MEDREG

DIGITALIZATION TRAINING

TRAINING REPORT:

THE DIGITALIZATION OF ENERGY MARKETS AND THE NEW ROLE OF CONSUMERS

Empowering Mediterranean regulators for a common energy future

Consumer Working Group (CUS WG)

Co-funded by the European Union

ABSTRACT

This document introduces a new topic within MEDREG activities which is the digitalization of energy markets. Aimed at MEDREG members, it presents the concept of digitalization of energy markets on different levels and exposes the pros and cons of digitalization. It also addresses cybersecurity and the importance of developing relevant procedures, national standards, and best practices.

This document was developed with the aim of providing a manual for the regulators who are interested in the topic and who are looking at enhancing their grids and services. It summarizes the contents and knowledge shared during the MEDREG training titled "Regulatory Implications of the Digitalization of Energy Markets and the New Role of the Consumers" by renowned experts, held in October 2021.

It may be used as an informative document for issues concerning the digitalization of the energy sector and as a resource to develop efficient national strategies to achieve the aspired goals.

AKNOWLEDGMENTS

This report is the result of the work of the MEDREG Consumer Working Group (CUS WG), which helped organise the digitalization training. MEDREG wishes to express its gratitude to the members of the CUS WG for their hard work and contributions. MEDREG is particularly grateful for the support of the speakers who shared their knowledge with the participants and helped reviewing this report.

DISCLAIMER

This publication was produced with financial support from the European Union. The contents are the sole responsibility of MEDREG and do not necessarily reflect the views of the European Union.

ABOUT MEDREG

MEDREG is the Association of Mediterranean Energy Regulators, bringing together 27 regulators from 22 countries, spanning the European Union, the Balkans and the MENA region.

Mediterranean regulators work together to promote greater harmonization of the regional energy markets and legislations, seeking progressive market integration in the Euro-Mediterranean basin. Through constant cooperation and information exchange among members, MEDREG aims at fostering consumers rights, energy efficiency, infrastructure investment and development, based on secure, safe, cost-effective, and environmentally sustainable energy systems. MEDREG acts as a platform providing information exchange and assistance to its members as well as capacity development activities through webinars, training sessions and workshops. The MEDREG Secretariat is located in Milan, Italy.

MEDREG wishes to thank in particular all the experts for their work in preparing the training and for sharing their knowledge.

For more information, visit www.medreg-regulators.org

If you have any queries relating to this paper, please contact:

MEDREG Secretariat

E-mail: vlenzi@medreg-regulators.org

EXECUTIVE SUMMARY

When energy actors discuss the move towards a low-carbon economy, digitalization is a word much used. The Northern Mediterranean countries are already experiencing a competitive and mature market structures, while Southern Mediterranean countries are progressively opening their markets, oftentimes through technologically advanced moves that allow them to cut a few steps of the process.

In both cases, consumer expectations with respect to what the energy market can do for them are growing. This is leading utilities and regulators alike to embrace and support new digitally enabled business models, where consumer is at the core of the market. This shift brings with it several interesting developments. On one side, data exchange is growing and becoming more complex, thus requiring stronger central market facilitation tools. On the other side, the increased need to use data to manage energy markets entails that an effective market infrastructure is even more necessary to enable efficient operations by market participants.

This training that formed the base of this report had the scope of introducing MEDREG members to the challenges that digitalization is going to bring to the drafting of regulations for this new technological era. The training worked around four main aspects: flexibility, open data platforms, usage of these data and cybersecurity, and the growing role of consumers.

Under flexibility, the training discussed how the development of local trading platforms or alternative models of procurement serve to purchase flexibility, which can play a significant role in balancing the network and system. The training explored the opportunities for distributors to use market-based procurement for flexibility services, considering when a marketplace can be efficient and discussing how flexibility helps network tariffs sending the right signals to network users.

Concerning open data platforms and privacy, the training discussed how operators and regulators should evaluate the quality of network data and data from distributed energy sources connected to the grid. The speakers also discussed the importance of ensuring that relevant network data is easily available to present to market participants, thus allowing the interoperability of data management. Trainers also looked at how regulators can ensure that data are used to improve the efficiency of distributors' investments, operations, and planning.

As for data usage and cybersecurity, which are indeed aspects that go far beyond the energy market, speakers clarified the importance of fully assessing the risks related to data control and usage, especially when it involves an extensive number of consumers. As energy markets become more complex and reliant on it, the speakers highlighted why it is key that data is not managed by a single, all-powerful entity but rather that information exchange and knowledge be shared in an open, transparent, and non-discriminatory market to support utilities in solving their problems effectively.

Security and quality of supply are important for consumers. To pair them with the benefit of digitalization, speakers analyzed whether digitalization could propose viable business models that reduce costs and increase the transparency of energy consumption and the consumers' awareness of their environmental footprint. Key aspects that can open to consumer the benefits of digital services were discussed, namely smart meter roll-out and cost-reflective and market-based, transparent price signals.

TABLE OF CONTENT

EXECUTIVE SUMMARY 3

INTRODUCTION 6

OBJECTIVES AND CONTENTS OF THE DOCUMENT 7

PRESENTATIONS 8

2.1. Introductory Remarks by Mr. Stefano Besseghini 9

2.2. Submarine Optical Cable Systems: Key Enablers and Critical Infrastructure for the Global Digitalization Transformation by Mr. Giuseppe Valentino 10

2.3. Smart Meters and Flexibility of Services in Digitalized Markets: Impact on Regulated Tariffs and Network Operations by Ms. Arina Anisie 12

2.4. The Impact of Digitalization on Network Codes: A DSO Perspective by Mr. Özge Özden 14

2.5. Digitalization of Energy Markets: Challenges and Opportunities by Mr. Igor Telebak 15

2.6. Cybersecurity in Energy Markets: Challenges and Opportunities by Mr. Roman Picard 17

2.7. Energy Cybersecurity: Indicators and Tools for Operators, Suppliers, Prosumers, and Regulators by Ms. Giovanna Dondossola 19

2.8. Exchange of Data Among Operators (TSOs and DSOs): The Monitoring Role of Regulators by Mr. Manuel Sanchez 20

2.9. The Cybersecurity Act and Cybersecurity Certification for the Energy Sector by Ms. Renate Verheijen 22

2.10. The Role of Consumers/Prosumers and the Evolution of Quality of Service: A New Business Model by Mr. Juan Ortiz Noval 24

2.11. What is the Role for Energy Regulators in Cybersecurity: Approaches and Critical Points by Ms. Elena Ragazzi 26

Conclusions 27

LIST OF FIGURES

Figure 1. Bandwidth Users Throughout The Years 11
Figure 2. Thirty Key Innovations that will Help in the Integration of Solar and Wind Power 12
Figure 3. Benefits of the Digitalization of the Energy Sector 14
Figure 4. Schematic Representing the Management of Future Smart Grids 15
Figure 5. Benefits of Digitalization in the Different Sectors 16
Figure 6. Risk Treatment Plan Concept 18
Figure 7. The Building Blocks for Access to Data 21
Figure 8. Benefits of Digital Meters at the Consumers' Houses 25
Figure 9. EPRI's Security Metrics 26

LIST OF TABLES

Annex 1. List of Abbreviations 27

1
INTRODUCTION

In the wake of the development that is currently being witnessed worldwide in the energy sector, digitalization and cybersecurity are important cornerstones on which to base future investments. This document was developed with the aim of having a manual for the regulators who are interested in the topic and who are looking to enhance their grids and services. It contains a summary about the presented topics and discussions that took place during the MEDREG training titled "Regulatory Implications of the Digitalization of Energy Markets and the New Role of the Consumers", held in October 2021.
The online training was attended by more than 60 participants and was presented by 11 highly qualified trainers in the topic. The speakers were from a wide array of companies and regulators including the Italian Regulatory Authority for Energy Networks, and Environment (ARERA), the Energy Regulatory Agency of Montenegro (REGAGEN), Sparkle, the International Renewable Energy Agency (IRENA), the Turkish Electricity Distribution Services Association (ELDER), the French Energy Regulatory Authority (CRE), Energy System Research Italy (RSE), the European Union Agency for the Cooperation of Energy Regulators (ACER), the European Union Agency for Cybersecurity (ENISA), e-distribuzione, and the Research Institute on Sustainable Economic Growth (CNR-Ircres).

OBJECTIVES AND CONTENTS OF THE DOCUMENT

This document in its final version may be used as an informative document for issues concerning the digitalization of the energy sector and its pros and cons, along with the need for cybersecurity and an overview on how to develop efficient national strategies to achieve the aspired goals.

2
PRESENTATIONS

The online training took place on the 27th and the 28th of October 2021 and featured 10 sessions presented by multiple experts in the field of digitalization and cybersecurity. The event was moderated by Mr. Igor Telebak, chair of the Consumer Working Group (CUS WG), and was launched with introductory remarks on "the importance of digitalization and its future impacts" by Mr. Stefano Besseghini, President of ARERA. The following paragraphs present the highlights and important information that passed through the speakers' interventions.

2.1. Introductory Remarks by Mr. Stefano Besseghini (MEDREG Permanent Vice President, and President of ARERA)

Mr. Besseghini started the training by highlighting that cybersecurity has been a concern for the regulators for some time now and that digitalization of the society played an important role in the way that the current difficulties were faced, especially during the pandemic.

Digitalization is like electricity, if you bring the infrastructure needed to any place in the world, somebody will certainly benefit from it. Some of the users might also be able to identify new opportunities, services, and business models that have not yet been identified.

Digitalization cannot be achieved without mentioning infrastructure and services. The distribution infrastructure for the electricity grid and gas distribution networks is a familiar concept. But there is also the distribution of the infrastructure for communication in the Mediterranean area. The digital connection infrastructure is developed all around the area, but it is not equally distributed. An even development of infrastructure should be sought to make digitalization services available to all energy systems. As for the services, human capital is of paramount importance to deal with the opportunities and challenges of digitalization.

Aggregation of different types of services will be the next challenge that regulators will face. Digitalization services are key elements to maintain the cost of such aggregations at an acceptable level. Currently there is an energy crisis from the point of view of rising prices. The markets should be able to extract the maximum efficiency from the different sources that can enter them to deliver the services. Digitalization is an enabling factor to satisfy energy demand and maintain reasonable costs through the aggregation of different kind of services.

However, attention must be drawn to the other side of the coin: digitalization, which can help manage the complexity of the system will also entail potential risks concerning cyber security.

In the dawn of the era of artificial intelligence (AI), new action plans should be put in place to deliver better services. AI is a real opportunity as it is enabling further exploitation of the field of managing complex systems. Many technologies are prevented from entering abruptly the field of energy systems because of the management responsibility of the system and what it could entail. In the future, regulators' approach should be open to understand how to allow these technologies to enter the system.

Mr. Besseghini finished by highlighting that this training is important to develop a common understanding and approach among regulators and introduce this topic within the regulators' organization. He also hoped that the event will raise questions, as well as provide important information, to move the work forward and debate on the future of digitalization.

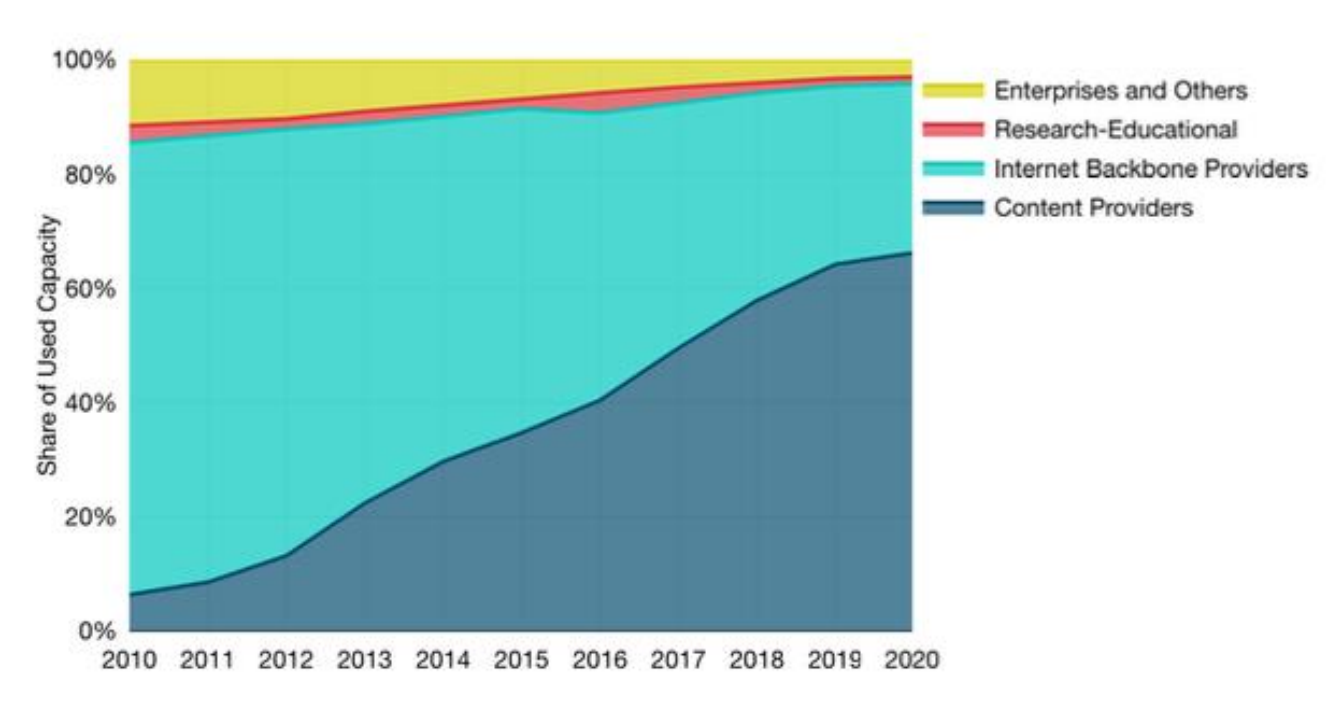
2.2. Submarine Optical Cable Systems: Key Enablers and Critical Infrastructure for the Global Digitalization Transformation by Mr. Giuseppe Valentino (Director, Backbone and Infrastructure Solutions, Sparkle)

Sparkle is the largest international service provider in Italy and 5th worldwide in internet backbone. Sparkle operates a state-of-the-art fiber backbone. Around 600,000 km of fiber optic cable infrastructure is managed by the company.

Rules for international fiber backbone within each cable ecosystem are very similar to the energy backbone for energy distribution and transport. The key network elements for a digital network are the national and local mobile networks and international long-distance backbones to interconnect data between large cloud sources. A submarine cable is a relatively small part of the manufactured components but has a very relevant set of rules in digital communication environment. These cables are connected to the rest of the networks and centers around the world. Digital applications are based on physical infrastructure. Although submarine cables do not have a big environmental impact, data centers are huge energy consumers and some of them which are currently being developed are increasingly relying on alternative ways of supplying energy to the centers. A new generation center has been built last year in Athens and some environmental measures were developed for this center.

The need and trend for connectivity is increasing every year and great work must be done to keep up with it especially with the decentralization of the energy and communication sector. The infrastructure to support these bandwidths needs to be upgraded and significantly developed on a continuous basis. The following graph shows the users of the bandwidth during the last years and their development. Ten years ago, internet backbone providers such as Sparkle were the main users of the backbone. Now the biggest users are content providers such as Google, Facebook, Amazon, and Microsoft, while backbone providers have diminished in size because the content providers have started owning and developing their own submarine and terrestrial assets as they have several millions of users. This means that what companies like Sparkle used to see as costumers, are increasingly becoming peers to the large internet service providers.

Figure 1. Bandwidth Users Throughout The Years



The lifespan of submarine cables is 20-25 years because it has electronic components that are submerged under water and become obsolete even in technology terms, so they must be changed and upgraded. The source of the digital communication is not always close to the place where it is consumed. Geography is a key element for the digital backbone. For example, the digital communication of this training is generated in servers in north of Europe and in the USA and is consumed in the Mediterranean basin.

In Africa, some projects are under development in the digital infrastructure world. For example, the project by Facebook which, when deployed, will be the longest single submarine cable system that will go around Africa. More specifically, North Africa, which is on the Mediterranean basin, is the most developed area in the continent. This is seen especially in the information and communication department.

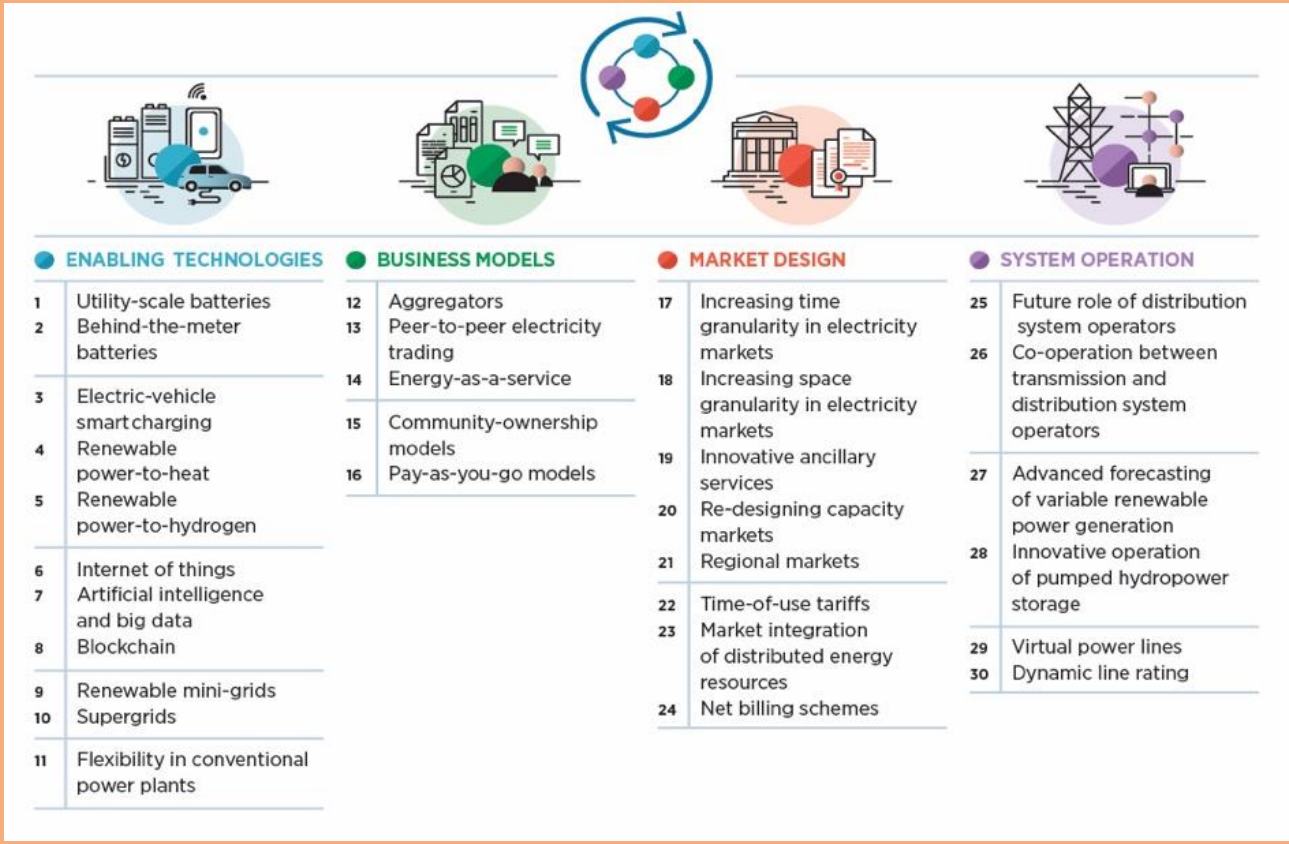
International Bandwidth Demand is doubling every two years. Telecom & Internet Companies are heavily investing in new submarine and terrestrial backbones. Wide opportunities exist for cooperation and synergy between telecom backbone and the energy infrastructure projects. Cooperation with the players in the energy transport already exists but can be improved both in terms of joint conception of the infrastructure, which can bring the most out of the digital and energy capabilities, and in terms of finding some synergies even with the institutional counterparts for the international backbones. The Mediterranean basin can be the ideal playground to test this enhanced cooperation especially with projects dealing with energy development.

2.3. Smart Meters and Flexibility of Services in Digitalized Markets: Impact on Regulated Tariffs and Network Operations by Ms. Arina Anisie (Associate Program Officer, IRENA)

As Renewable Energy Sources (RES) are unpredictable, more flexibility is needed in the energy systems. Flexibility is needed to integrate the large, forecasted volume of renewables by 2050. Multiple innovations to enable this exist such as:

- Enabling technologies (e.g., storage facilities, hydrogen, EVs, blockchain, etc…)
- Business models are included in the form of aggregators and energy as a service.
- Market design is important to encourage a more flexible behavior.
- System operators should adapt as the system becomes decentralized and digitalized.

Figure 2. Thirty Key Innovations that will Help in the Integration of Solar and Wind Power



Enabling technologies represent a new opportunity to operate the system which leads innovations in system operation. To monetize the value created, regulations should be designed which in turn will create new business cases that will help generating new revenue streams for technologies. This is called systemic innovation and the key message is that innovation is not implemented in isolation and innovative solution

for integration of RES comes from the synergies across all four dimensions. Thirty key innovations were identified to integrate RES in the systems. A report is available online for further information[1].

Three main innovation trends are being noticed, and they concern the electrification process such as:

- Electrification of end use sectors
- Decentralization in the form of the increasing deployment of RES which turns consumers into active participants
- Digitalization that enables faster response and better management of the assets.

New consumers can currently produce, store, trade energy and manage the load. This transforms the consumers into active participants. Several briefs on the available technologies are also available on IRENA's website[2] [3] [4].

Looking into technologies, three main pillars are identified and are: the internet of things (IoT), artificial intelligence (AI), and blockchain. IoT helps connect small smart devices to the internet, gathers data in real time, and helps creating smart homes. AI helps with decision making and can have new applications in the power system. Blockchain helps automate the transactions via smart contract and decreases transaction costs. Additional information can be found in documents developed by IRENA[5] [6] [7].

Tariffs are also key enablers for more flexibility. For example, time of use tariffs enable flexibility by sending price signals to consumers instead of flat tariffs. This enables the user to adjust his consumption time based on the time of use rates. Some of the key enabling factors of use of time tariffs are advanced metering infrastructure and digital technologies for automation. Different ways to implement time of use tariffs are available, for example the consumer can check the next day prices with15 mins intervals, while other systems where energy prices are not that volatile would benefit by only applying peak and off-peak pricing. Net billing is also a flexibility generator especially for prosumers as it helps charging or compensating the consumers for injecting electricity to the grid when prices are high and consuming when prices are low. This differs from net-metering by adding the dimension of the value of electricity at the time of injection or use.

---

[1] https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Feb/IRENA_Innovation_Landscape_2019_report.pdf

[2] https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Sep/IRENA_BTM_Batteries_2019.pdf

[3] https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Sep/IRENA_Power-to-heat_2019.pdf?la=en&hash=524C1BFD59EC03FD44508F8D7CFB84CEC317A299#:~:text=Renewable%20power%2Dto%2Dheat%20refers,heat%20pumps%20or%20electric%20boilers).

[4] https://irena.org/-/media/Files/IRENA/Agency/Publication/2019/Sep/IRENA_EV_smart_charging_2019.pdf?la=en&hash=E77FAB7422226D29931E8469698C709EFC13EDB2

[5] https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Sep/IRENA_AI_Big_Data_2019.pdf

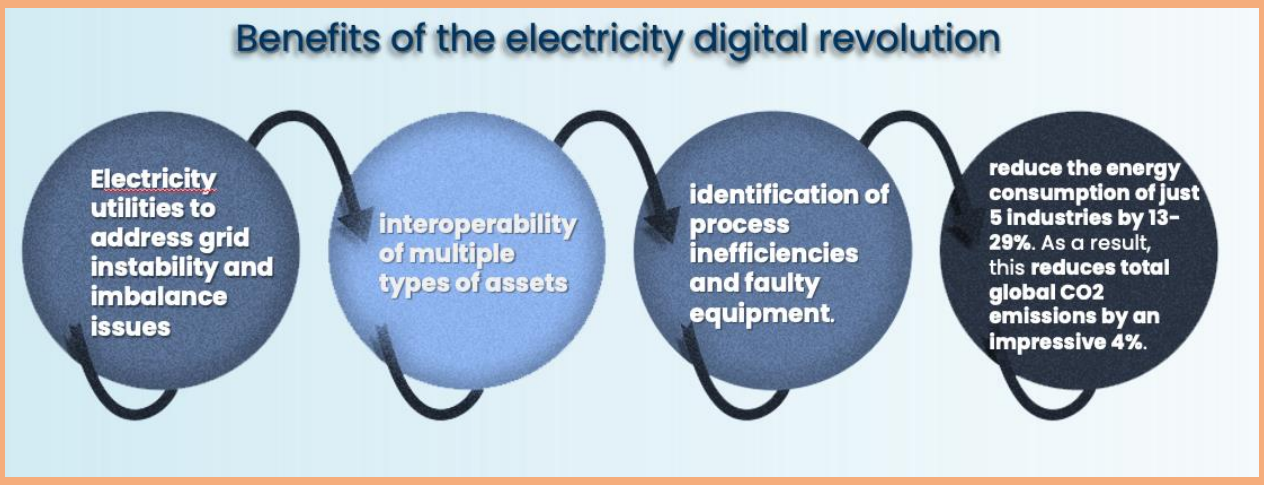
[6] https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Feb/IRENA_Landscape_Blockchain_2019.pdf?la=en%26hash=1BBD2B93837B2B7BF0BAF7A14213B110D457B392

[7] https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Sep/IRENA_Internet_of_Things_2019.pdf

2.4. The Impact of Digitalization on Network Codes: A DSO Perspective by Mr. Özge Özden (Secretary General, ELDER)

Network codes are generally defined for TSOs, but as the whole system is transforming, standards must be set to give everyone a common definition of the various components of the system. A timetable must be developed to perform actions in a previously set order to balance the system in the same way in the different countries. DSOs must apply the same codes everywhere and they must make some changes to the codes to connect EVs to the grid. Monitoring the system also requires defining standards and procedures so when any kind of problem arises, they can be solved. Operational disruptions can be managed with some automated systems and people's expertise. In the last decade the energy development sped up as the prices of the technologies decreased and can now be implemented more widely.
Decarbonization, sustainable development, and digitalization are of extreme importance. To minimize the environmental effect, curtailment and losses should be decreased and efficiency should be increased. To decarbonize the system, RES must be connected to the grid with alternative fuels and nuclear energy. For sustainable development, energy efficiency is needed to increase flexibility and eco-mobility. Digitalization is key to support all these things, and can be achieved through the IoT, blockchain, and virtualized power plants. These benefit the power system as they help reduce operation and maintenance expenses, improve power plant and network efficiency, reduce planned outages and downtime, optimize dynamic pricing for consumers, and extend operational lifetime of assets.

Figure 3. Benefits of the Digitalization of the Energy Sector



Benefits of the electricity digital revolution can be seen in Figure 3. On DSO levels, inefficiencies can be detected through the acquired data of multiple parameters and help understand the faults without physical presence. Energy consumption can be reduced by 13 to 29% of the total consumption in certain industries. This is a costly process, and to achieve it, DSOs must include the government and the public in this approach.

DSOs are going to balance the system and create price signals for participants to the market at DSO level. By doing this, the security and quality of supply will be enhanced. Social welfare for the society can also be created by providing a higher quality of service for lower prices.

Figure 4. Schematic Representing the Management of Future Smart Grids

Multiple types of small-scale distributed electricity are emerging and there is a need to develop standards to connect them to the system. Storage is the tool that will provide power system flexibility. The implementation of smart charging of EVs is important as in some markets they are already presenting a huge load. According to some research an additional flexibility of 67 TWh can be created by demand response and storage technologies. To do this, the network codes should be set for all market players operating in different countries.

2.5. Digitalization of Energy Markets: Challenges and Opportunities by Mr. Igor Telebak (CUS WG Chair, and Economic Analyst, REGAGEN)

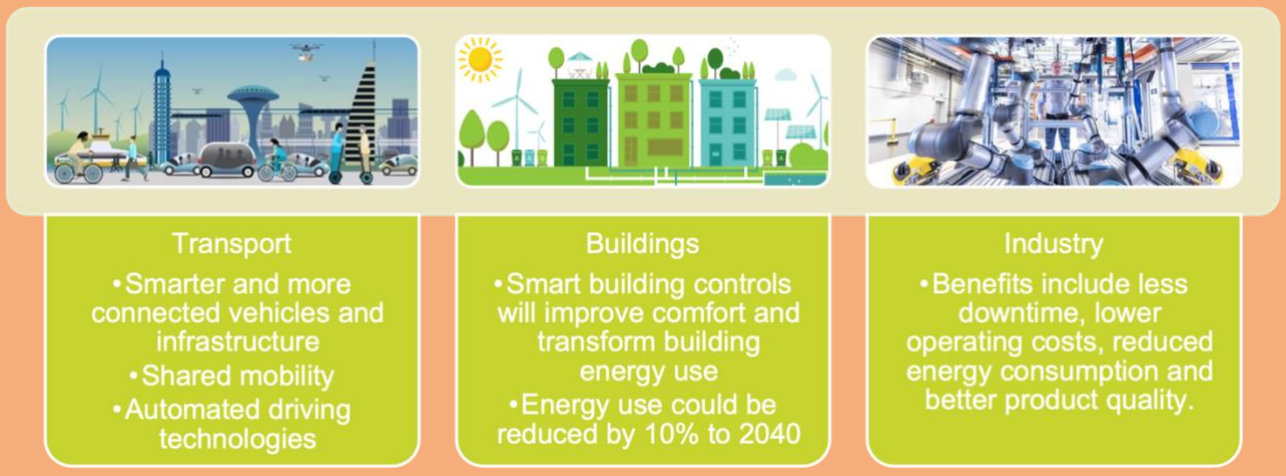
Digitalization describes the growing application of information communications technology (ICT) across the economy including the energy sector. The digital world has 3 fundamental elements: data, analytics, and connectivity. The energy sector has undergone many changes in the previous years. Data has become one of the world's most available resources. Around 90% of the data in the world was created during the last 2 years. Global annual internet traffic surpassed the exabyte threshold in 2001 and is supposed to pass 4.2

zettabytes in 2022. Advanced analytics like AI and automation are needed to analyze this huge amount of data.

On the demand side, for example, digitalization will lead to smarter and more connected vehicles and infrastructure that collect and analyze large volume of data. Automated driving technologies are widely deployed in the railway business, primarily on direct transit as well as in aviation. Buildings currently account for nearly one-third of global final energy consumption, 55% of global electricity demand, and 60% of total growth in electricity consumption. Digitalization will tackle the largest potential of savings in heating, cooling, and lighting which represent 60% of the energy demand in buildings. Industry is well versed in digitalization, and can further benefit from less downtime, lower OPEX, and better products quality.

On the supply side, digitalization affects the oil and gas, coal, and power sectors. The role of renewable energy (RE) is expanding which is closely related with digitalization that enhances the possibility of integrating renewables in the systems.

Figure 5. Benefits of Digitalization in the Different Sectors



Digitalization in the power sector consists of two branches: data and analytics, and connectivity. Data analytics provide reduced operation and maintenance (O&M) costs, improve efficiencies within the system, reduce unplanned outages, and extend assets lifetime.

Traditionally, electricity is generated in power plants, transferred through networks, and delivered to users in the residential, commercial, industrial and transport sectors. This model will be changed dramatically by digitalization, by matching demand to the need of the system in real time. The four main elements of transformation of electricity system are:

- Smart demand response
- Integration of variable RES
- Implementation of smart charging for EVs
- Emergence of small-scale DERs such as household solar Photovoltaic (PV).

Even though digitalization brings many benefits, it also brings challenges and risks to all players in the energy market. Risks can come both from natural hazards such as geomagnetic storms and cyberattacks. Governments and companies need to work together to mitigate these threats. Full protection is impossible, but the effects of the threats can be limited if the stakeholders are well prepared. Privacy is also affected by digitalization because of the ownership of the data topic. The big question is how much data the consumers are willing to share with the providers and how good will the confidentiality of information be protected.

In MEDREG Consumer Working Group a report is currently being developed on the "Role of Digitalization and its Impact on Consumer Issues". The report will begin with digital communication at regulator, DSO, and supplier levels. Then smart meters and distributed electricity generation are discussed and at the end, the report tackles cybersecurity. Smart meters are a fundamental piece of the smart grid. Many countries already have a high share of smart meters deployed especially in the northern shore of the Mediterranean. The report tried to have an outlook on the national strategies or policies related to the security of network information system and if they cover the energy sector. In conclusion, twelve countries have national strategies related to security of networks of which ten include the energy sector.

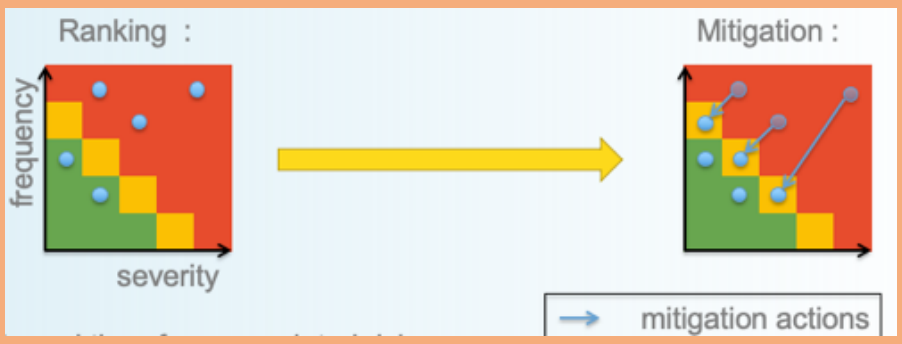
2.6. Cybersecurity in Energy Markets: Challenges and Opportunities by Mr. Roman Picard (Analyst, CRE)

System operators know how to protect the grid from usual threats such as works, falling trees, lightnings, etc. but with the cyber world the threats are changing with new components being introduced to the networks. The level of cybersecurity in an interconnected energy network is lower than the level of the weakest operator in this interconnection. Introducing highly interconnected technologies and services that involve new interfaces also present risks.

Among the challenges is the outsourcing of infrastructure and services. In this case, the operator should check if the outsourced entity is as efficient as the initial entity in cyber security. Another challenge is the integrity of components used in energy systems, some material can be originally corrupted, and the operator must be aware and try to have a first check before including them in the system. The increased interdependency among market stakeholders is another question where consumers consume plenty, and the providers supply the needed energy without a problem. If RE was to provide the needed energy, consumption should be able to adapt to the production. If this is not achieved, the balance of the network will be lost.

To reach the required cybersecurity level, a risk treatment plan should be developed. It starts with an impact analysis by identifying threats and their associated risks and assess the frequency and severity of these occurrences. The lower the severity and frequency the better the system is. The risks that are beyond the limit of non-acceptability should be mitigated to let them at least reach the acceptable zone.

Figure 6. Risk Treatment Plan Concept



The actions to meet the new challenges are mainly four types of priorities. First, an effective threat and risk management system should be set-up by identifying the operators of essential services for the energy sector, completing a risk analysis and treatment, defining the framework of rules for a regional cooperation, and developing trust between stakeholders. A framework for vulnerability disclosure for the energy sector is also needed to provide classification methodology for risks. The objective of the first part is completing the inventory.

Then an effective cyber response framework and coordination should be defined and implemented. Furthermore, the regional cooperation for emergency handling should be implemented and strengthened. The aim of this part is to respond to attacks and emergencies.

The third part calls for the continuous improvement of cyber resilience by establishing a cyber security maturity framework for energy through the development of network codes on cybersecurity, establishing a contractual Public Private Partnership (cPPP) for supply chain integrity, and fostering international collaboration by having forums with member states, regulatory authority, and all related stakeholders. The last part consists of building-up the required capacity and competences as human resources are scarce.

In France, in 2012, a cybersecurity rule for smart metering was created. Currently there are around 30 million smart meters in France. This entailed the need for cybersecurity as there were no general rules at national or European levels yet. After the European rule was created, France is updating its own rule for smart metering to make its implementation easier.

CRE is actively involved in the European work through the Council of European Energy Regulators (CEER) by participating in multiple groups working on cybersecurity, and privacy and security, and in the cybersecurity work stream of CEER that brings information to French stakeholders to be aware of all the developments in the regulations. Three main points are currently evolving in European regulations. The first is the cybersecurity network code for electricity. The second is the Network and Information Security directive (NIS) V2 on cybersecurity, and the third is the Resilience of Critical Entities directive (CER) on the resilience of critical entities and focus on cybersecurity protection against terrorism.

The national information systems security agency (ANSSI) oversees the cybersecurity aspect. For smart metering it is important to make sure that the functionalities requested from the DSO/TSO are cybersecurity

compatible. For example, in one instance, CRE asked for a function from the operator to be added to the meter, but the operator requested not to include it to stay cybersecure. CRE checked his claim with ANSSI who verified it, then they changed the item in the order, and they asked for another functionality that is cybersecurity friendly.

In cybersecurity, CRE deals with ANSSI which is not an independent regulator but part of the governmental institutions. Hence, CRE is not as free as when it is dealing with other regulators.

2.7. Energy Cybersecurity: Indicators and Tools for Operators, Suppliers, Prosumers, and Regulators by Ms. Giovanna Dondossola (ICT and Cybersecurity Leading Scientist, RSE)

RSE is a research company headquartered in Milan and 100% controlled by the Italian Energy Services Manager entity (GSE). In cybersecurity, RSE carries out activities related to the lifecycle development of cybersecurity such as specification of requirements, assessment of the architecture, modeling, simulation, and experimental activities. Different types of technologies are targeted such as the convergence of Information Technology (IT), Operational Technology (OT related to the devices in the field), and IoT technologies. The experimental activities are performed in three different labs. The first lab is the Power Control Systems lab that deals with cybersecurity in operational environment, the second is for IoT and Big Data targeting open platforms and new applications based on the new types of architecture, the third are two energy test facilities to demonstrate cybersecurity measures and to validate their capabilities in the field. RSE also supports ministries and regulators by performing vocational trainings for industries along with national and European universities.

The cybersecurity act regulation[8] is related to the certification schemes linked to ICT products, services, and processes. Ties exist with the NIS directive because there is a need to certify the maturity level of the organizations and the security level of products in the infrastructure. Certification schemes related to cloud services, industrial automation and control systems, IoT devices, and 5G. are under development.

The cross-border cyber risk assessment is related to the use of qualitative and quantitative criteria to measure risk treatment using cyber–Risk Impact Matrix (RIM). Risk impact must be measured not only with loss of generation and consumption as done typically in the energy field, but also by introducing the impact related to unauthorized access to the infrastructure and modification or unavailability of information and unauthorized access and simultaneous control over many of the same IoT devices, and exploitation of serious vulnerabilities in the system. Typical standards that support the identification of minimal security requirements also exist. These standards include organizational standards, technical standards, and standards dealing with the process towards compliance. Minimum security requirements focus on the essential business processes, so it is important to start by identifying these processes, then identifying the associated risks to map the risks with the security controls to mitigate them.

[8] https://eur-lex.europa.eu/eli/reg/2019/881/oj

Many tools help in specifying the security requirements such as NISTIR 7628. It can be used to design a component view of the architecture where you define the different interfaces of the components, and with a specified methodology, you can associate to each interface a set of security requirements from the standards. Another tool is CSET designed in the USA, in this one, more details are available to evaluate the compliance to standards. CSET allows to perform architectural analysis to identify the asset categories and the criticality level of each security domain and the applied security controls. From these inputs, the architectural analysis develops the network warnings, improvements in network segregations, the number of controls and measures that need to be included in the asset categories as well as the percentage of compliance within the control categories.

When analysing attacks modeling, tools that are based on probabilistic analysis and that apply AI algorithms can model architecture attack graphs and derive indicators. For example, the time taken by attackers to compromise one of the vulnerable components in the network can be modeled. Attack graphs also include analytics to exploit the variability of data and to estimate the evolution of the attacks.

Resilience is the capability to include cybersecurity functionalities within the infrastructures to study how to react to an anomaly to guarantee the functionality of control systems and the security of supply. There are two steps of recovery in case of incidents, one is based on ICT recovery and the other is adaptive control. Anomaly detection platforms are being developed to collect observations and events from different components and spot the attacks early on.

The EV charging infrastructure involves different kinds of actors. Cybersecurity must be included in the charging infrastructure as well as in the back-hand systems that use the data and must communicate with the system, hence there is a need to guarantee the level of security and interoperability for this type of applications. This makes the chain of trust much more extended as it involves different providers and platforms. Therefore, the whole chain of information should be able to guarantee the level of security and privacy that is required. The chain of trust means that all the links of the chain must be secured and interoperable.

2.8. Exchange of Data Among Operators (TSOs and DSOs): The Monitoring Role of Regulators by Mr. Manuel Sanchez (Former Team Leader for Smart Grids at the European Commission, ENER)

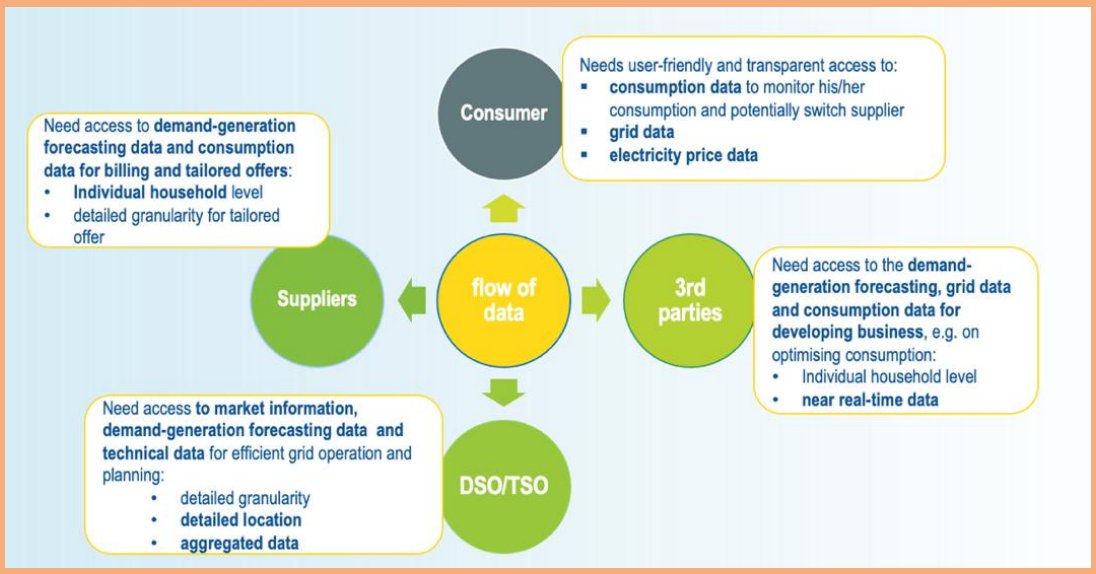
Active consumers and energy communities are new actors that have been introduced in the market design. They have the right to have smart meters even in member states where smart meters are not mandatory. Empowering the participation of the active consumer in the energy transition is essential because if they do not participate, energy transition will never be fully accomplished. DSOs and TSOs should enhance their collaboration to give added value to the flexibility of the system. This will help in congestion management and integration of renewable energies, etc. Data is necessary to empower the consumer and is key for the energy transition. In the new electricity market design, there is an emphasis on the empowerment of the consumer. This empowerment is achieved by the regulations for consumers in the electricity markets where

they are engaged in consumer choices, where different topologies are being implemented in multiple member states producing new business opportunities. The empowerment is also achieved by the right of consumer in the choice of technologies such as the dynamic pricing right, smart meter right, self-generation right, storage right, and demand-response right.

Article 23[9] of the electricity directive established what are the data management responsibilities. Member states should organize the management of the data. In some countries it could be centralized, and the TSO or DSO could take responsibility of data management, in others it could be decentralized, and another entity takes the responsibility.

Data is defined in the electricity directive as covering consumption data, switching supply data, data necessary for demand response schemes, and services data. It is proposed that the commission should develop secondary legislation and implementing acts and technical law on interoperability and harmonization of access to data.

Figure 7. The Building Blocks for Access to Data



There are many available programs for data sharing that are already running and under use. There are also demand side flexibility commercial platform, and some of them are already in use, and not only being developed, such as: Enera, Gopacs, Nodes, and Piclo.

Market flexibility is something that is introduced in the electricity market design. Some countries have developed this flexibility market and it is linked with the digitalization of the sector. This market has 2 sides:

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0944

vendors, and buyers. In the picture below,10 these sectors can be seen divided to the left and to the right, and each actor is linked to the service that they provide/need.

The European Commission is currently preparing a Digitalisation of Energy action plan to address all these points. The action plan, planned for publication in June 2022, will be one of the key initiatives to accelerate the implementation of digital technologies in the energy system, as highlighted in the EU energy system integration strategy.

Looking ahead towards a secure, competitive, and cleaner European energy market, the implementation of the CEP (Clean Energy Package) calls for accompanying actions to develop and implement access to data, flexibility markets, interoperability, cybersecurity, and synergies with other sectors. Investments on new data processing infrastructures which guarantee cost-effective investments and add value to grid operators and system users are also required. Additionally, in an increasingly digitalized world, research and innovation on power electronic technologies and emerging disruptive technologies to overcome physical restrictions and further integrate distributed energy resources is of exceptional importance. Finally, it is crucial to update and train human resources as well as creating new "digital" skills at all levels.

2.9. The Cybersecurity Act and Cybersecurity Certification for the Energy Sector by Ms. Renate Verheijen (European Union Legal Officer Cybersecurity Certification Framework, ENISA)

Cybersecurity certification is a mechanism that helps to build an ecosystem ensured by continuous improvements and checks. It also helps to demonstrate that taken measures are really taken and if they are effective. it is a tool to demonstrate the ability to adhere to requirements contributing to cybersecurity resilience.

Certification should be transparent and useable in the entire sector and ecosystem of energy exchange. Objectives can be translated through the certification mechanisms. Certification is also important for companies that procure products because they can guarantee a certain level of quality through this certification as certification bodies and testing laboratories check the quality of the product and monitors if any changes occur in the environment of the service or product. It builds trust as it demonstrates that the requirements are met. A complaint and penalty system supports this scheme to check the licenses in case there are any doubts concerning their authenticity. Certification also contributes to a more sustainable society with robust cybersecurity systems that users of energy can rely on, and where businesses can feel secure about their data privacy. The complete system of certifications ensures that there is a continuous improvement cycle of the product.

When creating a framework, it is important to identify in what areas cybersecurity certifications are needed, what areas are important, and what are the principles to be highlighted. The commission and the member

[10] European Smart Grids Task Force - EG3_Final_report_demand_side_flexiblity_2019.04.15.pdf **(europa.eu)**

states are looking to define areas for schemes, then they include products and services in these schemes. Afterwards member states represent it in the European cybersecurity certification group. The stakeholders form another group, then both groups present their opinions on the program, and they approve together the future program of schemes. Then the commission makes a final draft and launches it to be seen by all member states and stakeholders.

Schemes should allow international cooperation and mutual recognition. To do that, it is important for all countries to be able to exchange and create cross-border cooperative activities. The use of standards makes it easy for other countries to follow the same path for security requirements. Certifications need to be integrated into each other and to fit like a puzzle. If you have a certified component that you want to use in another product that you also aim at certifying, you should have the advantage of already having a certified component. Certified products are the building blocks as they can be reused and should complete each other and not overlap. The product should be certified based on its intended use. Using a product in a critical part of the energy sector is totally different than using a product in the supermarket. Hence, the risks in the environment need to be considered to adjust the level of security requirements.

Market demand leads to the inclusion of products and services in the cybersecurity scheme as it clarifies the needed measures to enhance cybersecurity. Additionally, country laws and policies also have a big influence in the inclusion of these products and services in the schemes and an important example of this is the energy sector. The threat landscape also imposes the inclusion of other components. A future program might have a specific scheme for a certain sector, or technological schemes, and horizontal schemes that are designed for all products and processes. Once the areas of the schemes are available, they should be able to detect, prevent, and respond to incidences.

The commission is assisted by the stakeholders to develop the Union Rolling Work Program (URWP) who advises on strategic matters, on the design, and the update of the program. Member states ensure that there is a consistent implementation of the URWP. All stakeholders of the ecosystem play an important role in ensuring that the URWP is endorsed by all parties based on the commonly developed ideas. ENISA is then obliged by the cybersecurity act to design schemes upon request of the commission. ENISA designs and evaluates the schemes in parallel with the commission to see if they are operating well.

For checks and balances, the commission and the member states can ask for a review of schemes to allow the scheme to be revised and update it to be consistent with the new ones. Changing one scheme should be coherent with other schemes that are under development or being used in the system and it can include new areas in the program. all stakeholders are involved in the way schemes are supposed to work in their environment. Collaboration plays a crucial role for cybersecurity and energy. Once a scheme is published, it will not be a static scheme, but it will be able to adjust and respond to the ecosystem that it is operating in.

The first cybersecurity scheme took a long time to build but then the following schemes were developed in shorter time periods as they are like building blocks that are used to build and refine cybersecurity certifications. The effectiveness of these schemes will increase with their development. Cybersecurity frameworks are built neutral so all kind of sectors can use these general elements in their specific settings.

2.10. The Role of Consumers/Prosumers and the Evolution of Quality of Service: A New Business Model by Mr. Juan Ortiz Noval (Head of Network Development, E-Distribuzione)

The electric system is changing from the traditional power systems where tools were well defined from generation to consumption, to a more distributed model with different emerging stakeholders, in particular prosumers. The effective participation of the customers to the electrical energy system is the key to energy transition.

Grid Futurability is an initiative fostered to improve resilience of network and improve security of supply to mitigate extreme weather events. While working on a holistic approach through all the value chain, sustainability is important to integrate RES while working for an overall 0-emission network.

Flexible grids are important to be able to support the increasing demands of prosumers. A lot of investments are moving towards distribution networks, and it is important to optimize them. With flexibility it is possible to manage congestions, regulate voltage levels, and support operators in case of faults and in case of restoration support. Regulatory experiments are very important to put in practice all these technologies.

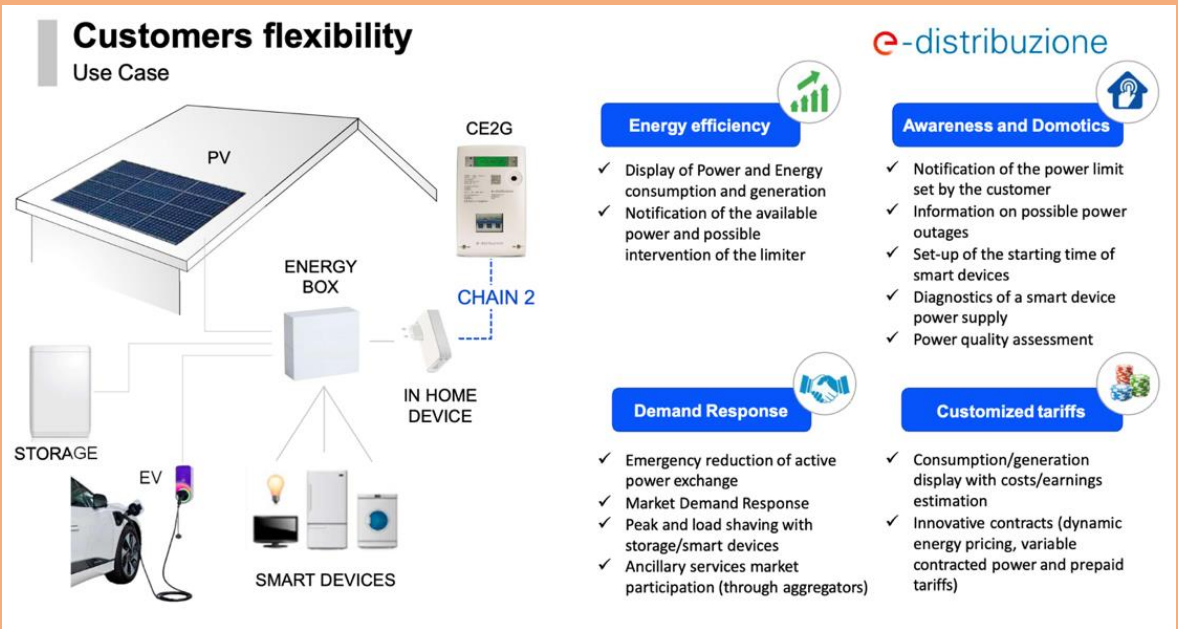
Flexibility is usually linked to generation. However, this is not the only kind of flexibility that the network will host in the coming future. Currently e-Distribuzione is connecting its secondary substations with fiber optics because they need to have the real pulse of the network second by second. This will help monitor all the distributed energy; information sharing is crucial. Monitoring is key in all parts of the grid to achieve the wanted flexibility for network control.

Advanced automatization techniques like the Smart Fault Selection can help isolating a faulty section of medium voltage lines in less than 1 second. Using these high-speed communication channels, information can be interchanged between network devices in real time to take the relevant measures. Thus, customers who will be affected by the faults will be minimalized to the ones that are directly affected by the faulty section. Other automatization techniques such as the Self-Healing Automatization is currently under development which is capable of intercepting almost all faults on Medium Voltage (MV) lines. The standard topology used to define the MV network will become flexible and will depend on the operating conditions.

The digital meter will be the prime enabler for the customer participation. It will provide open protocols to allow customers and third parties to access meter information. The meter will provide historic information of the customer as well as power limitations on the contract. The open meter can also contribute to advanced network management technics like peak identification or help network modeling technicians. The meter should interact with home energy boxes that will control the overall energy consumption of the houses.

Typical consumers that have a PV system on their homes with a digital meter connected to the energy boxes of these houses, will have the information collected by the meter momentarily transmitted to them. This meter will help these consumers improve their energy efficiency and will enhance their awareness as well as allowing them to participate in the demand response market and to access the customized dynamic tariffs.

Figure 8. Benefits of Digital Meters at the Consumers' Houses



The energy environment is changing rapidly and there are a lot of points like the following ones that remain open to discussion:

- Develop a precise definition of ancillary services;
- The cost benefit analysis between flexibility and network development;
- For the flexibility market, the platform that integrates all the market information is not standardized and some tests are being organized with commercial platforms;
- The coordination between DSOs and TSOs should be defined; and
- The biggest issue is the distributed energy resources engagement, as to engage these resources clear criteria should be defined for flexibility regulation.

Energy divide must be avoided between customers that have access to flexibility services and that may participate to them and understand how to do so, and the customers who can't. Regulatory frameworks are very important to overcome this hurdle.

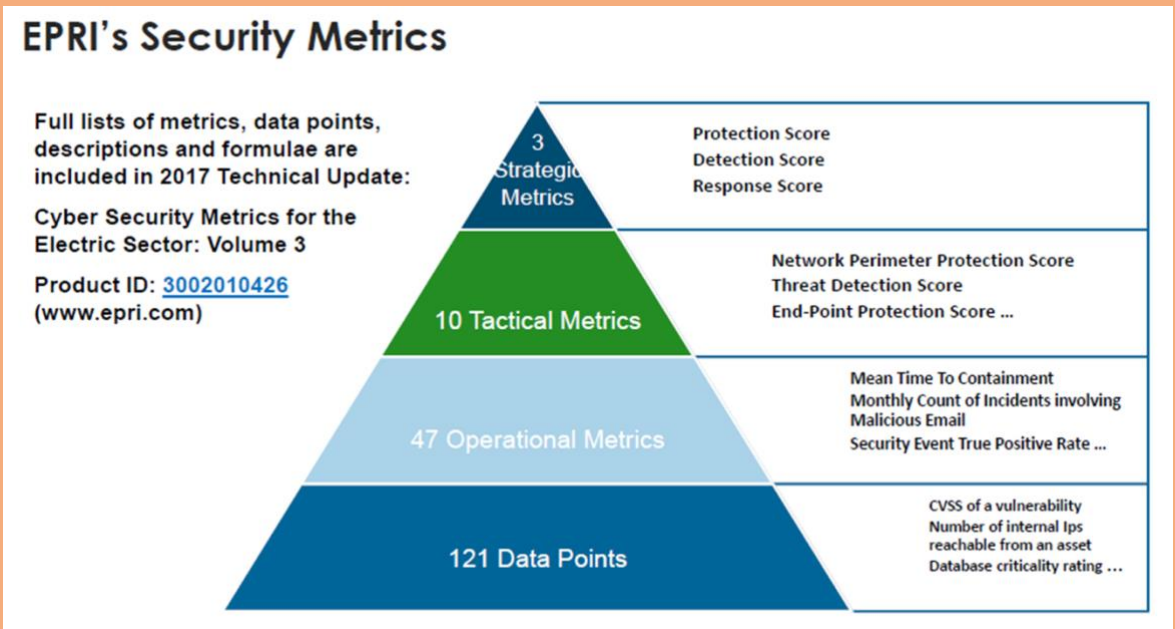
2.11. What is the Role for Energy Regulators in Cybersecurity: Approaches and Critical Points by Ms. Elena Ragazzi (Research Director, CNR-Ircres)

Regulators must make sure that the investments done are reasonable and are going in the right direction, and that they are prudent and effective, producing what they are intended for.

In performance-based regulation, the regulator wants to provide operators with economic signals to enhance the quality of service. They must define Quality of Service metrics, and in the case of cybersecurity this includes protection from cyber threats. Regulators must also fix the level of baselines objectives, the reward offered if the operators reach the objectives, and further options to consider the developments of the field. Here, companies and operators should choose how to reach the cybersecurity objectives given the system of incentives given by the regulator. The regulator will only check if the objective has been reached and not the cybersecurity measures that were taken. It is fundamental for the regulators to identify good indicators and baseline levels and fix procedures of calculation of these indicators. Regulators are supposed to acquire data and verify if this data was calculated correctly.

In cost plus regulation (Compliance regulation), the regulator decides what are the priorities and how they will be translated in countermeasures, and the company must comply with this list of countermeasures. The companies will be rewarded by the coverage of all expenses incurred with remuneration. Here, performance metrics are not regulatory tools but help to understand the effectiveness of the regulation and how to evolve them. The regulators should identify benchmarks, approve countermeasures, and cover the cost for the company. The firm must comply with the chosen strategy.

Figure 9. EPRI's Security Metrics



In most cases operators are in a better position to understand how to prevent cyber threats and protect the system. This leads to a basic conclusion that it is better to go with performance-based regulation, but in cybersecurity, performance metrics are in their early stages of development, and therefore difficult to implement in regulation.

A third possible way is to start working in collaborative approaches between the stakeholders. Such an approach is fulfilled by setting a meeting between the regulators and the companies to discuss the elements to be included in the regulation. Although it is a long process, it is an effective one.

There is no single best practice for all countries because it depends on the characteristics, values, and laws of the country, but there is a list of steps in the regulation that should not be skipped for the regulation to work well. This depends on the road to be followed if it is cost plus regulation or performance-based regulation.

In Performance Based regulations, the following steps should be followed:

1- Define a cybersecurity strategy for the power system;
2- Define objectives coherent with this strategy that must be clear-cut, measurable, and reasonable;
3- Define indicators and targets to be reached;
4- Define procedures to calculate the indicators (regulatory guidance for recording CS events);
5- Perform controls and inspections on the way indicators are calculated (audit in fields and sanctions);
6- Schedule a constant update of steps 3 and 4, based on experts, feedback by companies, and the regulator's experience. The problem with the incentive philosophy is that they must be constantly fine-tuned with the evolution of the context.

In Cost Plus regulations, the following steps should be followed:

1- Define a cybersecurity strategy for the power system;
2- Define the countermeasures coherent with this strategy by requiring compliance to a standard, or defining a list of required/suggested countermeasures, or by agreeing on a list of countermeasures with the operators;
3- Define the regulation for the expenses connected to these countermeasures (e.g. coverage of all compliance costs, fines if minimum requirements are not reached, funding if further countermeasures were adopted…);
4- Define accountability procedures. If the cybersecurity stance is one important goal of the policymaker, the related expenses must be clearly identifiable in investment plans;
5- Verify ex-post the compliance of performed activities and of expenses to the plan. Make sure there are skilled people to accomplish these activities;

Schedule a constant update of step 2, based on experts, feedback by companies, and the regulator's experience. The problem with the compliance philosophy is that it is not reactive to environment and it may give a false sense of security.

3
Conclusions

Digitalization is an important service, all people will benefit from it while some might even identify new opportunities, services, and business models that have not been recognized yet.

Traditionally, the energy grid consisted of generating the electricity in large power plants, then transmitting and distributing it to the end users. This model will be changed dramatically by digitalization, which will lead to advances in matching demand to the need of the system in real time. Having said that, the digital world is based on a physical infrastructure that should be updated and developed regularly as the trend for connectivity is increasing yearly.

Flexible systems are needed to achieve the integration of the quantity of renewables aimed for by 2050. There are lots of innovations to enable this in the fields of technologies, business models, market design, and system operation. Hence, innovative solutions to integrate RES lie in the synergies across all dimensions. DSOs and TSOs should enhance their collaboration to give added value to the flexibility of the system, and data is essential to accomplish this. Flexibility opens the opportunity for congestion management, voltage levels regulation, and many other services. Using high-speed communication channels, information can be interchanged between network devices in real time to take the relevant measures for the different services. Even though data is diverse, they should be interoperable so if one actor generates this data, other actors can understand its meaning.

Using big data and processing it in real time, is crucial for the management of the system. Emerging technologies such as IoT, AI, and Blockchain should be integrated in the energy system to act quickly, safely, cheaply, and efficiently on the network.

In a world that is increasingly interconnected, there are no frontiers to face cyber-attacks and the level of cybersecurity in an interconnected energy network is lower than the level of the weakest operator in this interconnection. To reach the required cybersecurity level, a risk treatment plan should be developed to mitigate risks that are considered non-acceptable.

The impact related to unauthorized access to the infrastructure and control of several devices leading to the exploitation of serious vulnerabilities in the system should be included in the risk impact analysis. The risk impact analysis should not only be quantified with the conventional metrics for the loss of generation and consumption.

There are two main ways to develop regulations: Performance Based regulations where operators choose the measures to reach the cybersecurity objectives and the regulator only monitors if the objective was reached, and Cost-Plus regulations where the regulator defines what are its priorities and how they will be met, and the operator must comply with the list of provided countermeasures. In both cases there is a set of steps that should be strictly followed to reach the objective. In most cases operators are in a better position to understand how to prevent cyber threats and protect the system. A third possible way is to start working in collaborative approaches between the stakeholders. In cybersecurity, it is important to work on enrichment of competencies of employees and to upgrade procedures and processes as the field is still in its early stages.

Certification should be transparent and useable in the entire sector and ecosystem of energy exchange. It builds trust as it demonstrates that the requirements are met. Certification schemes should allow international cooperation and mutual recognition. Individual products should be certified based on their intended use in a certain sector.

Term	Definition
ACER	European Union Agency for the Cooperation of Energy Regulators
AI	Artificial Intelligence
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Informations (National Information Systems Security Agency)
ARERA	Italian Regulator Authority for Energy Networks, and Environment
CAPEX	Capital Expenditures
CEER	Council of European Energy Regulators
CEP	Clean Energy Package
CNR-Ircres	Research Institute on Sustainable Economic Growth
cPPP	Contractual Public Private Partnership
CRE	French Energy Regulator Authority
CUS WG	Consumer Working Group
DER	Distributed Energy Sources
DSO	Distribution System Operator
ELDER	Turkish Electricity Distribution Services Association
ENISA	European Union Agency for Cybersecurity
EVs	Electric Vehicles
GSE	Energy Services Manager
ICT	Information Communications Technology
IoT	Internet of Things
IRENA	International Renewable Energy Agency
IT	Information Technology
MEDREG	Association of Mediterranean Energy Regulators
MV	Medium Voltage
O&M	Operation and Maintenance
OPEX	Operating Expenditures
OT	Operational Technology
PV	Photovoltaic
RE	Renewable Energy
REGAGEN	Energy Regulatory Agency of Montenegro
RES	Renewable Energy Solutions
RSE	Energy System Research Italy
TSO	Transmission System Operator
URWP	Union Rolling Work Program

Co-funded by
the European Union

MEDREG – Association of Mediterranean Energy Regulators
Via Fieno 3, 20123 Milan, Italy –Tel: +39 3402938023
info@medreg-regulators.org www.medreg-regulators.org