staffing initiatives). To further support the accelerated RES deployment, the recently adopted provisions on permitting should also be effectively and speedily implemented in Member States (Renewable Energy Directive 2023/2413/EU) and consistency ensured when negotiating and adopting the proposals under the Grids Package.

- **Timely adoption of the revised Network Code on Requirements for Generators (RfG 2.0.):** The adoption of the delegated act establishing the RfG 2.0 has been significantly delayed and is of utmost importance to update the technical requirements necessary to ensure reliable and secure grid operation and support RES integration.
- **A system-of-systems approach to energy security**: Greater involvement of DSOs as equal partners to TSOs and enhanced TSO-DSO cooperation for the assessment of pan-European security incidents, with DSO Entity as privileged partner.

DSO Entity | Rue Belliard, 35 – 1040 Brussels BE
www.eudsoentity.eu | info@eudsoentity.eu