MEDREG

WORKSHOP ON “DIGITALISATION AND CYBERSECURITY”

20 December 2022

Empowering Mediterranean regulators for a common energy future

Consumer
Working Group
(CUS WG)

Co-funded by
the European Union

Introduction

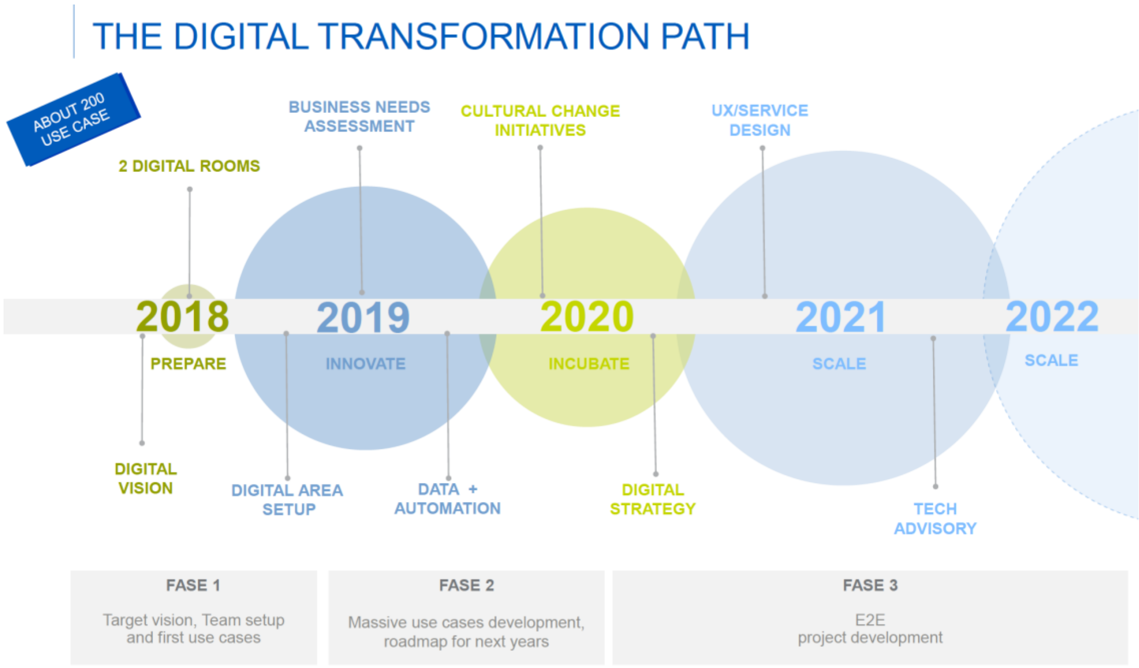
Digitalisation is also playing an increasingly important role in the energy market, as it provides new opportunities for improving the efficiency and reliability of the energy grid. This includes the use of advanced analytics and machine learning to optimize the operation of power plants and the grid, as well as the deployment of smart meters and other digital technologies to improve the accuracy and reliability of energy consumption data.

However, the increasing reliance on digital technologies also brings new challenges in terms of cybersecurity, as it creates new vulnerabilities that can be exploited by cyber criminals. To address these challenges, energy companies must implement robust cybersecurity measures, such as encryption, authentication, and access controls, to protect their systems and data from cyber-attacks.

Keynote Speakers

Mr. Lorenzo Montelatici – *Edison Spa.*

Through the years, Edison has been taking solid steps towards a digital transformation. The digital vision started back in the year 2018, where a vision was in place and hence a team was set up to achieve the deliverables and to make the vision become a reality. The figure below shows the steps that have been taken since 2018 till the current date.



Currently, the digital section of Edison has specific roles within the business. The activities and competencies handled by the digitalization team include data science, demand and project management, UX/service design, automation, motivation of a cultural change, and establishing and promoting technology partnerships to develop innovative solutions.

Thank to digitalising, work has transformed into an agile methodology. The agile methodology of getting things done is characterized by a high level of innovation with a high level of complexity, but at a low budget. Furthermore, Machine learning applications which include automated marketing, asset management and forecasts have been realized by Edison in multiple fields.

Edison currently forecasts wind energy production, where an optimal bidding strategy in day-ahead and continuous trading market can be made. The goal of such project is to reduce the imbalances in the network and their related costs, as well as optimizing the planning of maintenance activities. This project was a major success, where it has been extended to the entire Edison wind portfolio.

Mr. Polat Baskurt – *TEİAŞ, Türkiye*

Digitalisation at TEIAS has allowed Türkiye to improve transmission system stability, also allowing the system to be interconnected with the European grid following the ENTSO-E guidelines. Furthermore, fluctuations have decreased. A major step in line with digitalising the system can be owed to the SCADA system, which has optimised the processes overall. Thank to digitalisation, errors have also decreased, and investments have been reduced in less significant areas, allowing TEIAS to focus investments on more critical aspects. In that regard, smarter methods of accounting for demand response, integration of new Renewable Energy Sources, smart charging and small distribution resources have been realised.

TEIAS is currently using a market management system, which was completely developed and coded in-house, and it is used to forecast supply and demand using solar and wind load forecasts. In that regard, balancing supply and demand has become easier.

Furthermore, TEIAS is not capable of preparing climate maps that are updated frequently. Cameras and sensors have been places on numerous transmission towers to monitor wind related telemetric data such as wind speed, angle of attack, pitch, role, and other aspects. When TEIAS updates the climate map, they can see a bigger picture of the status of the infrastructure and equipment.

Although there are benefits of digitalisation, there are cybersecurity problems. It is commonly known in the industry that full prevention from cybersecurity is impossible, however, if prepared, limited impact can be attained. In that regard, TEIAS focuses on cyber resilience, where cyber resilience is an organisation's ability to overcome and recover from cybersecurity incidents. Furthermore, TEIAS adopts CIA guidelines, which are Confidential Integrity and Availability.

Mr. Nikos Raftopoulos – *IPTO, Greece (Med-TSO)*

As a part of IPTO's digitalization attempts, a strong development of the IT infrastructure data centre took place. A heavy investment was made to focus on the IT service management and to have a cloud, which allows for efficient data handling and easier data handling. IPTO has also developed a new SDLC methodology and using the DevSecOps methodology by creating a new business unit for each specific and complex TSO project.

The digitalization strategy started back in 2018 by creating an action plan which builds the vision of the IT modernization and digitalization, which consists of the initial building blocks, the first systems that need to be developed and how can they be connected to the operational technology (OT). Later, in 2020, some pilot projects were launched.

A data analytics ecosystem was also established, which is a customer centric model which focuses on the business needs rather than the technological ones. This model is a collaborative model and involves lots of cross functional tasks, where employees from different backgrounds get to meet and brainstorm to understand the next potential steps in implementing a system.

Regarding cyber security, since IPO and the TSO in general are the most critical infrastructure of all critical infrastructures in the country, IPTO has realized a resilient security system using the DevSecOps methodology, both on the in-house systems and on the platforms that are acquired from the market. The cybersecurity standards implemented comply with 27001 and 27019 ISO standards for the energy sector. Furthermore, as people are the most vital asset, IPTO invests in awareness by training technical and non-technical employees starting from governance implementing the zero-trust architecture considering supply chain management at party vendors if they're connections with third party system.

Panel 1: Cybersecurity Network Code and Handling Cyberattacks in the Digitalisation Era

Moderated by: **Ms. Karima Sadou –** *CREG, Algeria*

Mr. Davor Bajs – *Energy Community.*

The Energy Community has established a coordination group for cybersecurity and critical infrastructure aligning MC Procedural Act of the 29th of November 2018. The cybersecurity initiative targets critical infrastructures and essential services in electricity, fossil fuels and emissions, as well as digital and electronic communications (services provided to energy operators). The stakeholders that take part in the initiative include the ministries of energy, climate, communications, and information technologies of the respective countries as well as the TSOs and DSOs that service the critical infrastructures and the national computer security incident response teams (CSIRT).

The tasks that are established as per the cybersecurity infinitive include establishing an administrative and operational environment, communicating reports, data, strategies and Research and development material to develop and apply EU coherent methodologies and standards for risk assessment of the existing necessary infrastructures and securing information and other relevant technologies. Furthermore, the initiative attempts to establish a CSIRT network, where necessary.

The objectives of the recent cybersecurity study carried in the energy community countries were to assess the legal and regulatory environment, identifying regulatory gaps, assessing potential cyberthreats, identifying relative provisions, carrying out impact assessment and proposing measures that can be adapted on national level and hence design a model for regional cooperation.

Mr. Øyvind Anders Arntzen Toftegaard – *NV, Norway (CEER)*

Due to the ever-growing importance of cybersecurity, especially during through the digitalization era, CEER has proposed to launch a cybersecurity workstream in July 2014. This initiative came in a time where cyberattacks and secure smart metering have become a trending subject in the European Union, where many NRAs had to deal with cybersecurity topics at the national level and had the capacity to share their experiences with their peers.

The cybersecurity workstream breaks down its activities into short-, medium- and long-term ones.

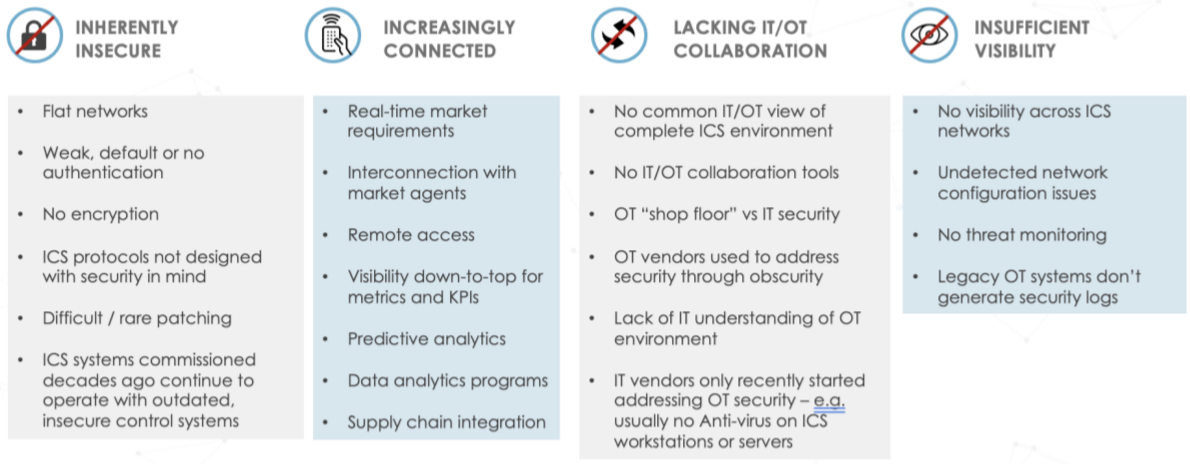
Short term activities by then workstream comprise of comprehending the problem from an energy context, raising awareness in NRAs, clarifying the role of the NRAs in that matter and stock-taking of cybersecurity activities, project experience and registered attacks. Medium-term activities include CEER assessment reports on cyber resilience and the publishing of a CEER paper on the role of NRAs regarding cybersecurity.

Meanwhile, long-term activities contain the linking and synchronization of the cybersecurity work stream with the other CEER activities and workstreams as well as the creation of a CEER training course on cybersecurity.

As for the ACER's network code on cybersecurity, CEER ensures that the guidelines are followed by the NRAs. The network code on sector-specific rules for cybersecurity aspects on cross-border flow (NCCS) constitutes of the three levels of cybersecurity (union-wide and regional, member state and entity level), guidelines on the cooperation between authorities and methods of information sharing.

Mr. Rafael Aranha – *REN, Portugal (Med-TSO)*

As a part of the measures taken to ensure Cybersecurity in the Electricity Transmission System, REN breaks down the reasons why Integrated Computer Systems can be vulnerable. The leading reasons can be seen in the table below:



INHERENTLY INSECURE	INCREASINGLY CONNECTED	LACKING IT/OT COLLABORATION	INSUFFICIENT VISIBILITY
• Flat networks • Weak, default or no authentication • No encryption • ICS protocols not designed with security in mind • Difficult / rare patching • ICS systems commissioned decades ago continue to operate with outdated, insecure control systems	• Real-time market requirements • Interconnection with market agents • Remote access • Visibility down-to-top for metrics and KPIs • Predictive analytics • Data analytics programs • Supply chain integration	• No common IT/OT view of complete ICS environment • No IT/OT collaboration tools • OT "shop floor" vs IT security • OT vendors used to address security through obscurity • Lack of IT understanding of OT environment • IT vendors only recently started addressing OT security – e.g. usually no Anti-virus on ICS workstations or servers	• No visibility across ICS networks • Undetected network configuration issues • No threat monitoring • Legacy OT systems don't generate security logs

Even though ICS networks hold numerous advantages, however, the lack of visibility inside an ICS network is an issue when it comes to protecting them – in other words, you cannot protect what you cannot see. Hence, the discovery and ongoing visibility of endpoints, their status and connections are vital.

Among the key intiatives that have been taken by REN that came from the outcome of risk analysis include information security management system, privileged access management, multi-factor authentication for employees and partners, soc & penetration tests, security orchestration, automation, and incident response, "security by design" in industrial environments, information security incident crisis management, awareness programs, and security monitoring on industrial network.

To ensure REN's resilience and fortitude, a huge effort is placed on cultural change, where the employees and users, being the most important asset, can also be the first source of vulnerability of the system. In that regard, REN holds awareness programs, publishes information security policies, carries out phishing simulations, and showcases monthly cybersecurity tips and best practices.

Ms. Erjola Sadushi – *ERE, Albania*

The Albanian legal framework addresses cybersecurity at many levels. Most notable mentions are in the primary legislation, in Law No.2/2017 on Cybersecurity, which defines the security measures, roles and responsibilities of the council of ministries and ministries and the responsible body for proposal and approval of the list of critical infrastructures and important information (updated once every two years). Furthermore, cybersecurity is addressed in law No.43/2015 on power sector which discusses the role of ERE, which is to promote the internal competitive market, to make sure it's safe and friendly operation for customers and suppliers, as well as to ensure the appropriate conditions for safe and sustainable operation of the electrify networks in a close collaboration with the energy community.

The adoption of regulations regarding cybersecurity in ERE obliges the operators to establish appropriate measures during the design, installation, and operation to guarantee security, availability, integrity, and sustainability of the energy systems. Furthermore, the regulations necessitate report submissions to ERE regarding unplanned interventions, violations, and incident in the scope of the security, availability, and integrity of the network, to protect the important infrastructures.

ERE's evaluation comes as follows; In case of the reported incidents, ERE shall review the reported case with the licensee to access if the incident is caused by an action or lack of action from the operator and if there is a need to review regulatory acts or to support as a law enforcement institution to support proposed actions that are aimed to avoid and reduce incidents. ERE may also require detailed information from the CIIO to support any assessment regarding the compatibility of the stakeholder's actions with the rules. ERE's evaluates by providing the identified failures, setting a deadline for the correction of such failures. Should the stakeholder or licensee not conform with the action plan set, sanction of conformity may be applied, as per article 107 of law No.43/2015.

Panel 2: Digitalising the Mediterranean Region (MEDREG Member Case Studies)

Moderated by: **Mr. Igor Telebak –** *REGAGEN, Montenegro*

Mr. Guillaume Bullier – *CRE, France*

Since France has one main DSO, Enedis, which runs distribution activities in 95% of the French mainland, free and mandatory installation of smart meters is possible, where by 2022, 35 million smart meters have been deployed, which accumulates to over 90% of Enedis clients.

The link smart meters do not only provide an easy way to measure electricity consumption, but it is also a solid step in the direction of digitalisation. Due to its presence, physical presence of a technician is not necessary for meter reading, and there is also not need for the technician to be present for the operation and setting. The advantages of the smart meters include the decrease in non-technical power losses, the ease of detection of failures, and a better and more efficient network observability.

Furthermore, thanks to the digitalisation of most of the grid, new innovative tariffs have been set on the retail market, where there used to be 1 or 2 periods of tariffs. Currently, suppliers can create more complex time-of-use pricing, a dynamic activation of the price periods has been initiated and the potential dynamic tariffs with load curve. Due to this, there is a low deployment of new offers, versus new services being added to provide consumption data and recommendation to the consumers.

Smart meter costs are covered by the reduction of losses and the automation of metering data collection. Among the disadvantages of smart meters are the difficulties in penetrating the market and the lack of scalability.

Mr. Andre Buttigieg – *REWS, Malta*

Malta has also witnessed a nationwide smart meter rollout. By the end of 2021, Malta reached a percentage of smart meter rollout of 90.87%, which goes beyond the threshold set by the Electricity Directive 2009/72/EC that requires the EU Member States to rollout electricity smart meters for 80% of consumers by 2020 (Malta the 80% target was reached back in 2017).

The smart meters in Malta, which were rolled out by the Maltese DSO Enemalta plc., have numerous functionalities. Using the smart meter, remote spot reading for import and export registers are possible, time-of-use consumption reading, remote activation and deactivation, remote power limit curtailment, voltage variations data collection and remote meter diagnostics to detect if meter is healthy or faulty.

For the households which do not have a smart meter installed, bills are calculated on the actual consumption at least every six months; while households that are already provided with a smart meter connected to the Automatic Metering Management (AMM) receives bills based on actual readings on a bimonthly basis. The frequency of actual bills for non-household consumers varies from one month to six months.

The bill includes a breakdown of the bill calculations, total electricity consumption for the period covered by the bill, the average consumption per day, applicable tariffs, and CO2 emissions. The bill also includes the consumption related to the previous year and projections for electricity annual consumption.

Mr. Okan Yardımcı – *EMRA, Türkiye*

REPUBLIC OF TÜRKİYE
ENERGY MARKET
REGULATORY AUTHORITY

Within the Turkish Energy Regulator, EMRA, there exists the Energy Transition Department. Within this department there are numerous groups like EV charging station group, Complementary markets and alternative fuels group, the research and development and innovation group, and the digital transformation group.

Focusing on the Digital Transformation group, among the tasks that are carried out by the group are the monthly update of a bulletin to keep up with the latest developments and maintaining a dictionary titled as ‘Digital Transformation in the Energy Sector’ to ensure language unity between the IT team and the Energy team. Thanks to the group, there also the authorisation for EV users to use the ‘Free Access Platform’ for public charging stations, which provides dynamic and static data. The group is also responsible for the development of some R&D projects such as the national smart meter system, the creation of a domestic software development ecosystem for the energy industry and methods for measuring and monitoring the digital maturity levels of the DSOs, as well as the approval of DSO R&D projects.

Conclusions

Cybersecurity and digitalization are becoming increasingly important in the energy market, as the industry becomes more reliant on digital technologies to manage and control critical infrastructure.

Cybersecurity and digitalization are important considerations in the energy market, as they impact the reliability and security of the energy grid and the protection of sensitive data and information. Digitalisation offers many benefits for the energy market, but it also brings with it new cybersecurity risks. By implementing robust cybersecurity measures, energy regulators and companies can protect their digital infrastructure and ensure the reliability and security of the energy supply.

Co-funded by
the European Union

MEDREG – Association of Mediterranean Energy Regulators
Via Lazzaretto 3, 20124 Milan, Italy – Tel: +39 3402938023
info@medreg-regulators.org   www.medreg-regulators.org