CEDEC

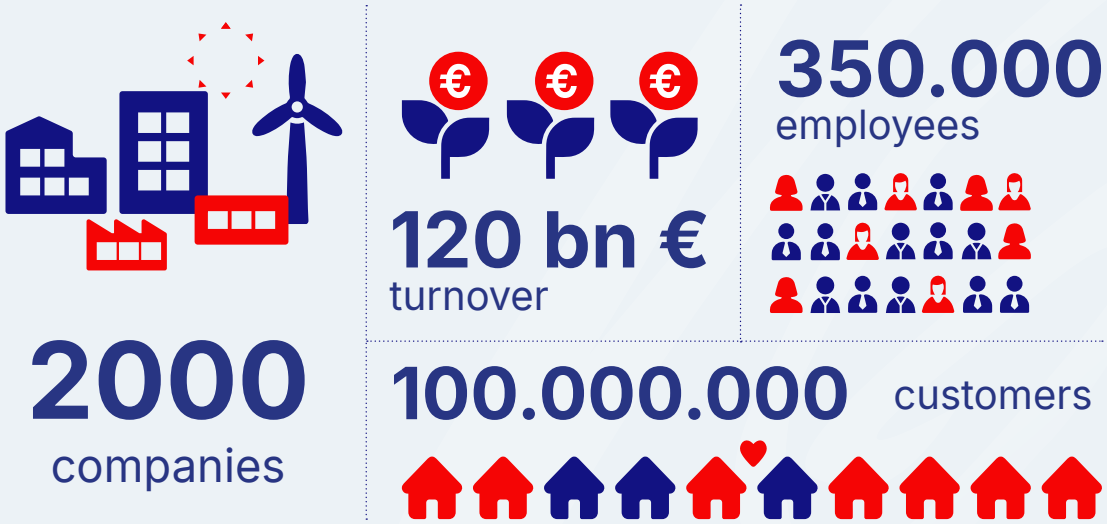
Enhancing energy system resilience:
the local integrated perspective

CEDEC

CEDEC

CEDEC is the European Federation of local and regional energy companies, representing the interests of 2000 local and regional energy and broadband companies across Europe, close to citizens and businesses, serving 100 million electricity, gas and district heating customers and broadband connections.

These predominantly small and medium-sized local and regional energy companies have developed activities in every part of the energy value chain. The wide range of services provided by these local utility companies is reliable, sustainable and close to the customer. Through their investments and local jobs, they make a significant contribution to local and regional economic development.



Introduction

The European Federation of local and regional energy companies (CEDEC) represents the interests of over 2000 local and regional energy companies, serving 100 million electricity, gas and district heating customers.

With rising instability of both the EU's natural and geo-political climate, these companies are increasingly subject to a variety of man-made or natural threats to the energy system, whether from extreme weather events, cyber-attacks, or acts of sabotage.

The unique characteristics of integrated local energy companies offer opportunities for increasing resilience of the energy system to these various threats. However, additional support through appropriate regulatory, financial and security frameworks will be necessary in order to enable local energy companies to be fully prepared to face these significant challenges.

Defining 'resilience' for energy systems

In general terms, 'resilience' refers to a system's ability to withstand disruptive events and adapt to and/or recover from them. The Critical Entities Resilience (CER) Directive defines the term as 'a critical entity's ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident'.

In relation to energy, this notion overlaps with other more well-established concepts such as security of supply, reliability, robustness, or operational flexibility – these all relate to a resilient system's ability to 'absorb' disruptive events. However, resilience also has some unique aspects, such as the speed with which a system can return to its normal state. Resilience is also concerned with rarer and more extreme events going beyond the 'expected' interruptions considered under resource adequacy or reliability.

In this paper, 'resilience' is approached from an integrated energy system vision, looking at every link in the value chain, from (local) generation over grids to storage and supply.

The resilience landscape for local energy companies

Climate change

Climate change is already causing significant disruptions to the operation of local energy companies, and these can be expected to intensify in future. As global temperatures rise, the climate becomes progressively more unstable, leading to increasingly severe and frequent extreme weather events. These extreme weather events can have major impacts on the energy system in a variety of ways.

Disrupting supply

The largest proportion of existing renewable energy capacity is connected to the distribution grid, and this decentralisation trend will continue as the energy transition progresses. However, most renewable energy sources are variable and weather-dependent, making them vulnerable to extreme weather events. Storms can force wind turbines to shut down (as was the case in Germany with storm Sabine in 2020), and solar panels lose efficiency in heatwaves or stop producing in bad weather. Regions can be locked up for weeks in the same weather pattern, causing a lack of wind and/or solar energy during a prolonged period, especially in winter. In addition, droughts due to heatwaves can even impact baseload generation from thermal plants (fossil, biomass, nuclear) or hydropower. These events impact security of supply and put grid stability under stress.

Damaging infrastructure

Extreme weather events of all kinds can cause serious damage to different parts of the grid. Overhead electricity lines are particularly vulnerable, as they can be damaged by falling trees due to high winds or wildfires, or build-up of ice sheaths from prolonged cold weather. Other above-ground infrastructure such as substations can also be affected by direct damage from floods, storms or wildfires. Extreme heat can additionally reduce the efficiency of both substations and powerlines. While underground energy infrastructure is generally better shielded against the elements, it is not impervious: after the severe floods in western Europe in July 2021, up to four months were required to restore gas supply in parts of Germany and Belgium.

Peaking demand

> Heat or cold waves can stress the grid through sharp increases in demand for cooling or heating. For example, in February-March 2018, the UK and Northwest Europe experienced freezing weather (dubbed 'the Beast from the East') due to a change in the Jetstream bringing cold air from Siberia. The resulting spike in heating demand and lower availability of gas imports from its neighbours almost brought the UK gas system to a stress condition. More recently, the heatwave that scorched Europe in summer 2023 caused power outages on parts of Rome's electricity grid.

In addition to these sudden shocks, both climate change and the response to it (e.g. the rise of renewables generation, electric vehicles or heat pumps) have more long-term and structural impacts on generation and consumption of energy which create challenges for management of the energy system.

Geo-political threats

In today's turbulent geo-political climate, and particularly since the Russian invasion of Ukraine, the threat of hostile actions against energy assets in the EU has increasingly come into focus.

As the energy sector becomes more digitised and interconnected, cyber-attacks represent a growing challenge for local energy companies. The multiplication of renewable and distributed energy sources, as well as increasing integration of internet of things (IoT) devices such as smart meters, sensors and controllers involves considerable exchange of data with and among system operators, as well as other relevant actors in the energy system. While these developments are essential to the energy transition, they also raise the exposure of the energy system to cyber-security threats. Energy companies are attractive targets for cybercriminals due to the critical nature of their services and the potential for significant disruption. Successful cyber-attacks can indeed result in loss of control over devices and processes, which in turn can damage infrastructure and cause wide-scale interruptions of service.

The vulnerability of EU critical energy infrastructure to physical attacks was also brought into focus by the ongoing military conflict in Ukraine. Although large-scale transmission infrastructure is a more obvious target for these kinds of acts of sabotage, local energy companies must also take appropriate measures to safeguard against this eventuality.

Local utility companies, connecting households and most industries, are at the centre of the energy transition. Their continued ability to safely and reliably provide energy to customers is essential to a functioning and flourishing society. Enhancing the resilience of the local energy system against the effects of climate change, as well as physical or cyber-attacks must therefore become a top priority in the coming years.

The contributions of local integrated energy systems to resilience

Decentralisation

Local energy companies are increasingly playing a key role in moving away from a traditional centralised and unidirectional energy system based on fossil and nuclear to a decentralised one dynamically integrating a variety of energy sources.

As the energy transition progresses, increasing amounts of renewable energy are being integrated at local level: by 2030, the distribution grid is expected to connect 70% of renewables capacity. Besides on-shore wind turbines and solar parcs, this includes a rapidly growing number of distributed energy resources (DERs) such as rooftop solar PV or small wind turbines. This decentralisation is not only occurring in the power system, but also for the gas system: the vast majority of biomethane plants are connected to the distribution grid. Electrolysers to produce renewable hydrogen are now mainly installed locally, giving additional value to renewable energy, and provided via the existing gas network to industry, transport or households.

Decentralised systems are inherently more resilient: if one part is affected, the rest of the system can

continue operating. By distributing energy production across multiple, smaller-scale sources, the risk of widespread interruptions of service caused by single points of failure on centralised grids can be greatly reduced. A shorter distance between the point of generation and the final customer also means that less infrastructure is needed to bring energy to its destination, reducing transport losses and exposure to extreme weather events or physical attacks.

From a cybersecurity standpoint, the growing number of distributed energy resources undeniably comes with increased exposure to attacks. However, the risk here is commensurate to the number of DERs operated by an entity: whereas a successful hack of a domestic solar installation will have negligible impacts on the energy system, access gained to a platform managing many assets can cause significant disruption. Ensuring that such entities have appropriate protocols in place to guard against cyber-attacks is therefore paramount to the resilience of decentralised energy systems.

Decentralised energy systems can also more easily adapt to fluctuations in energy demand. Local energy companies can intervene with a mix of measures through local generation, storage and timing of consumption enhancing grid efficiency and reducing the need for transportation from distant sources. Proximity to relevant municipal services (e.g. firefighters) and knowledge of local circumstances, resources and needs further enables local energy companies to more rapidly respond to any potential disruption to the energy system.

Diversification

Locally embedded multi-utilities and their related grid operators can harness and optimise the use of all the locally available resources through various technologies, so as to implement energy solutions specifically tailored to the potential and needs of the community. This enables a diversified energy profile combining a wide mix of energy sources, reducing the impact of disruptions to any single source – be it from extreme weather events or physical attacks – and increasing resilience. The differences in systems used for different types of energy infrastructure also reduce the likelihood of successfully disrupting several sources of generation via a cyber-attack.

According to geographical and geological conditions, a variety of renewable energy sources – such as solar, wind, geothermal, hydro, or biomass energy – can be leveraged. Excess renewable electricity from these projects can be converted to hydrogen via electrolysis, to be used in a variety of sectors. Creative uses of waste can also be found, providing sources of energy which would otherwise remain unexploited. Waste heat from industrial processes or residential wastewater can be integrated in local heating grids, while sustainable biomethane can be produced using a variety of locally available feedstocks – such as for example crop residues or manure from the agricultural sector, as well as municipal waste.

Local companies are also typically more agile and open to innovation than larger utilities. This flexibility allows them to adapt quickly to new technologies or methods for energy generation, management, and distribution, further diversifying their activities and thus strengthening the resilience of their local energy system.

Integrated energy system approach

Local integrated energy companies operating electricity, gas and district heating networks have a holistic vision of the energy system and the needs and available resources at the local level. They are therefore well positioned to optimally use the strengths of each energy vector to complement the others, enhancing the resilience of the overall system.

Electrification will be a major driver of the energy transition, due to the inherent efficiency of electricity as an energy carrier and due to its decarbonised character if produced from renewable energy sources and nuclear plants. However, it is not a silver bullet. Renewable electricity has high daily and seasonal variability, imperfectly aligns with the timing of energy demand, especially the lack of electricity from PV in winter for heating, and storage options (particularly seasonal) are limited. At the same time, increasing demands will be put on the power system by evolving uses of electricity, such as electric vehicles, heat pumps and industrial processes. This creates very significant challenges for power grid development and management, and requires appropriate measures to address the vulnerabilities arising from overreliance on weather-dependent renewable electricity.

Integrated local energy companies can enhance resilience by interlinking and combining different energy systems such as electricity, gases and district heating, as well as other sectors (transport, buildings, waste and wastewater). This approach is essential to enable the integration of increasing amounts of

renewable electricity, while also ensuring security of supply and stability of the system. In times when renewable electricity is in overproduction, power-to-gas provides a solution for long-term seasonal storage by transforming it into chemical energy (e.g. hydrogen or syngas). These renewable gases can then be used directly by industry, or to produce electricity and heat in a high-efficiency cogeneration plant, possibly also in connection with a district heating and cooling system. Surplus renewable electricity can also be turned into heat for use in district heating systems or kept in thermal storage.

Through their overview of site characteristics and customers' usage patterns, local energy companies can also optimally use existing energy grid infrastructure, avoiding the need for complex and costly overbuilding of the power system. District heating systems can for example provide heat with very high efficiency using a variety of sources, including electricity, molecules, or heat from industrial processes. Where energy intensive applications and processes are difficult to electrify and where electrification costs for specific end uses are too high, locally produced renewable and decarbonised gases can bring an efficient solution.

In addition, horizontally or vertically integrated energy companies can better guard against cyber-security threats through better coordination and management across different services. This integration can lead to more comprehensive security measures that cover all aspects of the company's operations, potentially reducing vulnerabilities that could be exploited in a cyber-attack. These companies can leverage shared resources, including cybersecurity teams and systems, across various types of utilities. This means that the expertise and technologies do not need to be duplicated for each utility, allowing for more efficient allocation of cybersecurity resources. Having a central cybersecurity team with a broad overview of the entire operation can also lead to quicker detection and response to threats.

Providing an enabling framework for local integrated energy system resilience

European legislation already addresses specific aspects of energy system resilience, such as 'resource adequacy', 'security of supply', 'reliability', or 'restoration'. However, these requirements are often focused on the power system only and, when they address other parts of the energy system, do so in silos.

Providing the right conditions for local energy companies to enhance resilience will require a more comprehensive approach taking into account the interrelated effects of climate change on generation assets, energy networks and consumption patterns, requiring in turn the increasing integration of energy systems. In order to do so, resilience considerations must be integrated in bottom-up approaches for energy infrastructure planning. Appropriate investment and financing frameworks also must be in place to help local energy companies face the significant costs required. The resilience benefits of a more highly decentralised and integrated system must further be ensured by appropriate accompanying cyber-security measures.

Integrating resilience in local and regional energy planning

Important new concepts have been introduced in the recent update of the Energy Efficiency Directive[1] and the recast gas and hydrogen markets Directive[2] , with a special role for local heating and cooling planning.

Building on the detailed expected energy demand for heating and cooling over the next decades, and taking into account the current heating systems (individual and collective), energy efficiency of the building stock, available grid capacities and local energy resources, an optimal framework can be developed for future investments of citizens and companies in their heating and cooling system. This will in turn determine the needs for investments and possible decommissioning of existing grids, and for the enhanced exploitation of local resources.

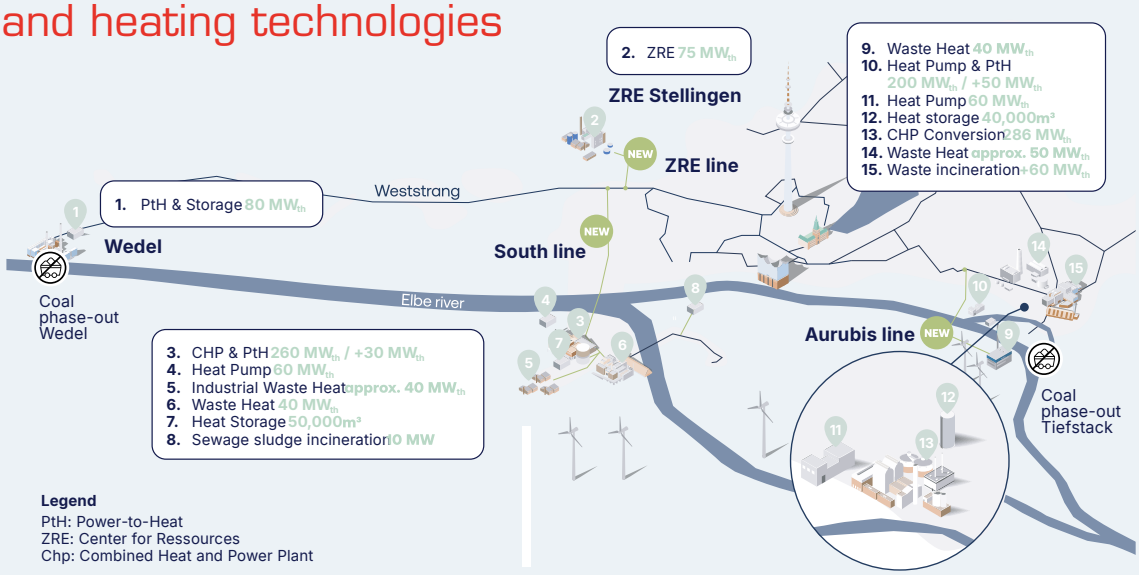
1 Directive (EU) 2023/1791 of the European Parliament and of the Council of 13 September 2023 on energy efficiency and amending Regulation (EU) 2023/955

2 Directive 2024/1788 of the European Parliament and of the Council of 13 June 2024 on common rules for the internal markets for renewable gas, natural gas and hydrogen, amending Directive (EU) 2023/1791 and repealing Directive 2009/73/EC

Coal phase-out by 2030 for district heating in Hamburg

Hamburger Energiewerke

Switch to a variety of sustainable heat sources and heating technologies



Digital twin for municipal heat planning

EWE, a regional energy provider in North-West Germany, provides a module for municipal heat planning that can be made available to local authorities. It consists of a digital twin that is designed to map several heat supply options. Due to the volatility of renewable energies, it is particularly important to be able to guarantee optimum security of supply. In addition, this approach aims to reduce pollutant emissions as much as possible. By pursuing these two objectives, a high level of resilience can be achieved, as dependence on fossil fuels can be reduced and cost pressure minimised. The heat planning module is also linked to an optimisation process for the energy infrastructure. Despite all the necessary resilience efforts, it is important not to build a parallel infrastructure for heat supply. This applies in particular to the construction of new hydrogen networks, which must be built in parallel to the existing electricity and gas networks. When decarbonising the heat supply, it is foreseeable that a significant proportion will be electrified. One of EWE's aims is to ensure the stabilisation of the electricity grid with the municipal heat planning module. The future demand for renewable electricity can thus go hand in hand with the requirements of the energy grids. This approach is essential to guarantee a secure and sustainable energy supply.

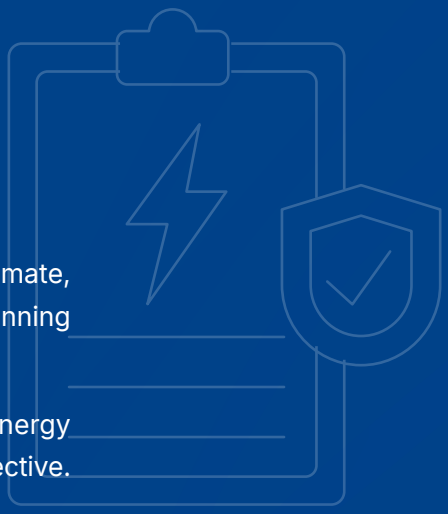
This heating and cooling plan must however be perfectly aligned and completed with the detailed multi-annual planning for electricity, gas and hydrogen grids that take also into account the energy demand for commercial and industrial consumption and for transport needs.

Although some resilience considerations may already be present in these planning requirements, including for distribution system operators, they do not take a sufficiently holistic view. In order to ensure resilience, any long-term planning must anticipate and integrate in a more systematic way the expected evolution of interlinked energy systems. To this end, systematic links between energy infrastructure planning and the risk assessments that critical infrastructure entities in the energy sector will have to carry out under the Critical Infrastructure Resilience (CER) Directive[3] should be ensured.

As the energy system becomes increasingly decentralised and integrates higher shares of intermittent renewables, promoting flexibility will be a key consideration for resilience. Therefore, the flexibility potential – through demand response by electricity customers, through energy storage (electricity, molecules, heat), and through sector coupling – should be structurally integrated in local and regional energy planning.

3 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC

Policy Recommendations



- Encourage the integration of aspects of resilience (climate, security, cybersecurity) in local and regional energy planning processes at an early stage.
- Create systematic links between local and regional energy planning and resilience assessments under the CER Directive.
- Structurally integrate assessment of flexibility potential in local and regional energy planning.

Incentivising investments in resilience

A new regulatory approach is required to incentivise all actors and all relevant elements in the energy value chains to contribute towards an enhanced resilience of energy systems.

Failure to address the impacts of climate change on the energy system, or to guard against physical or cyber-attacks, will lead to costs far in excess of those necessary to increase its resilience. However, the necessary adaptation investments still represent significant expenses, which operators will not enter into unless properly compensated.

Regulatory incentive mechanism for resilience in distribution grids

ARERA, the Italian energy regulator, has introduced resilience considerations in the DSO investment planning. This was decided after extreme snow events in 2017 led to prolonged disconnection of over 100.000 customers in Central Italy.

In 2018, an incentive-based regulation was introduced requiring all DSOs with over 300.000 to submit annual investment plans with a 3-year horizon aimed at increasing the resilience of the electricity distribution system against extreme climate events.

The resilience plans must identify interventions among those considered eligible under the mechanism to address specific risk factors. A cost-benefit analysis must also be provided for each planned investment, in accordance with ARERA guidelines.

If the DSO does not complete the intervention on time (within 12 months of the planned commissioning date), it is subject to penalties proportionate to the project costs and the accumulated delay. However, projects completed on time are eligible for a reward equal to 20% of the positive net benefit of the intervention.

In the 2019-2024 regulatory period, the 11 main DSOs in Italy to which this mechanism apply have concluded around 1000 interventions, not counting those still in the design/implementation phase. The most common interventions concerned the following risk factors:

- Ice sleeve formation on overhead lines (45% of total interventions)
- Heat waves (38% of total interventions).

For grid operators, the concept of 'anticipatory investments' – introduced in the recent Electricity Market Design review – offers a potential solution to reward investments in resilience enhancing assets and system solutions. Generally however there may be challenges to demonstrate precise ex-ante evaluations of the system-wide benefits of these investments in relation to capital investments and related operational costs. National regulators could therefore benefit from guidance at EU level on how to properly account for resilience benefits when analysing grid investments.

The current EU framework for electricity also imposes very restrictive conditions on DSOs to invest in and operate electricity storage at distribution level - de facto discouraging any initiative that could be developed at street level or district level. Given the importance of flexibility for the resilience of energy systems, investments in energy storage should be incentivised for all actors including DSOs.

Policy Recommendations

- Encourage NRAs to establish incentive frameworks for resilience-related investments, including through EC recommendations or ACER guidelines.
- Encompass resilience considerations when the concept of 'anticipatory investments' is specified in legislation or regulation.
- Review the restrictions in the Electricity Directive regarding ownership, development, management and operation of energy storage facilities, to enable DSOs to participate more actively in flexibility.

Financing a more resilient energy system

On national level, regulatory regimes should create appropriate frameworks for attracting the necessary capital that will be required to substantially expand and integrate the current separate energy infrastructures.

Dedicated funding must be earmarked – both at EU and national levels - for investments in climate resilience throughout the value chains.

At EU level, access for DSOs to EU funding is currently extremely limited, as the focus for EU-funds is on cross-border projects. The criteria for project approval – mainly the required minimum project size and cross-border elements - de facto exclude 99% of DSOs from general EU funding.

The complexity of application processes additionally creates challenges for all small and medium-sized DSOs (less than 1 million connections) to acquire EU funds for investments to ensure grid resilience. Some positive exceptions do exist, but are rare.

EU funding - ERA-Net Smart Energy Systems

The project **RESili8** is funded under Horizon 2020 involves a consortium of research institutes, industry, as well as the Austrian DSO Wiener Netze.

The project takes note of the inadequacy of over-provisioning to ensure the resilience of future energy systems, due to the social constraints on infrastructure buildout and the increasing complexity and digitalisation of energy systems.

RESili8 therefore focuses on developing a novel resilience solution package for cyber-physical energy systems, including optimal and sustainable planning and AI-based analysis of resilient architectures, continuous implementation and validation of resilient applications, and new solutions for resilient operation of energy systems. This innovative solution package will advance the green energy transition by ensuring security of supply and facilitates the further integration of green energy technologies.

Dedicated funding from the European Investment Bank for innovative energy projects apparently finds its way easier to the local energy companies. This demonstrates that adapted approaches and procedures can contribute to a more balanced access for small and medium-sized energy companies to European funding of projects.

Also at national level, more attention should be given to the earmarking of national investment funds for projects related with climate resilience throughout the value chains.

Policy Recommendations

- Earmark dedicated funding in EU, EIB and national instruments for resilience investments throughout the value chain.
- Facilitate access to EU and EIB funding for small and medium sized DSOs by streamlining and simplifying procedures.

Ensuring cyber-security in decentralised systems

The increasing integration of decentralised, interconnected and digitalised energy assets brings major benefits for the energy transition and the creation of resilient local energy systems. However, this also comes with a multiplication of the opportunities for cyber-attacks. Clear and well-designed obligations for both operators and manufacturers of these assets must therefore be in place to ensure local energy companies can fully employ their resilience-enhancing potential.

The updated Network Information Security (NIS 2) Directive[4], which will apply as of 18 October 2024, requires entities identified as essential to the provision of certain critical activities to implement cybersecurity risk-management measures and reporting obligations. However, it is currently unclear to what extent operators of distributed energy resources fall under the scope of these requirements. Although operators of DERs could correspond to several of the entity types listed in Annex I of NIS 2 (e.g. 'producers', 'market participants'), one of the main criteria for applicability concerns the size of the entity, which should be a medium-sized enterprise or larger[5]. However, concerning operators of DERs, the size of the entity is a secondary consideration to the type and number of assets controlled. Further guidance at EU level would be necessary to facilitate identification of DER operators with sufficient assets to create risks to the energy system and ensure they comply with proportionate requirements.

The differences in the size of entities covered under NIS 2 should however be considered when implementing the risk management requirements. Indeed, implementing the same 'gold standard' for compliance to

4 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148

5 According to Article 2 of the Annex to recommendation 2003/361/EC, a 'medium-sized enterprise' designates an enterprise which employs between 50 and 250 employees and has a turnover between EUR 10 and 50 million

all entities regardless of size can be counterproductive. Smaller structures may lack the resources and expertise to implement complex risk management frameworks compared to larger entities. The additional regulatory burden can impose higher compliance costs, potentially diverting resources from other areas for little additional benefit in relation to the risk profile. A differentiated approach enabling smaller structures to focus on proper execution of essential measures is therefore desirable.

Scalable risk assessments and assurances

The CyberFundamentals (CyFun) framework in Belgium has been set up by the Center for Cybersecurity Belgium (CCB) to provide tailored support and resources to help entities covered by NIS 2 to manage cybersecurity risks effectively.

The framework includes four different assurance levels which these entities can follow, each level containing additional measures to the previous one.

- **Small**: comprises non-technical recommendations intended for micro-organisations or organisations with limited technical knowledge, and allows them to make an initial assessment of their cyber-security risk management.
- **Basic**: contains standard information security measures for all companies. These provide an effective security value capable of addressing 82% of cyber-attacks with technology and processes that are generally already available.
- **Important**: designed to minimise the risks of targeted cyber-attacks by actors with common skills and resources in addition to known cyber security risks.
- **Essential**: includes measures to respond to the risks of advanced cyber-attacks by actors with extensive skills and resources.

A tool is provided to companies to assist in performing a risk assessment and identify the appropriate CyFun assurance level. Concerned entities can then undergo a certification process carried out by an accredited and recognised body for the relevant assurance level.

With the recently approved Cyber Resilience Act (CRA)[6], the EU now has a framework to adequately ensure the cybersecurity of DERs and other connected devices themselves. As of 2027, this legislation will indeed require manufacturers, importers and distributors to integrate cybersecurity into the design and development of all products with digital elements placed on the EU market. By ensuring that these products meet harmonised cybersecurity requirements, the risks of a cybersecurity incident on one

6 Regulation (EU) 2024/.... of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), not yet published in EU Official Journal

product being exploited to affect a whole system or other entities using this product are greatly reduced. Full implementation of the CRA is therefore essential to safeguard the resilience of local energy systems as increasing amounts of products with digital elements are integrated.

However, the CRA will only apply for new products. For legacy systems, technology providers should be required to make risk analysis carried out by specialists on the maturity of their cybersecurity systems. This will enable a balanced appreciation of the relevant measures to be taken in relation to these risks.

Policy Recommendations

- Provide guidance on NIS 2 implementation concerning operators of renewable energies, including classification of risk categories according to the type and number of assets.
- Promote the establishment of risk-based and scalable approach for implementation of risk management and incident reporting for entities under NIS 2.
- Set requirements for technology providers to carry out risk analysis on cybersecurity maturity of legacy systems.

Policy Recommendations

Integrating resilience in local and regional energy planning

- Encourage the integration of aspects of resilience (climate, security, cybersecurity) in local and regional energy planning processes at an early stage.
- Create systematic links between local and regional energy planning and resilience assessments under the CER Directive.
- Structurally integrate assessment of flexibility potential in local and regional energy planning.

Incentivising investments in resilience

- Encourage NRAs to establish incentive frameworks for resilience-related investments, including through EC recommendations or ACER guidelines.
- Encompass resilience considerations when the concept of 'anticipatory investments' is specified in legislation or regulation.
- Review the restrictions in the Electricity Directive regarding ownership, development, management and operation of energy storage facilities, to enable DSOs to participate more actively in flexibility.

Financing a more resilient energy system

- Earmark dedicated funding in EU, EIB and national instruments for resilience investments throughout the value chain.
- Facilitate access to EU and EIB funding for small and medium-sized DSOs by streamlining and simplifying procedures.

Ensuring cyber-security in decentralised systems

- Provide guidance on NIS 2 implementation concerning operators of renewable energies, including classification of risk categories according to the type and number of assets.
- Promote the establishment of risk-based and scalable approach for implementation of risk management and incident reporting for entities under NIS 2.
- Set requirements for technology providers to carry out risk analysis on cybersecurity maturity of legacy systems.

CEDEC

info@cedec.com

Galerie Ravenstein, 4 B2
1000 Brussels

www.cedec.com

CEDEC - European Federation of Local Energy Companies