Recommendation of interoperability platforms and data exchange for TSO-DSO-customer coordination

D11.3

Authors:

Ivelina Stoyanova (RWTH)	Gonçalo Glória (R&D NESTER)
Sonja Kajganic (RWTH)	Marjan Ilkovski (ULJ)
Emmanouil Zoulias (UoA)	Ondrej Cerny (E.DSO)
Arslan Ahmad Bashir (Volue Oy)	Valerie Reif (EUI)
Marko Petron (Cybernetica)	Daniele Stampatori (EUI)
Madalena Lacerda (E-REDES)	

Responsible Partner	RWTH Aachen
Checked by WP leader	José Pablo Chaves Ávila, 26/10/2023
Verified by the appointed Reviewers	Ferdinando Bosco, 31/10/2023 Kalle Kukk, 1/11/2023
Approved by Project Coordinator	Padraic McKeever (Fraunhofer), 31.01.2024

Dissemination Level	Public

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Issue Record

Planned delivery date	31.10.2023
Actual date of delivery	31.01.2024
Version	V1.0

Version	Date	Author(s)	Notes
0.1	26.04.23	Ivelina Stoyanova, Madalena Lacerda, Sonja Kajganic, Katerina Drivakou, Marjan Ilkovski, Ondrej Cerny, Valerie Reif, Daniele Stampatori, Arslan Ahmad Bashir	
0.2	16.10.23	Ivelina Stoyanova, Madalena Lacerda, Sonja Kajganic, Katerina Drivakou, Marjan Ilkovski, Ondrej Cerny, Valerie Reif, Daniele Stampatori, Arslan Ahmad Bashir, Anastasis Tzoumpas	
0.3	14.11.23	Ivelina Stoyanova	Updated after review

Disclaimer:

All information provided reflects the status of the OneNet project at the time of writing and may be subject to change. All information reflects only the author's view and the European Climate, Infrastructure and Environment Executive Agency (CINEA) is not responsible for any use that may be made of the information contained in this deliverable.

About OneNet

The project OneNet (One Network for Europe) will provide a seamless integration of all the actors in the electricity network across Europe to create the conditions for a synergistic operation that optimizes the overall energy system while creating an open and fair market structure.

OneNet is funded through the EU's eighth Framework Programme Horizon 2020, "TSO – DSO Consumer: Large-scale demonstrations of innovative grid services through demand response, storage and small-scale (RES) generation" and responds to the call "Building a low-carbon, climate resilient future (LC)".

As the electrical grid moves from being a fully centralized to a highly decentralized system, grid operators have to adapt to this changing environment and adjust their current business model to accommodate faster reactions and adaptive flexibility. This is an unprecedented challenge requiring an unprecedented solution. The project brings together a consortium of over 70 partners, including key IT players, leading research institutions and the two most relevant associations for grid operators.

The key elements of the project are:

1. Definition of a common market design for Europe: this means standardized products and key parameters for grid services which aim at the coordination of all actors, from grid operators to customers;
2. Definition of a Common IT Architecture and Common IT Interfaces: this means not trying to create a single IT platform for all the products but enabling an open architecture of interactions among several platforms so that anybody can join any market across Europe; and
3. Large-scale demonstrators to implement and showcase the scalable solutions developed throughout the project. These demonstrators are organized in four clusters coming to include countries in every region of Europe and testing innovative use cases never validated before.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

List of Abbreviations and Acronyms

Acronym	Meaning
AGNO	Adaptive Group Notification algorithm
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
ASVS	Application Security Verification Standard
BRP	Balancing Responsible Parties
BSP	Balancing Service Provider
BUC	Business Use Case
CEEPS	Central electro-energy portal
CGM	Common Grid Model
CIM	Common Information Model
CSV	Comma-separated values
DEP	Data Exchange Platform
DDEP	DSO Data Exchange Platform
DGIA	Deadline Guarantee and Influence-Aware Scheduling
DMM	Data Management Model
DR	Demand Response
DSO	Distribution System Operator
ECCo SP	ENTSO-E Communication and Connectivity Service Platform
EHV	Extra-High Voltage
EU	European Union
FSP	Flexibility Service Provider
FWGL	Framework Guideline
GDPR	General Data Protection Regulation
HEMRM	Harmonized Electricity Market Role Model
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HV	High Voltage
IMO	Independent Market Operator
JSON	JavaScript Object Notation
KORRR	Key Organisation Requirements, Roles and Responsibilities
LC	Low carbon
LMP	Local Market Platform
MARI	Manually Activated Reserves Initiative
NEMO	Nominated Electricity Market Operator

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

OMIE	Electricity market operator for the Iberian peninsula's day-ahead and intraday electricity markets
ONS	OneNet System
OPDE	Operational Planning Data Environment
OWASP	Open Web Application Security Project
PBCM	Process-Based Cost Modeling
PCR	Price Coupling of Regions
PTDF	Power Transfer Distribution Factor
RCC	Regional Coordination Centre
RDF	Resource Description Framework
RES	Renewable Energy Sources
SGAM	Smart Grid Architecture Model
STAR	System of Traceability of Renewables Activation
SO	System Operator
SO GL	System Operation Guideline
SUC	System Use Case
TDEP	TSO Data Exchange Platform
TSO	Transmission System Operator
UI	User Interface
UMEI	Universal Market Enabling Interface
UML	Unified Modeling Language
XBID	Cross-Border Intraday
XML	Extensible Markup Language

List of Figures

List of Tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Executive Summary

Task 11.3 aims to outline the harmonization of data exchange and interfaces for the EU wide adoption of solutions to enable TSO-DSO-customer coordination. Therefore, this document formulates recommendations for interoperability and data exchange starting from the implemented OneNet demo solutions and mapping these results on European level.

The contribution of this document is twofold. First, recommendations for the harmonization of TSO-DSO-customer data exchange and interoperability are formulated based on a review of the implemented OneNet demos and an analysis of the deployed common and proprietary solutions. Second, to map the findings to the EU level, various harmonization actions are evaluated and then prioritized for implementation based on their EU impact, timeline and implementation cost.

The in-depth analysis of common and proprietary solutions showed that very often proprietary solutions are preferred due to regional specifics and advantages for the existing infrastructure, which the common solutions fail to meet. For example, some of the demos mentioned that proprietary solutions are more easily compatible with existing systems, which lowers the cost and reduces the required effort from personnel. Moreover, existing common solutions often do not offer viable solutions for the specific requirements or do not fulfil the security standards of the system operator. However, the local specifics and existing proprietary solutions maintain the heterogeneous character of data exchange across Europe. Therefore, detailed guidelines leading to a roadmap for harmonized data exchange and interfaces would be highly beneficial. It is worth noting that interoperability does not necessarily require a fully harmonized data exchange, as long as the communication among proprietary and common solutions is secured and the integration into a common ecosystem is seamless. Here, the main challenge will be to find an adequate balance between, on one side, regional specifics and small entities which require proprietary solutions and, on the other side, an EU-wide harmonization of data exchange.

Furthermore, the wide investments into smart meters across Europe and the standardization of communication among end devices would significantly support harmonization in data exchange, as the low smart meter penetration is a limitation to the availability of flexibilities and has the potential to bring significant difficulties with the non-standardized data exchange from distributed flexibility assets. In the context of activation of end customer flexibility and the rollout of smart meters, this would mobilize the extensive use of data exchange and interfaces and highlight the necessity for harmonization, making it an enabler of market profitability by increasing liquidity and facilitating market transactions, apart from solely operational needs. Therefore, besides the activation of additional flexibility, the incentivization of the end customer would have additionally the indirect benefit to speed up the harmonization of the data exchange of the European energy sector.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Lastly, open-source solutions in combination with cybersecurity measures would facilitate data exchange and interfaces among TSOs-DSOs-customers, providing opportunities for adaptability, while at the same time cyber-shielding the system operators' activities to ensure the resilience of the energy system. in this sense, the "Network Code for cybersecurity aspects of cross-border electricity flows"[1] should be extended to emphasize the TSO-DSO-customer data exchanges, interfaces and setting the cybersecurity framework that will facilitate/cyber-shield open-source solutions.

In terms of the evaluation of harmonization actions according to their potential EU impact and feasibility, various aspects of data exchange and interoperability are discussed, and respective harmonization actions are suggested and prioritized. As a general remark, the literature review showed that there is no systemized procedure for the evaluation of actions on European scale. While it is understandable that the procedure and the concrete evaluation criteria may vary depending on the context and the field, following a European vision and using science-based rules for the elaboration of a roadmap seem crucial for a thorough and sustainable development of European solutions.

As expected, some aspects of the energy sector are more critical than others. For example, the harmonization in the field of cyber security has a very high priority for the secure energy supply, but also for the penetration of smart meters and for the development and introduction of European solutions and services, which could be applied in all countries. Pan-European business models indirectly enable the activation of additional flexibility and lower the costs for the system operators and for the end customer by avoiding additional cost for implementation and adaptation to meet different conditions and requirements in different countries. Further high-priority aspects are flexibility and platform communication.

[1] https://eepublicdownloads.entsoe.eu/clean-documents/Network%20codes%20documents/NC%20CS/220114_NCCS_Legal_Text.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

1 Introduction

To enable a secure and affordable energy supply in the future power grids with a significant amount of renewable energy sources, distributed resources and fluctuating availability of flexibility, the establishment of active system management is a central requirement. In this context, the coordination among Transmission System Operator (TSO), Distribution System Operator (DSO) and customer is considered crucial to maximize the integration of flexibility service providers (FSP), to improve the efficiency and reliability of the energy supply.

1.1 Task 11.3

WP11 outlines EU-wide implementation to procure standardized products through interoperable platforms. In this context, Task 11.3 reviews the harmonization of data exchange and interfaces to improve interoperability and formulate recommendations for harmonization actions. Therefore, first, recommendations for the harmonization of TSO-DSO-customer data exchange and interoperability are formulated based on a review of the implemented OneNet demo systems and an analysis of the deployed common and proprietary solutions. Here, the necessity to deploy proprietary solutions is analysed to identify potential gaps of the common solutions and suggest how to improve those and harmonize the data exchange. Second, to map the findings to the EU level, for various aspects such as platform communication and cyber security, concrete harmonization actions are collected, evaluated and then prioritized for implementation based on their EU impact, timeline and implementation cost.

1.2 Objectives of the Work Reported in this Deliverable

The objective of this work is to improve TSO-DSO-customer interoperability, enable EU wide deployment of solutions and support cross-border business models for the energy sector. This goal is achieved by outlining the harmonization of data exchange and interfaces for the EU wide adoption of solutions in terms of interoperable platforms, data models and formats, cyber security, protocols and common information models, market algorithms and system operation (operation of electric power systems including security, control and quality, as well as the synchronous operation of interconnected power systems, tools, platforms and systems), and the mapping of the outcome to the EU level by prioritizing harmonization actions from EU perspective.

1.3 Outline of the Deliverable

This document is organized as follows. Chapter 2 introduces the applied methodology. Chapter 3 holds a review of EU initiatives for data interoperability and evaluation of corresponding harmonization actions. Chapter 4 presents the implemented demo systems, as well as the outcome of WP4, WP5 and WP6, and consolidates the theoretical definition and the practical implementation. In Chapter 5, the implemented solutions in the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

demos regarding data exchange and interfaces are reviewed, and common and proprietary solutions are analysed to find potential barriers for harmonization. Chapter 6 presents possible harmonization actions and their evaluation regarding their potential to improve interoperability at EU level. Here, several harmonization actions in terms of data exchange for platform communication are evaluated based on the expected EU impact, urgency and timeframe, implementation cost, etc. Chapter 6 summarizes the conclusions of the work in T11.3 and the recommendations for harmonized data exchange measures to improve interoperability at EU level and enable TSO-DSO-customer coordination.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

2 Methodology

The goal of T11.3 is to suggest harmonization actions in terms of data exchange, interfaces and platforms to improve the interoperability and enable TSO-DSO-customer coordination. Therefore, the analysis was performed at two levels, first the OneNet solutions and second, mapped to the EU level. The chapter Methodology is organized as following. Section 2.1 introduces the methodology for the formulation of recommendations for harmonization in terms of data exchange and interfaces. Then section 2.2 presents the methodology used for the evaluation of concrete harmonization actions with the corresponding criteria and prioritization method.

2.1 Harmonization of data exchange and interfaces

In the first step, the implemented demo systems are compared to the theoretical requirements developed in OneNet in order to revise the degree to which the theoretical requirements were applied. In the next step, the implemented solutions in terms of data exchange and interfaces such as applied standards, communication protocols or cyber security measures are analysed as presented in Figure 2.1. Here, the analysis differentiates between common and proprietary solutions to evaluate the reasons which hindered the deployment of common solutions, and to verify if the deployment of a proprietary solution affected interoperability. The gaps and limitations of common solutions and the mismatch of requirements serve as a basis for the recommendations how to extend the common solutions to maximize their applicability in different conditions. Furthermore, this analysis provides an insight into the level of interoperability, if the applied proprietary solutions limited interoperability and what consequences this brings, but also what conclusions can be made regarding interoperability and how it can be improved. This consideration stems from the fact that proprietary solutions do not necessarily hinder interoperability if the interactions with the rest of the system are secured.

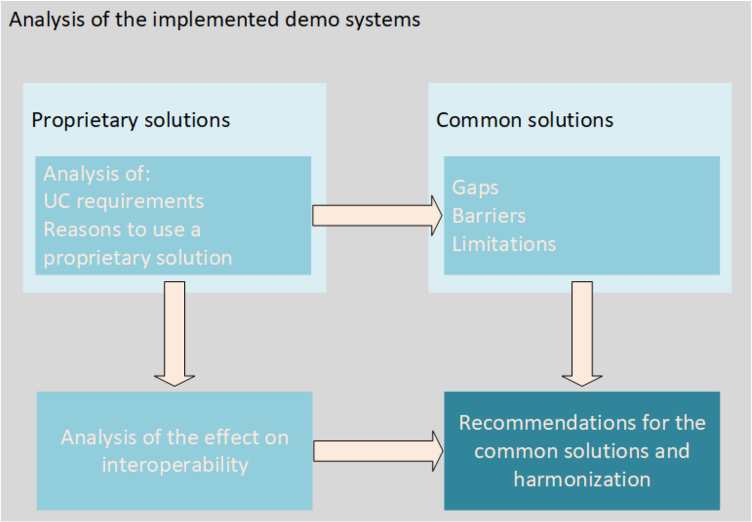
Analysis of the implemented demo systems
Proprietary solutions
Analysis of:
UC requirements
Reasons to use a proprietary solution
Common solutions
Gaps
Barriers
Limitations
Analysis of the effect on interoperability
Recommendations for the common solutions and harmonization

Figure 2.1 - Methodology for the formulation of recommendations for the adaptation of common solutions and harmonization of data exchange and interfaces

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

2.2 Evaluation of harmonization actions for data exchange and interfaces

The state of the art of the requirements for the implementation of EU-wide solutions builds the bridge to the mapping of the results to the EU level. In this context, according to the methodology presented in detail in section 6.1 and illustrated in Figure 6.1, concrete harmonization actions in various aspects of data exchange and interfaces have been collected, evaluated, and prioritized according to their potential EU impact, timeline and cost.

First, existing EU initiatives in the field of the harmonization of data exchange and interfaces were reviewed in order to follow a predefined methodology if available, apply existing guidelines and fulfil the EU requirements as presented in chapter 3 of this document. Then, the demos provided lists of potential harmonization measures for data exchange and interfaces and marked the expected EU impact, urgency and cost. Furthermore, ENTSO-E and E.DSO provided their insight on the topic in interviews, which is also included in the evaluation of harmonization measures.

Finally, the analysed harmonization measures are prioritized as high, medium and low priority actions to set the basis for the further work on interoperability in T11.7.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3 EU Initiatives for Data Interoperability

In order to set a basis for the evaluation of harmonization measures, to include previously set standards and requirements at EU level and to apply existing methodology for the harmonization of data exchange, existing EU initiatives were reviewed and analysed. Even though there is a wide landscape of policy, legislative and regulatory initiatives addressed at TSO-DSO-customers coordination at EU level [1], none of them focuses on harmonization of data exchange and interfaces. Further EU initiatives under the high-level policy themes of energy sector, general data economy, and general cyber security were also reviewed in order to find a general methodology for harmonization. To the knowledge of the authors, there is no universal methodology or guidelines for the drafting or prioritization of harmonization measures valid at EU level. An overview of the results of the literature review is presented in the following. This subsection is structured into three parts, namely data exchange, interfaces and cybersecurity.

3.1 Data exchange

Initiatives related to energy data exchange can be broadly categorised according to the type of data that is being exchanged. In [2], the authors analyse initiatives related to network and market data on the one hand and customer data on the other hand.

3.1.1 Network and market data

For network and market data, data models, formats and protocols generally have a higher level of harmonisation across EU member states. This is especially the case for data that is exchanged among TSOs, Regional Coordination Centres (RCCs) and, where relevant, Nominated Electricity Market Operators (NEMOs). Requirements to build the necessary infrastructure (both software and hardware) started to emerge with the Third Energy Package of 2009. Regulation (EC) No 714/2009 included provisions on the publication, exchange and transparency of data by TSOs [3]. TSOs shall share significant data on aggregated forecasts and actual demand, the operational status and utilisation of generation and load assets, network availability and usage, interconnections, and the equilibrium of power and reserve capacity. In the case of small generation and load units, summarised estimated data might be used. Furthermore, TSOs are mandated to transparently publish all pertinent information pertaining to network accessibility, usage, and availability. This entails a comprehensive report delineating congested areas, the methods employed for managing congestion, and forthcoming management strategies. In addition, data pertaining to cross-border trade, based on the most accurate forecast feasible, should be shared. To meet this requirement, the concerned market participants must supply relevant data to the TSOs. This information must be made readily accessible in a user-friendly format. It should also be accessible through standardised methods of information exchange, collaboratively determined with market participants. This data should encompass a historical span of at least two years, ensuring that new market

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

entrants have access. Lastly, TSOs must engage in regular data exchange, providing accurate network and load flow data that enables load flow calculations for each TSO in their respective operational domains. Regulation (EC) No 714/2009 also included the requirement for ENTSO-E to elaborate network codes and guidelines. [3]

3.1.1.1 System Operation Guideline

The subsequent System Operation Guideline (SO GL) includes, among others, the requirement for all TSOs to jointly agree on key organisation requirements, roles and responsibilities (KORRR) in relation to data exchange. These provisions pertain to the following key elements. Firstly, TSOs are obligated to rapidly communicate any modifications in protection settings, thermal limits, and technical capacities of interconnectors to their neighbouring TSOs. Secondly, DSOs directly connected to transmission systems must ensure timely notifications to the relevant TSOs concerning alterations in data and information, adhering to agreed-upon timeframes. Additionally, there are obligations for adjacent DSOs and those positioned downstream and upstream to mutually exchange information within designated timeframes, specifically addressing changes in data and information. Furthermore, Small Generation Units are entrusted with the responsibility of promptly informing their respective TSOs or DSOs about pertinent changes in data within the agreed-upon timeframes.

The scope of these regulations extends to encompass detailed guidelines [16] regarding the content of data and information, encompassing key principles, data types, communication methods, formats, standards, designated timing, and the individuals or entities accountable for compliance. Moreover, these provisions specify the timing and frequency of data and information submission by DSOs and SGUs. This information, vital for Transmission System Operators' utilisation across diverse time scales – be it real-time, scheduled, or structural data updates – is methodically defined. Lastly, the format for reporting established data and information, as required by [16], is meticulously delineated, ensuring clarity and consistency in compliance procedures. Further requirement for ENTSO-E sets up an operational planning data environment (OPDE) that would facilitate data exchange among TSOs and RCCs and serve as an enabler for the Common Grid Model (CGM) process [4].

In the implementation phase of the network codes and guidelines, ENTSO-E together with the European TSOs have worked towards a harmonisation of both software and hardware related aspects of the relevant data exchange. Concerning software, [2] give an overview of the harmonised data models, formats and protocols that are being used for the exchange of network and market-related data, in particular the Common Information Model (CIM) and related families of profiles as depicted in Table 3.1. Moreover, the OPDE consists of multiple parts that also include a distributed software platform called ‘ENTSO-E Communication and Connectivity Service Platform’ (ECCo SP) that acts as a data exchange service bus and serves to collect and distribute the data. Since its development, ECCo SP has been used in several European RD&I projects, including INTERRFACE and OneNet. Several tools and their usage have also been harmonised across both EU-wide implementation and research

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

projects. Examples are the use of the Smart Grid Architecture Model (SGAM) Framework, the Unified Modeling Language (UML), as well as the Harmonized Electricity Market Role Model (HEMRM).

Table 3.1 - Overview of differences in practices for the exchange of market and network data, source: [2]

	Market Data	Network Data
Complexity of data structure	Low	High
Data structures	Hierarchical	Meshed
Data model	Hierarchical (XML)	Graph (RDF)
Data format applied	XML	CIMXML

3.1.1.2 Framework Guideline on Demand Response

Most recently, a Framework Guideline (FWGL) was elaborated by ACER in preparation for a new network code or guideline on Demand Response (DR) [5]. It provides the broad framework for the development of new rules related to data exchange between TSOs, DSOs, Balancing Service Providers (BSPs), Balancing Responsible Parties (BRPs) and FSPs for the provision and the use of system services. Regarding the procurement of local SO services through market-based methods, there is an emphasis on transparent communication between TSOs and neighbouring TSOs. Additionally, DSOs directly connected to transmission systems are expected to notify relevant TSOs about data changes within stipulated timeframes. Interoperability between local markets and other wholesale markets is sought, ensuring streamlined access and coordination even if not immediately adopted in the national terms and conditions for local SO services' market design. When coordinating SO services, it is imperative to establish coordination areas comprising elements impacted by congestion or voltage issues. The degree of coordination varies based on the severity and relevance of the issue, with different levels of interaction. These rules also detail forecasting mechanisms, efficient solutions, and cost allocation protocols for SOs in managing congestion and voltage control. The rules emphasise the responsibility of each SO to address congestion and voltage control within their grid, with cost allocation proportional to the SO managing the issue. Furthermore, there's provision for activating SO services across different SO grids if deemed beneficial. Central to this coordination is data exchange, ensuring equitable access to resources, optimal selection, activation of resources, and synchronised service management. These data exchange principles are developed to align with existing regulations and regional methodologies. The national terms and conditions for SO coordination outlines the entire coordination process, ensuring consistency and optimal resource utilisation across all SOs. This proposal aligns with existing EU-wide methodologies and ensures actions taken by one SO don't negatively

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

impact others. While the FWGL DR sets out principles and processes, the detailed rules will be specified in the new network code or guideline, which at the time of writing is available in a draft version.[2]

3.1.2 Customer data

For customer data, the level of harmonisation is much lower across Member States due to existing legacy systems. Measures for customer protection, provisions for interoperability of smart metering systems and requirements for data management models were already included in the Third Energy Package of 2009. These provisions were reiterated and extended in the Clean Energy Package of 2019. Customers have been given the right to access and share their electricity metering and consumption data, and the implementation is ongoing. It is a challenging process due to the differences in data management models (DMMs) that exist across Member States. A DMM refers to 'the framework of roles and responsibilities assigned to any party within the electricity system and market and the subsequent duties related to data collection, processing, delivery, exchanges, publishing and access' [6]. Some countries like Austria or the Germany rely on decentralised models, while others like Denmark, Norway, Finland or the Baltic countries chose to implement centralised models (so-called 'data hubs').

To achieve interoperability, Article 24 of Directive (EU) 2019/944 enables the European Commission to adopt implementing acts specifying interoperability requirements and access to metering and consumption data, as well as data for customer switching, demand response and other services [8]. The first of a series of implementing acts was adopted in June 2023 [9]. It applies to metering and consumption data in the form of validated historical metering and consumption data and non-validated near-real time metering and consumption data. It sets out a "reference model" that defines common rules and procedures at Union level for the business, function and information layers of the SGAM, in line with national practices. The reference model is composed of a "role model" with a set of roles and responsibilities and their interactions, an "information model" that contains information objects, their attributes, and the relationships between these objects, and a "process model" detailing the procedural steps. The reference model is technology-neutral but reflects, as far as possible, definitions and terminology that are used in available standards and the relevant European initiatives such as the HEMRM or the CIM. By facilitating a harmonised documentation of customer data-related processes, the reference model aims to ensure that market participants have a mutual and clear understanding of the roles, responsibilities and procedures for access to data, and that national practices become more easily comparable.

A report by the Smart Grids Task Force gives an overview of the different choices that Member States have made in terms of data formats and models [6]. In the lead-up to the publication of the Clean Energy Package,

[2] The interested reader can consult the draft here: https://consultations.entsoe.eu/markets/public-consultation-networkcode-demand-response/supporting_documents/Network%20Code%20Demand%20Response%20v1%20draft%20proposal.pdf.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

there had been a discussion on whether or not one common EU model should be implemented. Since then, however, the consensus emerged that the solution should be to make the existing models interoperable rather than requiring countries to change their models [7]. To achieve data interoperability, it is crucial to involve all relevant stakeholders in open discussions and negotiations. This collaborative approach should be underpinned by transparent provisions for ongoing development, ensuring that reference models evolve to meet emerging needs and national variations. In the realm of electricity and gas markets, adopting a unified role model emerges as a pivotal step. This common framework streamlines responsibilities and assignments, ensuring seamless integration within the broader energy system. An equally vital aspect lies in the implementation of a shared information model. This serves to define the precise semantics of energy-related data exchange. With a clear understanding of terms, interoperability is enhanced, laying a robust foundation for effective communication between stakeholders. Flexibility emerges as a key theme, especially concerning core role, information and process models. These models must be capable of accommodating national peculiarities while also fostering ongoing interoperability. This measured approach allows for a gradual convergence, preserving established systems. When articulating business requirements, it is imperative to do so in a technology-neutral manner. Here, SGAM offers a framework for the unified definition of system architectures for Smart Grids. [10] By focusing on the Business Layer from the SGAM interoperability layers and leaving the finer technical details to individual states, adaptability to various environments is assured. Leveraging existing international standards and profiles provides a solid foundation for energy information exchange. By doing so, the groundwork for cross-border communication is firmly established. Continual alignment with reference models in terms of role models, information models and process models is paramount [11]. Regular assessments ensure that national practices remain in harmony with evolving standards, fostering a sustained trajectory towards interoperability. In terms of information exchange, it is prudent to centre efforts around harmonised roles rather than specific actors, as the characteristics, tasks and interactions among actors may change with time, and roles' definitions are stable and less variable with changing conditions. This approach allows for regional variations while still maintaining a cohesive process. Legal considerations in national markets can pose significant challenges to full interoperability. Recognising and addressing these regulatory barriers is vital for ensuring seamless cross-border compatibility. While prioritising interoperability is fundamental, cost/benefit analyses can provide valuable insights into the optimal path forward. These assessments help in tailoring convergence steps and timelines to the specific contexts and potential risks and opportunities. A step-by-step approach, guided by a well-monitored roadmap, proves invaluable. This allows for controlled adaptation and alignment with established national structures, recognising that achieving interoperability is an evolving process.

While DMMs are not harmonised across countries, several tools and processes have experienced a certain level of harmonisation in recent years. For example, standardised and harmonised processes have been elaborated by ebIX for liberalised downstream electricity and gas markets in the form of Business Specification Requirements [1]. In collaboration with ENTSO-E and EFET, ebIX has drafted the Harmonised Electricity Market

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Role Model (HEMRM) [11]. This model doesn't depict the actual electricity market structure; rather, it outlines the interconnected roles relevant to information exchange. HEMRM dissects the electricity market into a standardised array of roles and domains. This modelling is indispensable due to the intricate nature of market participation: a single entity can undertake multiple roles, while in decentralised competitive markets, different entities can assume diverse roles. To establish effective information exchange processes, precise role definitions are essential. This approach ensures that business processes are tailored to meet the requirements of harmonised roles rather than catering to specific entities.

The FWGL DR provides the broad framework for new rules on data exchange between TSOs, DSOs, BSPs and FSPs for the provision and use of system services [5]. The details of the new rules will be specified in the upcoming network code on Demand Response. For data exchange among SOs and between the SOs and service providers, the FWGL DR states that the new rules shall establish principles for interoperability on national level and shall ensure coherence with the interoperability rules for access to data for demand response (i.e., the implementing acts described above), not multiplying interfaces, to reduce costs.

3.2 Interfaces

An interface is a connection or programme that allows the connection and/or communication of one device or system to another. Practices regarding the existing interfaces between relevant actors involved in energy data exchange vary across Member States, in particular when it concerns customer data [6]. Market participants rely on the characteristics of the available interfaces, especially when they want to set up their operations in a certain Member State, but it is not always straightforward for them to get hold of it.

The recently adopted implementing act thus specifies a list of information that needs to be accessible for eligible market parties to register, on-board or establish prerequisite infrastructure to take part in procedures related to metering and consumption data exchange [9]. This includes information about standardised interfaces for historical and near-real-time data from of smart metering systems, including the basic class of the interface utilised, the physical interface standard, the communication protocol, and the data format. ”Near real-time metering and consumption data” is defined in the implementing act as “metering and consumption data provided continuously by a smart meter or a smart metering system in a short time period, usually down to seconds or up to the imbalance settlement period in the national market, which is non-validated and made available through a standardised interface or through remote access in line with Article 20(a) of the Electricity Directive (EU) 2019/944” [8]. The implementing act also states that Member States shall have due regard for the use of relevant available standards for the provision of non-validated near real-time data through a standardised interface, where applicable.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

3.3 Cybersecurity

At EU level, both general and energy sector-specific cybersecurity initiatives exist. The following provides an overview of selected legislative files: the generally applicable NIS-Directive and EU Cyber Security Act, and the sector-specific risk preparedness regulation and network code on cybersecurity.

The NIS-Directive (EU) 2016/1148 concerns security of network and information systems [13]. The Directive has increased the EU national cybersecurity capabilities, requiring Member States to elaborate national cybersecurity strategies, establish Computer Security Incident Response Teams (CSIRTs), and appoint NIS national competent authorities, improving the cyber resilience of public and private entities in specific sectors and across digital services. However, its implementation has proved to be difficult and resulted in fragmentation at different levels across the Member States.

In 2022, the NIS 2 Directive (EU) 2022/2555 was thus adopted, broadening the scope of the first NIS Directive and strengthening the imposed security requirements [14]. The core aim of the first NIS Directive is to ensure consistent high-level security for network and information systems across the EU. This is achieved by enhancing national cybersecurity capabilities, fostering EU-level collaboration, and mandating risk management and incident reporting for essential service and digital service providers. Member states must develop National Strategies on Security, outlining objectives, preparedness measures, public-private cooperation, awareness efforts, and risk assessment. These strategies ensure a coordinated approach to cybersecurity, contributing to a resilient and secure digital environment across the EU. NIS 2 addresses security of supply chains, streamlines reporting obligations, introduces more stringent supervisory measures and stricter enforcement requirements including harmonised sanctions regimes across Member States. It also includes proposals for information sharing and cooperation on cyber crisis management at national and EU level.

The EU Cyber Security Act (Regulation (EU) 2019/881) was adopted in 2019 [15]. The act reinforces the mandate of the European Union Agency for Network and Information and Security (ENISA) to better support Member States with tackling cybersecurity threats and attacks. It also establishes an EU framework for a one-stop shop for cybersecurity certification for products, processes and services that is be valid throughout the EU.

Regarding energy sector-specific legislation, Regulation (EU) 2019/941 on risk preparedness of the Clean Energy for all Europeans Package (CEP) sets out a common framework of rules on how to prevent, prepare for and manage electricity crises, bringing more transparency in the preparation phase and during an electricity crisis and ensuring that measures are taken in a coordinated and effective manner. It stresses the need to properly assess all risks, including those related to cyber security and proposes to adopt measures to prevent and mitigate those identified risks. The Regulation is already foreseeing and referring to the development of the new network code on cybersecurity that would lay out more specific rules.

The new network code lays out sector-specific rules for cybersecurity aspects of cross-border electricity flows [12]. It establishes a governance scheme, determines common criteria for performing risk assessments,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

promotes a common electricity cybersecurity framework, provides for clear verification rules, establishes information flows and effective processes to identify, classify and respond to cross-border cybersecurity incidents. It also sets up effective processes for crisis management and defines common principles for cybersecurity exercises. Moreover, it lays out rules for the protection of information exchange under the network code and establishes a framework for monitoring, benchmarking, and reporting on the new rules. Due to its nature as network code, it is binding in its entirety and directly applicable in the EU Member States.

3.4 Further related EU initiatives

This section presents a review of several EU initiatives on different topics with the common goal to draft a roadmap for the corresponding topic. The section is meant to investigate if there is a common procedure and certain principles to be followed, defined at EU level and to set the theoretical ground to draft a roadmap for interoperability starting with the evaluation of harmonization measures.

Several EU initiatives at least partially covering the interoperability topic are analysed: the Energy Roadmap 2050, the Action Plan for passenger rail, the Robotics 2020 Multi-Annual Roadmap. Furthermore, we also included ‘A Shared Nationwide Interoperability Roadmap version 1.0’ in our analysis: in fact, it can be considered as a reference in the context of the development of interoperable solutions, even though its applicability is limited due to the different conditions and regulatory framework. The aim of this section is to identify the focus and the methodology applied within these initiatives, in terms of priorities, assessment of implementation costs, etc. The initiatives were selected to cover sectors beyond the context of data harmonisation.

The Energy Roadmap 2050 lays out a comprehensive framework to achieve a sustainable, secure, and competitive energy landscape in the European Union by 2050 [17]. This objective is broken down into specific aims: to guide political decision-making, illuminate trade-offs, and support policymakers in setting milestones post-2020. The roadmap places emphasis on key priorities. Effectiveness through clear, targeted policies is crucial for driving emissions reductions and sustainable energy practices. Efficiency in costs and resource allocation is another pivotal priority, ensuring that the economic implications are balanced and manageable. Coherence across policies and objectives is central to align the roadmap with broader EU goals and societal needs. The methodology employed in crafting the Energy Roadmap 2050 starts with rigorous modelling and scenario analysis, allowing for the exploration of multiple potential futures. Assumptions are made transparent, acknowledging uncertainties, and allowing for flexibility in planning. The methodology also integrates extensive stakeholder consultation and expert input, recognising the value of diverse perspectives in shaping effective policy.

The Action Plan for passenger rail aims to invigorate rail travel by focusing on several key objectives [18]. These include increasing rail usage, particularly for long-distance and cross-border travel, aligning with the European Green Deal for reduced greenhouse gas emissions, and ensuring accessibility and affordability for all

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

Europeans, including those in rural and remote regions. Market opening is emphasised to foster competition, interoperability, and harmonisation within the European railway market. Leverage from the Recovery and Resilience Facility (RRF) is identified as a critical strategy to support rail investment and recovery from the impacts of the COVID-19 pandemic. To effectuate a modal shift towards rail for long-distance travel, the plan envisions promoting a departure from other transportation modes. Additionally, it aspires to establish a unified European railway area to ensure equal access to public railway transport. In terms of methodologies, substantial investment in rail infrastructure, including high-speed rail and trans-European transport networks (TEN-T), is advocated. A robust regulatory framework will be developed and implemented to encourage competition, interoperability, and harmonisation. Digitalisation of rail operations is prioritised to enhance service quality and stimulate price competition. Market opening remains a focal point, aiming to introduce competition and nurture the development of a single European railway area. The plan also underscores the importance of research and innovation in the rail sector to introduce cutting-edge solutions and technologies.

In its essence, the Robotics 2020 Multi-Annual Roadmap (MAR) is a technical companion to the Strategic Research Agenda (SRA), offering comprehensive insights into applications, markets, and technologies outlined in the SRA [19]. Updated annually, it adapts to evolving R&D&I priorities in Europe. The overarching objective is to establish a unified framework for European robotics, with a keen focus on technically driven market development.

The goals set forth in this endeavour are threefold. First, to define a clear description framework for robotics in Europe. Second, to specify objectives for market-driven technological development. Lastly, to demonstrate the relevance of these objectives for future market opportunities.

Methodologically, the MAR tailors perspectives for different readers, ranging from industry professionals and researchers to policymakers, financiers, and potential users. Proposals referencing the MAR should harmonise with its defined framework to establish context and impact. The MAR Background serves as a structured framework for proposals targeting specific calls, encompassing technology advancements, ability levels, market requirements, TRL assessment, and impact delivery mechanism.

Different sectors are analysed. For instance, the focus on logistics p seeks to advance autonomy in transport systems, particularly in robotics and embedded systems, to enhance efficiency and safety in transportation and logistics processes, especially within the European Union's manufacturing sector. Short to medium-term priorities include warehouse-based systems, order picking, distribution centres, and intra-logistics operations. The emphasis is on integrating robots into existing human-operated setups for flexibility and efficiency.

Technical opportunities lie in the development of autonomous vehicles, picking, packing, and loading for distribution, warehouse optimisation, operations planning, and safe human-robot interaction. Challenges encompass autonomous navigation, adaptability to dynamic environments, proximity to humans, and integration with existing infrastructure. The goal is to create flexible solutions for loading, unloading, and

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

repackaging goods in warehouses, as well as improving customer-level stock monitoring and product identification.

A Shared Nationwide Interoperability Roadmap version 1.0 envisions an interoperable health system that empowers individuals to utilise their electronic health information effectively [20]. It aims to enable smarter, safer, and more efficient care delivery while promoting innovation at all levels. The Health Information Technology for Economic and Clinical Health (HITECH) Act laid the groundwork, but progress towards interoperability has been a work in progress since 2015.

The Office of the National Coordinator for Health IT (ONC) is committed to expeditiously, systematically, and sustainably advancing this vision. The roadmap focuses on near-term actions (by the end of 2017) to make immediate progress in interoperability.

Three high-level goals for health IT interoperability have been identified:

- 2015-2017: Enhance the use of priority data domains to improve healthcare quality and outcomes.
- 2018-2020: Expand data sources and users in the interoperable health IT ecosystem to improve health and lower costs.
- 2021-2024: Achieve nationwide interoperability to enable a learning health system.

Four critical pathways have been highlighted to create a foundation for long-term success:

- Improve technical standards and implementation guidance for priority data domains.
- Shift payment policies to stimulate demand for interoperability.
- Clarify and align privacy and security requirements.
- Promote consistent policies and business practices that support interoperability.

The roadmap is organised into three sections:

- Drivers: Mechanisms to support a payment and regulatory environment that relies on and deepens interoperability.
- Policy and Technical Components: Essential items stakeholders will need to implement to enable interoperability.
- Outcomes: Metrics to measure collective progress in implementing the roadmap.

The roadmap is a living document that will be updated as milestones are met and new challenges emerge, with ongoing stakeholder feedback and involvement.

Based on our analysis, a common and standardised strategy for implementing a roadmap was not observed. In fact, the analysed strategies above have objectives and priority evaluation that greatly depend on the specific field of application of the considered roadmap. In light of the absence of a single standardised and universally accepted method for evaluating and implementing a roadmap, this deliverable presents an original approach in this context, as outlined in Section 6.1.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

4 OneNet System and Demo Systems

This chapter investigates the actual application of interoperable solutions in the work done within the OneNet project, namely in the project demos and in the OneNet System architecture.

The OneNet System (or OneNet Framework) consists of three main components, i) the OneNet Decentralized Middleware, ii) the OneNet Orchestration Workbench, and iii) the OneNet Monitoring and Analytics Dashboard. The OneNet Connector is a specific instance of the OneNet Decentralized Middleware placed inside each platform to facilitate an easy integration and cooperation among the platforms, maintaining the data ownership and preserving access to the data sources [35].

The section below defines the categories for which interoperability aspects are discussed, followed by the evaluation of demo systems and of the connector.

4.1 Definition of categories

Throughout this document, various aspects of data exchange and interfaces are analysed in order to harmonize the data exchange. In the following, the categories are listed and defined.

Data exchange

Data exchange defines the sharing of information among entities. Here, the information being exchanged among stakeholders such as TSO, DSO, aggregator, market operator, customer, etc. is considered, for example bids, flexibility, etc., but also the process and functionalities in relation with data as well as compliance and application with standards.

Data models

A data model is a conceptual representation defining the structure, relationships, constraints, and semantics of data in a system or database. It facilitates tasks such as understanding, storing, retrieving, and manipulating information. Examples of data models include the CIM.

Protocols

Protocols serve as essential mechanisms facilitating communication among various technological systems. The application of a reliable and secure data exchange is defined by the protocol's framework: format, transmission, and interpretation of the data. The following are some commonly used protocols such as RESTful HTTP, SML, IMAP, and SMTP.

Data formats

A data format is the definition of the structure of data within an existing system and describes how the data is to be interpreted to gain information. In the context of the digitalization of the energy grid, there are two widely used formats: JSON and XML. The former, JSON, offers a lightweight and human-readable structure, making it compatible with various modern programming languages, while the latter, XML, provides flexibility through text-based data, facilitating standardized and structured data exchange.

Interfaces

An interface defines a point at which entities are able to interact. This can be a device which enables the physical exchange of materials, a system that connects entities, etc. In the context of this work, an interface is a point at which different components exchange information.

The interfaces between the different roles (e.g., between TSO, DSO, FSP, Aggregator, MO) are vital for ensuring the efficient and reliable operation, especially in combination of technical coordination. Aligned with the designated responsibilities of each role, these interfaces serve as conduits for data exchange and communication, allowing collaborative efforts.

Cyber security

Cyber security is the deployment of measures to protect organizations, their IT systems and data from digital threads. Due to the growing decentralization and digitalization, defining cybersecurity measures has become crucial, such as data anonymization and encryption of the data. In the circumstances of digitalization and increasing data exchange, a system to enable observability and controllability is critical. Here, various cyber security measures are considered, which vary among the demos.

System operation

System Operation covers the complete area of activities for operating electric power systems, including security, control and quality in terms of fixed technical standards, principles and procedures, but also the synchronous operation of interconnected power systems, tools, platforms and systems. System Operation covers the following areas for network codes according to Article 8(6) (a), (d), (e) and (f) of Regulation No (EC) 714/2009, set out respectively below [3]:

- network security and reliability rules including rules for technical transmission reserve capacity for operational network security;
- data exchange and settlement rules;
- interoperability rules;
- operational procedures in an emergency.

Furthermore, in the context of system operations technical coordination platforms, tools such as forecasting and planning, but also systems are included.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Market algorithms

The energy market relies on mathematical models and computer algorithms to execute trades. The algorithms process real-time information form the grid and from the market to take decisions based on predefined rules. Market algorithms such as AGNO, DGIA, and PBCM provide the basis for an effective market operation and optimization.

4.2 Evaluation of demo systems

4.2.1 Western Cluster

In the context of the OneNet project, the Western cluster consists of the implementation of three demonstrators situated in Portugal, Spain and France. This cluster focuses mainly on the procurement of local flexibility by the DSO and TSO and aspects such as TSO-DSO coordination in the context of balancing, congestion management and operational planning of the network, and, particularly to the Spanish demonstrator, the interaction of FSPs with the market.

Following, a brief description of the System Use Cases (SUCs) developed in the different demonstrators will be given for each of the demonstrators. Note that a more thorough description of these SUCs can be found in D5.1 [36] and D9.1 [37].

Portuguese Demonstrator

SUC-PT-01: Evaluation of the Product & Grid pre-qualification requirements

This SUC is divided into two different stages: the product and the grid evaluation process. The use case will test each step, including the validation of a given set of requirements, some categorized as mandatory and others as informative/optional, to prequalify an FSP. Namely, for product evaluation, it identifies which mandatory and informative requirements are needed to evaluate whether the unit can (technically) deliver the product it aims to sell/deliver. For grid evaluation, in the pre-qualification phase, a grid impact assessment is done.

SUC-PT-02: Day-Ahead & Intraday Flexibility needs

This SUC defines and tests the coordination process between the DSO and TSO in order to determine how much flexibility will need to be acquired for a short-term timeframe. Coordination is needed to prevent congestions in the distribution and transmission grids, due to activation of active power flexibilities to fulfil the needs of both DSO and TSO.

SUC-PT-06: Maintenance plans information exchange

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

This SUC is aligned with the idea that an accurate definition of the maintenance plans is crucial for the operational activities of different stakeholders, such as customers and grid operators. The maintenance work plans should be defined between DSOs and TSOs on an annual basis (long-term). This SUC has the objective to keep track of the schedule of the maintenance works and update them, when necessary, by exchanging more detailed information during different timeframes (medium-term until close to real-time).

SUC-PT-07: Consumption and generation forecast information exchange

This SUC defines and tests the exchange of information between SOs to improve their planning activities in the short term. The generation forecast shall be disaggregated by technology type (Solar, Wind, Hydro, CHP, among others). The load forecast can also be exchanged in a disaggregated way by distinguishing different types of customers. This information will be exchanged day-ahead between operators, taking into consideration the market clearance results.

SUC-PT-08: Short-circuit levels information exchange

This SUC defines and tests the short-circuit levels forecast information exchange between the TSO and DSO for the Extra High-Voltage/High Voltage (EHV-HV) substations, by establishing the process to compute and exchange the complete short-circuit currents in the interface nodes that could be used for operational planning purposes.

Spanish Demonstrator

SUC ES-01: Local Market Platform

This SUC describes the platform that will be developed to enable the procurement of local flexibility by the Spanish DSOs, the communications among the different actors in the demonstration, the storage of information with regards to FSP pre-qualification and qualification, as well as the market-clearing for the different markets and products to be tested. In addition, the Local Market Platform will be the interface of the Spanish demonstrator and the OneNet System. This SUC serves the two Business Use Cases (BUCs) within the Spanish demonstrator, WECL-ES-01 and WECL-ES-02, related to the long-term and short-term congestion management, respectively.

French Demonstrator

SUC-FR-01: TSO automated activation

To simplify and optimize the management of renewable production curtailments through the System of Traceability of Renewables Activation (STAR) platform, this SUC aims to define and test the information exchanges and processes needed to perform the related BUC’s traceability objectives in the case of TSO automated activations.

SUC-FR-02: DSO manual activation

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

This SUC provides requirements for data exchanges and processes between TSO, DSO, FSPs and producers for the STAR platform to handle the related BUC's traceability objectives in the case of DSO manual flexibility activations due to DSO or TSO network congestions.

Table 4.1 presents the analysis of the Western cluster's SUCs in terms of data exchanges, including the interfaces between which the data is exchanged, and information related to the data models, the communication protocols and the data exchange formats used.

Table 4.1 - Information on data parameters used for the Western cluster

UC ID	UC Name	Interfaces	Exchanged data	Data models	Communication protocols	Data exchange formats
SUC-PT-01	Evaluation of the Product & Grid pre-qualification requirements	TSO-DSO (TSO Data Exchange Platform - TDEP)	FSP data and prequalification result	Custom (based on Universal Market Enabling Interface - UMEI)	REST API	JSON
		DSO-TSO (DSO Data Exchange Platform DDEP)	FSP data and prequalification result			
SUC-PT-02	Day-Ahead & Intraday Flexibility needs	TSO-DSO (TDEP)	Flexibility needs	Custom (based on UMEI)	REST API	JSON
		DSO-TSO (DDEP)	Flexibility needs			
		TSO (TDEP) - ONS (OneNet System)	Flexibility needs			
		DSO(DDEP)-ONS	Flexibility needs			
SUC-PT-06	Maintenance plans information exchange	TSO-DSO (TDEP)	Annual maintenance plans	Custom (based on UMEI, ENTSO-E outage planning coordination)	REST API	XML
		DSO-TSO (DDEP)	Annual maintenance plans			
		TSO-DSO (TDEP)	Weekly/ monthly works update			
		DSO-TSO (DDEP)	Weekly/ monthly works update			

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

SUC-PT-07	Consumption and generation forecast information exchange	DSO-TSO (DDEP)	Consumption and generation forecast	Custom (based on UMEI)	REST API	XML
SUC-PT-08	Short-circuit levels information exchange	TSO-DSO (TDEP)	TSO short-circuit contributions	Custom (based on UMEI)	REST API	XML
		DSO-TSO (DDEP)	DSO short-circuit contributions			
		TSO-DSO (TDEP)	Complete TSO-DSO short-circuit contribution			
SUC-ES-01	Local Market Platform (LMP)	FSP-LMP	Basic Participant information	Custom (based on OMIE's specific schemes)	AMQP, HTTP	XML, JSON
		FSP-LMP	Market participant pre-qualification information			
		FSP-LMP	Market resource pre-qualification information			
		LMP-DSO	Technical resource pre-qualification information			
		DSO-LMP	Generic attributes			
		DSO-LMP	Product parameters			
		LMP-IMO (Independent Market Operator)	List of pre-qualified units			

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

		LMP- IMO	List of qualified units			
		FSP-LMP	Bid			
		LMP- DSO/FSP	Validate market results			
SUC-FR-01	TSO automated activation	TSO/DSO-STAR	Activation orders	IEC ESMP 62325-503, ISO 8601, CIM-based	REST API, manual	JSON
		TSO-STAR	Estimated curtailed energy			CSV
		TSO/DSO-STAR	Production metering			CSV
SUC-FR-02	DSO manual activation	DSO -STAR	Activation orders	IEC 62325-503, ISO 8601, CIM-based	REST API, manual	JSON
		TSO-STAR	Estimated curtailed energy			CSV
		TSO/DSO-STAR	Production metering			CSV

The "Interfaces" column reflects the nature of the demos and applicability of the different SUCs. For the Portuguese demo, the information exchange happens between both the SOs, TSO and DSO, through the DDEP and TDEP (DSO/TSO Data Exchange Platform) and is specifically focused on the technical TSO-DSO coordination, therefore, no interaction with other market participants (FSPs – Flexibility Service Providers, IMOs – Independent Market Operators) is envisaged. The French demonstrator is also more centred on the technical coordination, foreseeing the exchange of data between the SO and the STAR platform, aiming to study DERs activation and management. The Spanish demo, on the other hand, relies on data exchange between the Local Market Platform (LMP) and DSOs, or with the FSPs. This illustrates the centricity of the Spanish demo on the interaction with the local market.

The data exchanged for the Portuguese demo illustrates the variety and applicability of the SUCs, from flexibility information (FSP data and prequalification results); maintenance plans (annual, weekly or monthly works update); and consumption and generation forecast and short circuits contribution by the SOs. The Spanish demo relies on exchanged data regarding market participants and resources, such as on prequalification. There is also subsequent information exchanged concerning prequalified, bidding and validated market results, which is aligned with the scope of this demo, more focused on the market. For the French demo, the exchanged data is related to activation orders by connecting the DSO with the STAR, estimated curtailed energy through

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

communication between the TSO and STAR and production metering, for both SOs connected to the STAR platform.

The data models used for the Portuguese and Spanish demos are Custom based, whereas the French demo uses a CIM based one. Both demonstrators use REST APIs while the Spanish demo resorts to Advanced Message Queuing Protocol (AMQP) for the data exchange. All the SUCs from the Western cluster use JavaScript Object Notation (JSON), Extensible Markup Language (XML) or Comma-separated values (CSV) formats.

Table 4.2 presents information regarding cybersecurity measures taken for data security and privacy, market algorithms applied (power exchange, bidding, optimization, forecasting...) and system operations (data exchange and existing tools for forecasting, monitoring, settlement and activation) in the Western cluster demonstrations.

Table 4.2 - Cybersecurity, market algorithms and system operations used for the Western cluster

UC ID	UC Name	Interface	Cybersecurity	Market algorithms	System operations
SUC-PT-01	Evaluation of the Product & Grid pre-qualification requirements	TSO-DSO (TDEP) DSO-TSO (DDEP)	• Compliance with entity-level cybersecurity rules • Firewall IP rules • HTTPS • Token-based authentication	None	• DDEP and TDEP (data exchange platforms)
SUC-PT-02	Day-Ahead & Intraday Flexibility needs	TSO-DSO (TDEP) DSO-TSO (DDEP) TSO (TDEP)-ONS DSO (DDEP)-ONS	• Compliance with GDPR • Compliance with entity-level cybersecurity rules • Firewall IP rules • HTTPS • Token-based authentication	None	• DDEP and TDEP (data exchange platforms) • TSO Flexibility Needs Evaluation and FSP flexibility provision simulation tool
SUC-PT-06	Maintenance information exchange	TSO-DSO (TDEP) DSO-TSO (DDEP) TSO-DSO (TDEP)	• Compliance with entity-level cybersecurity rules • Firewall IP rules • HTTPS • Token-based authentication	None	• DDEP and TDEP (data exchange platforms)

		DSO-TSO (DDEP)			
SUC-PT-07	Consumption and generation forecast information exchange	DSO-TSO (DDEP)	• Compliance with entity-level cybersecurity rules • Firewall IP rules • HTTPS • Token-based authentication	None	• DDEP and TDEP (data exchange platforms) • DSO operational planning tool (includes optimal power flow calculations) (DPLAN) • DSO Production and consumption forecast tool (PREDIS)
SUC-PT-08	Short-circuit levels information exchange	TSO-DSO (TDEP) DSO-TSO (DDEP) TSO-DSO (TDEP)	• Compliance with entity-level cybersecurity rules • Firewall IP rules • HTTPS • Token-based authentication	None	• DDEP and TDEP (data exchange platforms) • Short-Circuit levels forecast Tool in TSO-DSO substations • DSO operational planning tool (includes optimal power flow calculations) (DPLAN)
SUC-ES-01	Local Market Platform (LMP)	FSP-LMP	• Compliance with entity-level cybersecurity rules • Firewall IP rules • HTTPS • Digital Certificate authentication provided by OMIE	None	• Data exchange through LMP: Register and basic information about the market participant such as username and password
		FSP-LMP		None	• Data exchange through LMP:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

					Contact information; Fiscal data; Access contract; bank details; power of representation; confidentiality agreement; declaration of non-collusion
		FSP-LMP		None	• Data exchange through LMP: market participants provide information on the resources they want to prequalify facility/resource name; type of technology; location; market participant; etc.
		LMP-DSO		None	• Data exchange through LMP: Verification of the installed capacity to provide the service: Power; CUPs (Universal Supply Point Code acronym in Spanish); Maximum flexibility quantity; Response time; etc. • Tools: DSO power flow analysis tools to develop

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

					technical pre-qualification
		DSO-LMP		None	• Data exchange through LMP: composed of generic parameters concerning the market session being requested • Tools: DSO power flow analysis tools to identify congestion problem
		DSO-LMP		None	• Data exchange through LMP: composed of product parameters concerning the market session being requested: service window, availability, activation window... • Tools: DSO power flow analysis tools to identify flexibility requirements
		LMP-IMO		Algorithm for identification of pre-qualified units	• Data exchange through LMP: list of pre-qualified units for a given market session
		LMP-IMO		None	• Data exchange through LMP: list of qualified units for a given market

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

					session. The list can refer to the market qualification, technical qualification or the consolidated list
		FSP-LMP		None	• Data exchange through LMP: Composed of bidding information
		LMP-DSO/FSP		Algorithm for sorting and prioritizing bids	• Data exchange through LMP: Validated market results by either the IMO (market), the DSO (technical) or the consolidated market results
SUC-FR-01	TSO automated activation	TSO/DSO-STAR	• Compliance with entity-level cybersecurity rules • HTTPS • Token-based authentication (blockchain)	None	• Predictive Control algorithm for automated orders (only for generating orders, only tracking in STAR platform) • Data exchange through STAR
		TSO-STAR		None	• Estimated Energy not served tool • Data exchange through STAR
		TSO/DSO-STAR		None	• Metering data collection process • Data exchange through STAR
SUC-FR-02	DSO manual activation	DSO - STAR	• Compliance with entity-level cybersecurity rules	None	Data exchange through STAR

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

		TSO-STAR	- HTTPS - Token-based authentication (blockchain)	None	- Estimated Energy not served - Data exchange through STAR
		TSO/DSO-STAR		None	- Metering data collection process - Data exchange through STAR

Concerning cybersecurity measures, all the demonstrators of Western cluster are adopting Hypertext Transfer Protocol Secure (HTTPS) and compliance with entry-level rules, for the data managed by the TSO or compliance with GDPR (General data protection regulation) for the Data Exchange Platforms (DEPs). Also, commonly used solutions, such as Firewall IP rules are used both for the Portuguese and Spanish demonstrators. Regarding cybersecure authentication measures, the Portuguese and French demos using a token-based approach, with the French demonstrator resorting to a blockchain-based solution. The Spanish demonstrator has adopted a Digital Certificate for authentication, provided by OMIE.

Given that the Western Cluster demonstrators are more directed to the technical/operational management of the networks, only the Spanish demo is implementing market algorithms, either to choose the units which comply with requirements of prequalification or to conduct a prioritization to sort bids considering offered flexibility amount and price.

Concerning the category of system operations, it varies from use case to use case. Regarding the Portuguese demonstration, the central pieces are the DDEP and TDEP, which are used to fulfil the main purpose of the demo, that is the technical TSO-DSO coordination. The demonstration also foresees the development and/or adaptation of tools for the assessment of flexibility needs, daily forecast of generation and demand and short-circuit forecasts. As seen in Table 4.1, the Spanish demonstrator relies on data exchange between the several involved parties in the LMP, and it will not only allow the registry of participants but it will also foresee the exchange of information to/from the platform to allow the implementation of the market, including basic information about the market participants and their resources, input and output data from the product and grid prequalification and market results. The demo will also resort to DSO power flow analysis tools to identify congestions and flexibility requirements for the technical prequalification. For the French demo, predictive control algorithms are applied for automated orders (only for generated orders, tracked in the STAR platform), together with tools to estimate energy not served and a metering data collection process.

4.2.2 Southern Cluster

In the context of OneNet project, the Southern cluster demonstrator consists of the implementation of two pilot projects situated in Greece and Cyprus respectively. The objective of the Southern Demonstrator is to devise, develop, implement and evaluate two pilot projects in Greece and Cyprus dealing with balancing and congestion management challenges facing system operators in the clean energy era, in compliance with the OneNet overall architecture. The results will be evaluated to provide recommendations for future market reforms in the region and harmonise a pan-EU electricity market. The primary activity of the Greek demonstrator is the improvement of the procedures for congestion management resolution. The Greek demonstrator focuses on the technical-based TSO-DSO coordination based on the existing market architecture. On the other hand, the Cyprus demonstrator aims to provide an effective collaboration framework for the TSO-DSO-Customer value chain and the energy market by developing an active balancing and congestion management platform. The Cypriot demonstrator includes the definition of a market-based TSO-DSO coordination.

More specifically, in the Cypriot demo, two business scenarios will be considered for demonstration purposes. The first scenario deals with the participation of FSPs to balance the frequency of the system after a disturbance, while the second scenario with the congestion management in the distribution grid including sub-scenarios for line overloading and voltage limit violation. The four system use cases (SUCs) mentioned in the table below will be used to accomplish both BUCs for the specific demonstration. The SUCs consider the monitoring of the operating conditions at both the transmission and the distribution grid, the prequalification of the location-based limits for the market products, the evaluation of the FSPs response, and the online coordination of the flexibility services by the distributed resources.

In the Greek demo, also two business scenarios will be considered for the demonstration purposes. The first scenario deals with improved identification of the available flexibility resources, focused on a DSO voltage level, together with the improved identification of the power system flexibility needs, focused on a TSO voltage level grid, on a longer time-span and wider geographical scope than the one being utilised today, through simultaneous DSO and TSO and grid simulations. The second scenario deals with enhanced severe weather condition management with predictive maintenance algorithms with the enhanced storm and icing predictions in order to preserve power system from running into dangerous topological or operational states. These business scenarios will be implemented through one system use case focusing on making available the Greek TSO/DSO Flexibility Platform data and services to the OneNet system through a gateway.

In Table 4.3 and Table 4.4 introduced below, the analysis of the Southern cluster system use cases in terms of data exchanges is presented.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Table 4.3 - Information on data parameters used for the Southern cluster

UC ID	UC Name	Interface	Cybersecurity	Market algorithms	System operations
Cypriot Demo: **SUC 2**	Prequalification of the location-based limit of each market product	TSO (real time monitoring–system) - TSO (limit prequalification algorithm)	Current operational conditions real time data	Custom-based data models with data format JSON and CSV	REST, IEEE C37.118, Modbus TCP, HTTPs
		DSO (real time monitoring–system) - DSO (limit prequalification algorithm)	Current operational conditions real time data		
		Historical database - TSO (limit prequalification algorithm)	System operation historical data		
		Historical database - DSO (limit prequalification algorithm)	System operation historical data		
		TSO-MO	Prequalification limits		
		DSO-MO	Prequalification limits		
Cypriot demo **SUC 3**	Evaluation of the Flexible Services Providers response	MO - TSO	Current operational conditions real time data	Custom-based data models with data format JSON and CSV	REST, IEEE C37.118, Modbus TCP, HTTPs
		MO - DSO	Current operational conditions real time data		
		MO - FSPs	System operation historical data		
		TSO (real time monitoring–system) - TSO (evaluation of FSPs' response system)	System operation historical data		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

		DSO (real time monitoring–system) - DSO (evaluation of FSPs' response system)	Prequalification limits		
		TSO - MO	Prequalification limits		
		TSO - SPs			
		DSO - MO			
		DSO - SPs			
Cypriot demo SUC 4	Coordination of distributed flexible resources	MO - TSO	Cleared awarded bids–		
		MO - DSO	Cleared awarded bids–		
		MO - FSPs	Cleared awarded bids		
		DSO (real time monitoring–system) - DSO (coordination of distributed flexible resources system)	Distribution grid real time monitoring data		
		DSO - FSPs	Coordination signals		
Greek demo	Greece TSO/DSO Flexibility Platform data and services - gateway to the OneNet System	GTDCP - ONS	Critical information (critical forecast/ occurrence data)	Custom-based data models with JSON, CSV, netcdf	REST API
		ONS - ONS	Critical information (critical forecast/ occurrence data)		
		GTDCP - ONS	Required information report		
		MO - TSO	Required information report		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

In Table 4.4 below, the analysis of the Southern cluster system use cases in terms of cyber security measures, market algorithms and system operation aspects is presented.

Table 4.4 – Cybersecurity, market algorithms and system operations used for the Southern cluster

UC ID	UC Name	Cybersecurity	Market algorithms	System operations
Cypriot demo SUC 2	Prequalification of the location-based limit of each market product	The data communication is performed within the laboratory with the digital twin, so no additional security measures have been taken.	Forecasting of the 3 hours ahead power flow at the substation (flexibility needs assessment)	Real time measurements are taken for monitoring the system operation (state estimation tool); forecasting upward and downward limits are calculated by the TSO-DSO and exchanged with the energy market through the OneNet system.
Cypriot demo SUC 3	Evaluation of the Flexible Services Providers response	The data communication is performed within the laboratory with the digital twin, so no additional security measures have been taken.	No	Real time measurements are taken for monitoring the system operation and monitoring the response of the FSPs; The market results are also used to evaluate the proper response of the FSPs.
Cypriot demo SUC 4	Coordination of distributed flexible resources	HTTPs that is used for coordination with an actual prosumer which is an encrypted protocol.	Forecasting of the maximum needs for DP and DQ at the substation level for 1-hour ahead to be procured by the DSO to the energy market.	DSO procures DP and DQ to the energy market; DSO coordinates the provision of ancillary services by the FSP according to the real time monitoring of the system (ABCM-T and ABCM-D platforms).
Greek demo SUC	Greece TSO/DSO Flexibility Platform data and services - gateway to the OneNet System	Requested User login and password hashing are mandatory to use F-channel platform	Forecasting RES production and possible power flow congestions	Calculations of RES production and power flow are done for selected geographical region. Resulted data are exchanged through ONENET system together with the weather forecasts for the predefined location and timeframe and information exchange on severe weather condition.

Table 4.3 and Table 4.4 indicate that in the Southern demo the JSON and CSV are the most used data exchange formats irrespective of the kind of data exchanged. Regarding the cyber security measures adopted, they focus on the use of HTTPS protocol and password hashing when logging to the F-channel platform. In terms of market algorithms, the Cypriot demo focus on developing forecasting algorithms for power flow and maximum needs of SOs at substation level and the Greek demo on production and power flow congestion

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

forecasting. In terms of system operation, the Cypriot demo considers data exchange for forecasting, monitoring, and settlement, while the Greek demo only for forecasting.

4.2.3 Eastern Cluster

The Eastern Cluster consists of the demonstrations in the Czech Republic, Poland, Slovenia, and Hungary. All four demonstrations were concluded successfully, aiming to provide an overview of how they defined their areas, selected services, and implemented research and development in their respective IT environments.

In the Czech Republic Demo, the first phase occurred in autumn 2022, testing a network traffic light scheme reflecting various grid issues. The second phase involved EV charging infrastructure tests and a platform for non-frequency services, proving the platform's ability to deliver flexibility in a market-based environment.

The primary objective of the Polish demonstration was to validate supporting DSO and TSO operations through market services, enhancing network flexibility. Specific regions were chosen, and a prototype flexibility platform was created, emphasizing the role of aggregators and the effectiveness of active power services.

The Slovenian Pilot focused on flexibility services, congestion management, and voltage control. It systematically improved over three years, successfully connecting to the OneNet System and proving the benefits of flexibility services for DSOs and end consumers.

The Hungarian Demo, based on regulatory intentions and challenges from solar PV in-feed, proposed functional extensions to the flexibility platform. Due to delays, a simulation environment was created for validation, providing insights into challenges and solutions. The integration with the OneNet system ensured findings were accessible in the broader project context.

In conclusion, these demonstrations underscore the potential of market-based approaches, the crucial role of aggregators, and the need for effective communication and simulations in addressing grid challenges.

EACL-SL-01 deals with congestion management in distribution grids under market conditions. Here, the only prequalification for FSP is to register on the DSO web portal, and to insert the flexibility offer at their measuring point. In the activation phase, customers are activated per e-Mail or SMS messages, or, alternatively, through an activation signal from mail meter as a dry contact. Aggregators are addressed via MQTT. In the settlement phase, FSP can view settlement data in the DSO portal and aggregators in CEEPS. Settlement data are transferred from DSO’s flexibility system to web portal by MQTT message with CIM XML. Then, during the bidding phase, FSP place their bids on the DSO web portal. Aggregators place bids for measuring places in Central electro-energy portal (CEEPS).

EACL-PL-01 deals with the prequalification of FSP resources. Here, FSP resources are certified by the DSO through a Web UI.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

In **EACL-PL02**, DER are managed to provide balancing services to the TSO, as well as to support the congestion management and the voltage control at DSO level.

EACL-PL-03 supports congestion management and voltage control with medium- and long-term market-based active power flexibility coordination.

Table 4.5 and Table 4.6 present the data parameters and the cyber security, system operation details and the market algorithms used in the Eastern Cluster.

Table 4.5 - Information on data parameters used for the Eastern cluster

UC ID	UC Name	Phase	Interfaces	Exchanged Data	Data models	Communication Protocols	Data Exchange Formats
EACL-SL-01	CM in distribution grids under market conditions	Prequalification	FSP-DSO portal	Flexibility potential	CIM XML	MQTT	CIM XML
EACL-SL-01	CM in distribution grids under market conditions	Offering	FSP-DSO portal	Flexibility	CIM XML	MQTT	CIM XML
EACL-SL-01	CM in distribution grids under market conditions	Activation-OTC	FSP-DSO portal Agg-DSO	Activation signal	CIM XML	SMTP GMS MQTT	CIM XML Email SMS
EACL-SL-01	CM in distribution grids under market conditions	Settlement-OTC	FSP-DSO portal Agg-CEEPS	Settlement data	CIM XML	MQTT	CIM XML
EACL-SL-01	CM in distribution grids under market conditions	Grid prequalification					
EACL-SL-01	CM in distribution grids under market conditions	Product prequalification					

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

EACL-SL-01	CM in distribution grids under market conditions	Bidding	FSP-DSO portal Agg-DSO CEEPS	Bids	CIM XML	MQTT	CIM XML
EACL-SL-01	CM in distribution grids under market conditions	Activation-Flexibility market	FSP-MO Aggr-MO	Activation signal	CIM XML	MQTT	CIM XML SMTP GSM
EACL-SL-01	CM in distribution grids under market conditions	Settlement-Flexibility market	FSP-MO Agg-MO	Settlement data	CIM XML	MQTT	CIM XML
EACL-PL-01	Prequalification of FSP resources	Prequalification	FSP-DSO	Status of resources Technical attributes Localization attributes	Web UI JSON	HTTPS JSON	Web UI JSON
EACL-PL-02	Management of DER for balancing services towards TSO CM and VC for DSO	Offering	TSO-DSO FSP-DSO	Auction data Bids (volume, price, time stamp) Volume quantity Price per volume Band Timestamp	Web UI JSON	HTTPS JSON	Web UI JSON
EACL-PL-03	CM and VC with market-based active	Offering	DSO-TSO FSP-DSO	Auction data	Web UI JSON	HTTPS JSON	Web UI JSON

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

	power flexibility Medium and long term			Volume quantity and price			
EACL-CZ-01	CM in distribution grids under market conditions	Offering	ECP	Availability Aggregated availability Required availability	CIM XML		CIM/XML
EACL-CZ-02	CM in distribution grids under market conditions	Activation-OTC		Demand Offer Notifications Executed contracts		HTTPS, REST	JSON

Table 4.6 - Cybersecurity, market algorithms and system operations used for the Eastern cluster

UC ID	UC Name	Phase	Cybersecurity	Market algorithms	System operations
EACL-SL-01	CM in distribution grids under market conditions	Prequalification	For login at Moj elektro portal consumer use two-factor authentication - proprietary	None	None
EACL-SL-01	CM in distribution grids under market conditions	Offering	For login at Moj elektro portal consumer use two-factor authentication - proprietary	None	None
EACL-SL-01	CM in distribution grids under market conditions	Activation-OTC	Consumer's GSM phone no., Activation message between DSO and aggregator is protected using TLS encryption. SCRAM-SHA 512.	None	None
EACL-SL-01	CM in distribution	Settlement-OTC	two-factor authentication	None	None

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

	grids under market conditions				
EACL-SL-01	CM in distribution grids under market conditions	Grid prequalification	two-factor authentication	None	None
EACL-SL-01	CM in distribution grids under market conditions	Product prequalification	two-factor authentication	None	None
EACL-SL-01	CM in distribution grids under market conditions	Bidding	two-factor authentication	None	None
EACL-SL-01	CM in distribution grids under market conditions	Activation-Flexibility market	two-factor authentication	None	None
EACL-SL-01	CM in distribution grids under market conditions	Settlement-Flexibility market	two-factor authentication	None	None
EACL-HU-01	MV feeder voltage control	N/A	N/A	Sensitivity factor calculation, merit order list formulation	N/A
EACL-HU-02	HV/MV overloading mitigation	N/A	N/A	Sensitivity factor calculation, merit order list formulation	N/A
EACL-PL-01	Prequalification of resources provided by FSPs to support flexibility services in the Polish demo	Prequalification of resources	Login at PL DEMO platform (JWT)	None	None

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

EACL-PL-02	Managing active power and/or active energy delivered by DER to provide balancing services to TSO and support CM and VC in DSO grid in Polish demonstration	Offering	Login at PL DEMO platform (JWT)	None	None
EACL-PL-03	CM and VC with market-based active power flexibility in long/medium term in the Polish demo	Offering	Login at PL DEMO platform (JWT)	None	None
EACL-CZ-01	CM in distribution grids under market conditions	Offering	ECP security. See ENTSO-E standard.	None	None
EACL-CZ-02	CM in distribution grids under market conditions	Activation-OTC	GUI: User Login in +4U, access rights by Profiles. API Commands: requires token generated from +4U OIDC Authentication	None	None

4.2.4 Northern Cluster

OneNet Northern cluster (WP7) proposes a flexibility market architecture that enables universal participation of resources irrespective of their physical location to offer services to multiple grids enabling value stacking. To support the single flexibility market end-to-end solution concept, harmonized market products, Flexibility Register and TSO-DSO Coordination Platform are envisioned. In the Northern cluster, the flexibility procurement using harmonized market products is demonstrated in each participating national market, i.e., Finland, Estonia, Latvia, and Lithuania. For this purpose, the current MO platforms will be developed to include a locational or metering point ID among the resource and bid attributes. In the Northern cluster, market clearing is based on optimization, i.e., by matching grid needs with available bids in the most economical way, enabling value-stacking potential. Clearing price is the bid price (pay-as-bid), contrary to the pay-as-cleared price. The grid impact assessment is incorporated into the optimization-based clearing. The optimization considers bids, purchase offers and network information (topology, line limitations, base flows, PTDFs (Power Transfer Distribution Factors)) and yields a list of cleared bids (including the cleared volume) which most optimally solves the congestions in both TSO and DSO networks, as well as power imbalances. Such bids are then sent back to the relevant MO for clearing and activation.

Analysis of the Northern cluster system use cases in terms of data exchanges and processes involved from grid / product pre-qualification to flexibility settlement, are listed in Table 4.7.

Table 4.7 - Information on data parameters used for the Northern cluster

UC ID	UC Name	Interfaces	Exchanged Data	Data Models	Communication Protocols	Data Exchange Formats
DSUC_NO_01	Preparation to flexibility trading	FSP-FR	Contract information	Custom model	Hypertext Transfer Protocol Secure (HTTPS), Internet Protocol, REST API; specific APIs; OpenAPI 3.0	CIM-data formats; JSON
		MO-FR	Product specification	Custom model		NA
		FSP-FR	FSP registration	Custom model		JSON
		SO-FR	Flexibility needs	None		NA
		FSP-FR	Resource information	Custom model		JSON
		FR-T&D CP	Information for grid impact assessment	Custom model		JSON
		FR-FSP/SO/MO	Prequalification results	Custom model		JSON
DSUC_NO_02	Procurement and delivery support	MO-FR/T&D CP/SO	Market results	Custom model		XML, JSON
		T&D CP-FR	Activation confirmation	Custom model		JSON
		T&D CP-FR	Production/consumption plans	Custom model		JSON
		FSP-FR	Real-time metering	Custom model		JSON
		FR-FSP/SO	Information about under or over-delivered flexibilities in real-time	NA		NA
DSUC_NO_03	Flexibility verification and settlement	MDR-FR	Metering data	Custom model		JSON
		FR-SO	Invoicing data	NA		NA
		FR-ISR	Adjusted volumes to imbalance settlement	NA		NA

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

DSUC_ NO_04	Add New Product	SO-MO	Product information	NA		NA
		MO-FR	Product specifications	Custom model		JSON
DSUC_ NO_05	Procurement	FSP-MO	Flexibility bid	NA		NA
		MO-T&D CP	Compliant flexibility bids for grid impact assessment	CIM		CIM XML
		T&D CP-MO	Optimisation results	CIM		CIM XML
		MO-FSP/FR/T&D CP	Market results	NA		NA
		FR-MO	Verified amount of flexibility delivered for each product/FSP	Custom model		JSON
DSUC_ NO_06	Secondary trading	FSP-MO	Need for a take-over of the contract	NA		NA
		FSP-MO	Bid for contract	NA		NA
		MO-T&D CP	Contract bids for grid impact assessment	NA		NA
		MO-FSP	Market results	NA		NA
DSUC_ NO_07	Grid Qualification of Resource	RP-CA CA-T&D CP	Resource provider's consent	NA		NA
		FR-T&D CP	Information about flexibility resources	Custom model		JSON
		SO-T&D CP	Grid information (Grid Nodes, Grid Connecting Elements, Grid Element Capacity)	Custom model		XML, JSON
		T&D CP-FR	Grid qualification results (restrictions)	Custom model		JSON
DSUC_ NO_08	Bid Optimisation	MO- T&D CP T&D CP-(EU)MO	Flexibility bids	CIM		CIM XML
		RP-CA CA-T&D CP	Resource provider's consent	NA		NA
		T&D CP-SO	Flexibility purchase offers Grid information (Grid Node, Grid Connecting Element, Grid Element's Capacity, Grid Element's Base Flow,	Custom model		XML, JSON

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

			Grid Element's Sensitivity Factor)			
		T&D CP-SO/MO	Optimisation results (Cleared Bid, Updated Grid Information and Procurement Cost)	Custom model		XML, JSON
DSUC_ NO_09	Flexibility Call for Tender Opening	T&D CP-SO T&D CP-MO	Flexibility call for tender	CIM		CIM XML

System use cases DSUC_NO_01 to DSUC_NO_03 are described in detail in OneNet deliverable D7.2 Annexes 1-3. DSUC_NO_04 to DSUC_NO_06 are described in detail in OneNet deliverable D7.3 Annexes A-C. DSUC_NO_07 to DSUC_NO_09 are described in OneNet deliverable D7.4 Annex A-C. A brief presentation of the use cases follows.

DS–C_NO_01 - Preparation to flexibility trading

The processes include managing flexibility contracts, registering FSPs and their resources and conducting product prequalification.

DS–C_NO_02 - Procurement and delivery support

The role of Flexibility Register in process phases during flexibility trading and delivery.

DS–C_NO_03 - Flexibility verification and settlement

The verification process quantifies the delivered flexibility and settlement process uses this information to conclude financial and imbalance settlement done partly outside of FR.

DS–C_NO_04 - Add New Product

Prequalification of a new flexibility product from MO perspective.

DS–C_NO_05 - Procurement

The procurement process of flexibility products in a market can be divided into five main processes: opening the market, trading, matching, closing the market, and settlement.

DS–C_NO_06 - Secondary trading

When an FSP, which has a bidding contract for providing a flexibility product for future, realises that cannot fulfil the contract, it can inform and ask market operator to find a replacement for it. This process is called secondary trading and it is quite similar to the normal trading, but the process trigged by sending a request from the FSP, which is not capable to fulfil the contract.

DS–C_NO_07 - Grid Qualification of Resource

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Grid impact assessment is central activity of grid qualification process. Two alternatives are possible. First, concerned SO identifies grid restrictions (constraints) by itself. Second alternative is that restrictions are calculated by TSO-DSO Coordination Platform (T&D CP). The objective is to determine in which network node the activation of the resource would violate the node limitation.

DS–C_NO_08 - Bid Optimisation

Optimising the flexibility bids based on minimising total costs, avoiding further issues in the grids and enabling value-stacking.

DSUC_NO_09 – Flexibility Call for Tender Opening

A call for tender of flexibility services is used in case of capacity products and it is initiated by the SO who needs the flexibility.

The above use cases are validated using different marketplaces, namely TSO-operated markets, Piclo and Nord Pool. Piclo offers Piclo Flex, a leading marketplace for energy flexibility services, enabling distribution system operators to source energy flexibility from flexible service providers during times of high demand or low supply. In particular, Piclo will be filling the Market Operator role in the LT-P-C-E product flexibility trading process for Latvian and Lithuanian demos.

On the other hand, Nord Pool offers an hour-ahead (intraday) marketplace for fine-tuning the commitments made in the day-ahead bidding. Within the Northern cluster, this marketplace is developed with a bid attribute called 'metering-point ID' of a flexibility resource owner that enables multiple SOs and coordination platform to perform grid impact assessment. Such an attribute is not only worthy during the grid pre-qualification but also has a key role in identifying the most optimal bids during the procurement process. The developed marketplace will be demonstrated for the ST-P-E product in the Finnish case.

Usage of Standard Vs Proprietary solutions

The Northern cluster (WP7) is creating technical software solution to implement flexibility process flow called Single Flexibility Platform. Solution contains both standard and proprietary technical components. Internal business logic, together with optimized bid selection algorithm is following proprietary use cases that are worked out by WP7 partners. Integration to external systems of regional stakeholders is implemented via REST API. Platform is opened also for external Pan-European market platforms (e.g., MARI) through OneNet Middleware implementing IDSA FIWARE communication stack.

The logical Data Model format that is used in communication to regional stakeholders are either standard CIM based or proprietary, dependent on communicating stakeholders' existing internal IT system.

As an example, the market operator Nord Pool has its existing proprietary communication data model as changing it was neither in the scope of the project nor the objective of the Nord Pool itself. Transmission system operator Elering has existing IT system supporting standard CIM communication. Based on this, the flexibility platform software solution created during the project was able to utilize the existing system operator IT system.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

In a nutshell, Northern cluster solution developed the capability to demonstrate flexibility use cases for communicating with systems that are implementing not only standardized but also proprietary IT systems. However, preference would be to use standardized CIM format whenever it is possible. Both XML and JSON data exchange formats are supported in the implemented communications.

Reasons of several proprietary solutions are derived by needs of demo partners' existing systems. Each of the system needs to be interfaced separately which diminishes common interoperability of platform. To resolve this barrier the existing systems should implement some common data structure standard.

By applying and implementing both standardized and some proprietary solutions, the Northern cluster has acquired necessary capability in cross-platform communications in the flexibility value-chain. Considering this, Northern cluster has achieved a fair level of interoperability in the developed flexibility platform software. Further proprietary systems can be interfaced with a reasonable effort.

The Northern cluster believes that the barriers to introducing more common solutions are mainly associated with internal motivations of the relevant stakeholders. All changes that require shifting to standardized solutions in the stakeholders' systems need resources that are always limited.

Table 4.8 - Cybersecurity, market algorithms and system operations used for the Northern cluster

UC ID	UC Name	Interfaces	Cybersecurity measures	Market Algorithms	System Operations
DSUC_NO_01	Preparation to flexibility trading	FSP-FR MO-FR FSP-FR SO-FR FSP-FR FR-T&D CP FR-FSP/SO/MO	HTTPS, Token-based authentication	PICLO(MO) and Nord Pool (MO) market operating systems, Fingrid (SO) and Elering (SO) balance management systems	Elering (SO) grid management system
DSUC_NO_02	Procurement and delivery support	MO-FR/T&D CP/SO T&D CP-FR T&D CP-FR FSP-FR FR-FSP/SO			None
DSUC_NO_03	Flexibility verification and settlement	MDR-FR FR-SO FR-ISR			Elering (SO) metering datahub, Flexibility register
DSUC_NO_04	Add New Product	SO-MO MO-FR			None
DSUC_NO_05	Procurement	FSP-MO			

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

		MO-T&D CP T&D CP-MO MO-FSP/FR/T&D CP FR-MO			-
DSUC_NO_06	Secondary trading	FSP-MO FSP-MO MO-T&D CP MO-FSP			None
DSUC_NO_07	Grid Qualification of Resource	CA-T&D CP FR-T&D CP SO-T&D CP T&D CP-SO T&D CP-FR MO-T&D CP			None
DSUC_NO_08	Bid Ranking and Optimisation	T&D CP-(EU)MO T&D CP-SO T&D CP-SO/MO		Intelligent bid selection based on required flexibility needs and provided bid offers.	Optimization module of T&D-CP
DSUC_NO_09	Bid Selection for Activation	T&D CP-SO/FR T&D CP-SO T&D CP-FSP		None	None

4.3 Horizontal WP: OneNet System

4.3.1 WP4 Integrated system operation for OneNet

The main objective of WP4 was to link the market activities with grid operation with the target to maximize the integration of FSPs. In this context, it explored the opportunities for using already existing models and tools for data exchange that were developed in previous H2020 research projects by carrying out a gap analysis of OneNet demo use cases both from a TSO and a DSO perspective.

From the analysis of OneNet demo use cases that focused on the data exchanges at TSO level, Table 4.9 shows the gaps and implementation requirements extracted:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Table 4.9 - Gaps and implementation requirements identified for the Western and Eastern clusters

Demo cluster	Gaps listed	Recommendations	Implementations requirements
Western cluster	Customized solution for data model is reported in the Western cluster use cases. There are missing details regarding the data model components and characteristics.	The use of CIM/CGMES is better option and recommended as a well-established standard data model, and that eases the interoperability of the solutions, however, currently there are Insufficient classes and attributes for business objects (Bos) for TSO-DSO data exchange in CIM/CGMES.	IEC 61970-301, CGMES: IEC 61970-600-1, and IEC 61970-600-2, should be extended in the future with respective classes and attributes to cover all TSO-DSO data exchange requirements.
Eastern cluster	Eastern cluster demo is intending to use CIM in the future. Currently no standardized data models are used. There is no information if the communication protocol is based on standardized format.	The use of CIM/CGMES is better option and recommended and this is in line with objective of the Eastern cluster, which is planning to adopt CIM/CGMES.	IEC 61970-301, CGMES: IEC 61970-600-1, and IEC 61970-48 EACL-PL-02, 04 should be used as a data model

From the analysis of OneNet demo use cases that focused on the data exchanges at DSO level, major gaps were identified in the harmonization and standardization, mainly because the markets for DSO ancillary services are so far only in the development (or early implementation) stage in most European countries, or non-existent at all. This is a stark difference to the TSO ancillary services market, which is effectively in mature state and in the process of pan-European harmonisation. DSO markets are also locally oriented and therefore requiring more often bespoke solutions adapted to local conditions. As a result, the incentives for harmonisation of applied solutions, as well as for wider-scale standardisation are limited.

The analysis also showed that communication protocols used are not defined per each interface between the different actors. One of the reasons for that is probably that households and other customers with lower technical capabilities are involved more often than in TSO operated markets.

The analysis indicated that both Czech demos use CIM XML. However, it was not clear whether standard profiles are used, or extensions were implemented. The Slovenian demo explicitly stated the need for extension of ESMP to DSO needs, e.g., non-frequency services. Another message was the insufficiency of available standards to cover all data exchanges, as on the national level in Slovenia. This is also in line with the Spanish and French demo experiences. Particularly interesting in that regard is the application of manual up- and downloads of messages. While data exchanges appear to be unified in Hungary, the need for standardization on a European level is given, which includes interfaces with the OneNet System. Eventually, some of these gaps, like unstandardized data exchange protocols and information models, could lead to a lack of coordination on the TSO-DSO level.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

As a consequence, task 4.3, which discusses customer-centred TSO-DSO interoperability and operation, but also presents the system-level perspective of TSO-DSO-customer coordination, the following conclusions were formulated:

- From the analysis of several H2020 projects, one can infer that there are various data exchange options; most of them have been developed in research and development projects. However, opportunities still exist to enhance the standardization of the data exchange processes. For example, some projects have already detected that there are EU-wide solutions without using the standards. Such characteristics do not allow the move of data exchange solutions across countries and extend business models to other countries. Furthermore, there is also reported limited interoperability among different vendors, leading to closed IT solutions' development. The experiences and lessons learned from different H2020 projects and other initiatives should contribute to defining a set of requirements for harmonizing data exchange solutions.
- The aggregation for flexibility services has been mainly focused on industrial loads. The number of aggregators working with residential consumers is small, corresponding to a barrier to market access for residential FSP. Such is a critical aspect for the electrical system to take advantage of the available flexibility provided by the residential sector.
- Another barrier concerns the communication requirements for smart FSPs to connect with other players. The communication requirements to participate in specific flexibility services are quite demanding, which also represents a barrier to the participation of small FSPs.
- From the analysis of H2020 projects, either already finished or under development, one can also notice that some projects do not consider all the roles, mainly the small FSP. This also affects the development of solutions for data exchange among different actors within the electric value chain and, consequently, the consumer's participation in the flexibility markets. Besides, this is also a limitation in understanding to what extent the small FSPs can be competitive in providing flexibility services.
- A set of standards has been proposed for data exchange across the electric sector through CIM. Several projects have highlighted that CIM has flexibility for proper data sharing, merging, and transformation into reusable information. It represents a common concept of controlling information for systems, applications, networks and services. Along with CIM IEC 61850 is another standard widely used in several projects to define communication between devices in the substation and related system requirements. Nevertheless, it has been pointed out that CIM needs to be extended for the distribution side.
- It is reported that CIM should be extended to adopt the aspects relevant to smaller DER (small FSPs). In particular, it is not widely addressed yet in the standards of the direct DER-SCADA communication between small DER of the prosumers, their aggregators and systems operators' SCADA.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

- A relevant aspect of the small FSP participation in the flexibility markets is the right to access own data and the ability to handle personal data. For instance, it is not addressed in the standards how to access meter day by the owners and by third parties through the data owners' consent. Hence, it has been recommended to cover the sharing access permission between data owners, other stakeholders, platforms, applications and data sources. Accordingly, more harmonization is required for the data aggregation and respective anonymization to ensure a secure and transparent data exchange.
- Data from consumers are mainly used for billing purposes. The data exchange interaction is mainly done from the consumers to the DSO. The consumers have difficulty understanding the difference between energy suppliers and DSO, which can be a barrier to deploying the flexibility markets. During the GRIFOn session, it was proposed to establish a single point of contact through better coordination and harmonized solutions between energy suppliers and DSOs. It was also highlighted the definition of the data management model in Europe is not completed, requiring an acceleration of that process, e.g., using data hubs like in Nordic countries.
- On the other hand, the smart meter rollout is lagging in some European countries. Consequently, it is necessary to review the regulatory framework to achieve high integration of smart meters in Europe to get the data that will be required for the different phases of flexibility services procurement.
- Requirements are also necessary for the standards to cover the market baseline calculations, bids selection and forecasting computation.
- Regarding regulatory questions, it becomes important to make clear the distribution costs due to the dissemination of the flexibility services and who pays for devices that are clearly needed to reach the decarbonization targets (e.g., smart meters, HEMS).
- Among the solutions addressed during the GRIFOn session, the following ones were highlighted: CIM data model for large FSP, OpenADR, SAREF, EEBUS and internally developed data models. Data models and ontologies for interaction with the consumer or flexibility provider are quite diverse, including tailor-made, vendor-made and not open-source solutions. This corresponds to a significant barrier to the interoperability of the TSO-DSO consumer [25].

4.3.2 WP5 Open IT Architecture for OneNet

WP5 set the basis for the establishment of the OneNet architecture and the implementation of the IT for OneNet, which is part of the work conducted within WP6. The main results and recommendations captured from this work package are summarized within this section, with focus on platforms and systems, interfaces, data, standards and cybersecurity, aiming in the end, to understand how and if the demonstrators are aligned with them.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

4.3.2.1 Platforms and systems

Main results and recommendations

The main results and recommendations gathered from WP5 are the following:

1. OneNet Network of Platforms focuses on the **integration of external platforms into the OneNet system**.
2. OneNet Connector is a specific instance of the OneNet Decentralized Middleware and will allow an **easy integration and cooperation among the platforms**, maintaining the data ownership and preserving access to the data sources.
3. The connector uses **REST APIs** (NGSI-LD) for the communication.

Demo analysis

The main system proposed within WP5 is of course the OneNet System, so from the demonstrators' side, it is important to assess whether the integration with the Connector is foreseen to capture the cross-platform interaction and replicability potential. And from this perspective, all the OneNet demonstrators will foresee the integration of their systems/platforms with the OneNet System, either directly in the scope of the demonstrator or also through regional use cases.

Also, not only does the connector resort to REST APIs for communication, but also several demonstrators choose this same approach, which is the case for the Portuguese, French, Greek and Northern demonstrators. Other approaches for communication reside in FTP (Greek), specific APIs and even OpenAPI (Northern).

4.3.2.2 Interfaces

Main results and recommendations

The main results and recommendations gathered from WP5 are the following:

1. "Cross-platform access" is fundamental for an interoperable ecosystem and entails that an application accesses services or resources (information or functions) from multiple platforms through the same interface.
2. Harmonization of multiple terminologies used to avoid redundancy and ensure singularity of roles assigned to cross-platform services.

Demo analysis

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The demonstrators make use of the cross-platform access provided by the OneNet system and of the cross-platform services included and fitting within the scope of each demonstrator. Harmonization of terminologies is something being widely addressed in the demonstrators, that make use either of standardized data models (CIM) or of custom-based data models to ensure this harmonization and ensure the data communicated is understandable from both sides.

4.3.2.3 Data and Standards

Main results and recommendations

The main results and recommendations gathered from WP5 are the following:

1. The OneNet harmonized semantics are based on **IEC CIM.**
2. Cross-platform integration and cooperation for market and network operation services is based on IDS reference model.
3. The **adoption of standardized data models** is fundamental for facilitating the interoperability and cooperation of different platforms and it plays a crucial role in the harmonization of formats and semantics that will be used by platforms both to consume and to publish data.
4. CIM will be key for efficient exchange between DSO and TSO SCADA systems for information on the current state of the network as well as with other distribution companies.

Demo analysis

There is big variation on the data models used throughout the OneNet demonstrators. The majority of the demonstrations opt for custom-based models that are fully crafted around the use cases developed. Nonetheless, some demonstrators resort to the CIM data model either fully, i.e., without adaptations, such as the demonstrators within the Eastern Cluster and the Northern Cluster, or an adapted version of the CIM data model, such as the French demonstrator, that is more fitted to the use cases' needs. The Northern Cluster has the particularity of using both CIM and custom-based data models, with the solution developed being able to communicate with systems that are implementing not only standardized but also proprietary IT systems.

4.3.2.4 Cybersecurity

Main results and recommendations

The main results and recommendations gathered from WP5 are the following:

1. It is important to integrate the requirement of data protection by design and by default.

2. Consent-based data processing is seen as the most appropriate approach since it allows the data subjects to make an informed decision.
3. Most relevant standards used to assure compliance with cyber security requirements are the NISTIR 7628 Smart Grid Cyber Security standard, SGIS Report, Open Web Application Security Project (OWASP), and Application Security Verification Standard (ASVS).
4. Cybersecurity measures adopted by partner companies: (a) Adoption of ISO/IEC 27019 standard; (b) Regulatory standards as a procedure to assess vulnerabilities in the organizations; (c) Training of employees; (d) Information on cyber threats from vendors, external consultants, media, associations and conferences; (e) Use of firewalls, antivirus, intrusion detection systems and anti-spam solutions for protection against attacks; (f) Security Information and Event Management, data loss prevention and safety endpoints.

Demo analysis

Most cybersecurity measures used by the OneNet demonstrators are aligned with usual practices from the entities, therefore, ensuring compliance of several of the measures under (4).

4.3.3 WP6 Reference IT Implementation for OneNet

The main goal of WP6 is to implement the OneNet architecture as it was developed and specified in WP5. the following section presents the main results extracted from WP6, with the focus on system and platforms, interfaces, data models, standards, and cybersecurity. Demo aspects of deployment of the OneNet solutions will also be presented.

System and platforms

The main results extracted from WP6 (more details about system and platforms can be found in D6.1 [31], D6.4 [33], D6.6 [34]):

- The OneNet System includes three main components: OneNet Decentralized Middleware, OneNet Orchestration Workbench and OneNet Monitoring and Analytics Dashboard.
- The OneNet Connector is a deployment instance of the OneNet Middleware and is a very important part of the OneNet System. It is responsible for the execution of the complete data exchange process, supporting the creation of the OneNet Network of Platforms.
- The OneNet Connector is based on IDS Reference model and FIWARE NGSI-API and each OneNet Participant can deploy and configure the OneNet Connector in its own system environment. Any external platform (participant) can be able to connect with the OneNet Middleware. In the OneNet Network of Platforms, which integrates external platforms, two participants can interact directly with each other, without intermediation by a third party.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Interfaces

The main results extracted from WP6 (more details about interfaces can be found in D6.1 [31], D6.4 [33]):

- The OneNet Connector can connect any kind of platforms using the REST APIs interface (NGSI-LD), so that participant can exchange harmonized data.
- The OneNet Orchestration Workbench interfaces itself with the OneNet Middleware (OneNet Connector) and offers a GUI and REST APIs to any OneNet Participants.
- OneNet Monitoring and Analytics Dashboard is the main GUI that allows access to OneNet Participants for monitoring and analytics of the data exchanges.

Data models and standards

The main results extracted from WP6 (more details about data models can be found in D6.1 [31], D6.3 [32]):

- Semantic interoperability is based on CIM data model.
- Data Integration & Homogenization sub-layer, as a part of OneNet Connector, manages the end-to-end data exchange process and provides a number of additional data-based services, directly at the connector layer.
- The OneNet Data Services Layer, which is part of the Data Integration & Homogenization sub-layer, includes a Data Homogenization tool, capable to integrate IEC 62325-451 entities with the FIWARE NGSI-LD information model, validate the entities and converting from XML or JSON formats into NGSI-LD valid format. All these functionalities are provided through standardized REST APIs interfaces and integrated within the OneNet Connector during the data offering provisioning.

Cybersecurity

The main results of WP6 are (more details about cybersecurity can be found in D6.6 [34]):

- Cybersecurity is one of the crucial aspects of an online, decentralized OneNet System. This involves securing sensitive information, protecting against unauthorized access or data breaches, fortifying the developed components against vulnerabilities, and ensuring the integrity and privacy of data generated by interactions and transactions throughout the OneNet Interoperable Network of platforms.
- Due to the nature of the project, the requirements provided in NISTR 7628 standard were selected as the most relevant cybersecurity guidelines to be considered and applied during the implementation of the OneNet project.
- The OneNet Decentralized Middleware is the key component of the OneNet Interoperable Network of Platforms since it enables the process of managing and sharing information in a controlled and administrative environment, dealing with the user management, central meta-data brokerage and the logging of all occurring transactions for auditing reasons. This framework does not have access to the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

data shared by the OneNet participants, nor does it forward or process such data. The owners of the data have total control of the sovereignty of their data.

- The OneNet Workbench, which is a web-based platform, is accessible through browser only for OneNet Participants, and the access control is completely integrated with the OneNet Identity Management, ensuring a centralized access management in the overall system.
- OneNet Monitoring and Analytics Dashboard employs an identity server such as Keycloak for the purpose of managing authentication and authorization to the OneNet system.
- Every user accessing the system is uniquely identified and verified. Identification and authentication mechanisms are centralized in the OneNet Connector and Decentralized Middleware, ensuring a unique identification and authorization mechanism for the whole OneNet system. Username and password (with strong password) are used for the UI access and Oauth Token are used for REST APIs authentication.

Demo aspect

From the analysis of OneNet demos, focused on the data models, standards, interfaces, and cybersecurity, we can identify that not all demos adopted CIM as a data model. Some of them are using custom-based data models. The analysis also showed that demonstrators are relying on REST APIs interface to connect with OneNet System. We can find also other approaches like FTP and specific REST APIs.

Regarding the cybersecurity measures demonstrators are using HTTPs and Firewall IP rules. Regarding the authentication measured some demos adopted Token-based authentication tools and specific digital authentications. Specific for the French demo is that they are using blockchain technology.

More details can be found in sections 4.2 and 5.1.2.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

5 Harmonization of Common and Proprietary Solutions

5.1 Common and proprietary solutions

When it comes to the actual deployment of the OneNet solutions, the choices often boil down to common or proprietary solutions, both having significant impact in the operation and scalability of the project. Hence, understanding these terms and their implications, together with identifying the adoption rate by the OneNet demonstrators is vital to understand their replicability potential and the barriers hindering that same replication and scalability.

Therefore, this sub-chapter is structured in the following way: first, main definitions are given to each of the options, as well the main benefits and drawbacks gathered from literature; second, a distinction between the common and proprietary solutions adopted by the OneNet demonstrators is done, to understand main tendencies and types of solutions that normally fit under each category; third and last, we derive main conclusions and learnings from this sub-chapter, which will be further explored in section 5.2, namely the reasoning behind these choices.

5.1.1 Main definitions and comparison between options

In a first stage, it is important to have a clear knowledge on the distinction between each solution categories, being common and proprietary solutions, how they differ from one another and what are the intrinsic benefits and drawbacks to each of them, that will certainly have a reflection on the adoption rate by each of the demos, which will be explored afterwards.

Open or common solutions can be defined as solutions that are not only available and accessible to everyone and are not owned or controlled by one single entity, but are also standardised and not tailor-made to a specific purpose. They can be either: i) Project/community open source, which are developed and managed by a community of developers that improve and support the source code at zero cost for the users; or, ii) Commercial Open-Source Software (COSS), where a single entity has control of the full copyright, patents, and trademarks, who also distributes the software for free or for a fee[3] . They generally offer a high degree of flexibility, allowing users to modify and customize them according to their specific needs, thus increasing their replicability potential.

Well-known examples of these are Linux and MySQL, which are both applied in many industries due to their high adaptability, robustness, and cost-effectiveness. More specific to the energy sector and thus, more related

[3] open-source-vs-proprietary-software-pros-and-cons.pdf (optimusinfo.com)

to the OneNet project, are solutions such as the CIM data model, which can provide a consistent definition and format for the data, so it can be used across different applications, even if developed by different manufacturers or vendors. One of the main advantages of these types of solutions is of course their high degree of scalability, being also generally less costly and time-consuming to integrate.

Private solutions, in this document referred to as **proprietary**, on the other hand, are owned and controlled by a specific organization, which holds the exclusive legal rights to the solution, and they normally include access restrictions and address specific needs of that same organisation. Examples of proprietary solutions can be Microsoft's Windows and Apple's iOS, and within the energy sector we can highlight specific tools for system operation (e.g., forecast tools) that are exclusive to a specific SO. These proprietary solutions are normally tailored, with cohesive user interfaces and features that often come with an associated cost, including the support and future updates from the parent company. Furthermore, because these solutions are crafted with a specific purpose in mind, they may offer unique features or superior integration with certain systems compared to common "open-source" alternatives. Note that a solution that originates from an open-source element can still be considered as proprietary if the solution is significantly adapted to fit the users' needs.

Thus, understanding the benefits and drawbacks of each of them is important, which are presented in Table 5.1.

Table 5.1 - Summary of main benefits and drawbacks from common and proprietary solutions[4]

	Benefits	Drawbacks
Common solutions	• **Cost-Effectiveness:** Since community open-source solutions are free to download (including the source code), they can significantly reduce costs. COSS normally have a fee, but a free version is also normally available. • **Flexibility:** Users have the freedom to modify and customize the solutions to meet their specific needs, providing an unparalleled level of adaptability, which can accelerate innovation.	• **Limited Customer Support:** They often lack dedicated customer support. This means users must rely on community support (documentation, tools, support systems), which may not always provide timely or precise solutions. • **Compatibility Issues:** These solutions may have compatibility issues with other software or hardware, particularly if they're highly customized.

[4] open-source-vs-proprietary-software-pros-and-cons.pdf (optimusinfo.com)

Open Source vs. Proprietary: Key Differences [2023] | Nexcess

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

	• **Community Support:** They often come with a large and active community of users and developers who can provide support to potential problems. • **Interoperability:** Common solutions normally adhere to open standards concerning communication protocols and data formats, which is meaningful to improved interoperability of solutions. • **Avoids vendor lock-in:** With exception of the COSS solutions, community open-source solutions don't rely on a single vendor for continued improvements, maintenance, and support.	• **Limited usability:** These solutions are not tailor made and are generally not aimed at unskilled end-users, which won't be able to adapt the source code to meet the organisation needs. • **Security Concerns:** Although not always the case, some open-source solutions might have more vulnerabilities due to their public nature, which could be exploited by malicious users.
Proprietary solutions	• **Dedicated Support:** Proprietary solutions often come with a dedicated support team that can quickly and efficiently address any issues or concerns. • **Quality and Reliability:** Being more targeted and developed by professional teams, they are normally of higher-quality and more reliable. They often undergo extensive testing before release. • **Ease of use:** Being more targeted on a narrower market of end-users they are easy-to-use and understand. • **Less Compatibility Issues:** Since these solutions are professionally developed, they are often designed to work well with a wide range of other software and hardware.	• **Cost:** Proprietary solutions can be expensive. When developed by a company that is not the final user, they often require an upfront purchase or a recurring subscription fee. • **Lack of Flexibility:** Unlike open-source solutions, proprietary software doesn't allow for customization. Users must use the solution as it is provided. • **Vendor Lock-in:** Relying on these solutions can lead to vendor lock-in, where a user becomes dependent on a vendor for products and services. This can make it difficult to switch to another solution if needed. • **Software opacity:** The source code is normally closed for viewing and editing, making the users unable to debug the issues effectively, constantly depending

		on the developer and on the priority of the request.

Thus, when deciding between common and proprietary solutions, it is important to consider several factors, namely, the initial and ongoing costs, the degree of customization needed, the technical expertise within the organization, the importance of dedicated support, and degree of integration with existing systems. These were certainly aspects considered in the decision making from the demos, to allow an effective deployment and exploitation of the solutions demonstrated. Understanding the reasoning for these choices can give us further input concerning potential barriers and limitations from these types of solutions, so that recommendations can be drafted in the end.

5.1.2 Approach taken by OneNet demonstrators

Having understood the distinction between each solution category, we are now at the stage of linking the solutions implemented throughout the demos that have been disclosed under Chapter 4.2 with these categories, in order to, in a later stage, understand the reasons behind these choices, so that recommendations can be built around it. This categorisation can be found in Table 5.2. Note that this analysis is carried out for the different components evaluated under Chapter 4.2, namely regarding the data exchange, data models, the communication protocols, data exchange formats, cybersecurity measures, market algorithms and system operations. Note that the "Interfaces" component has been dropped out of this analysis since it only referred to the actual interactions and flow of information (e.g., DSO-TSO), which can't be characterised neither by common nor proprietary.

Table 5.2 - Common and proprietary solutions from the OneNet demonstrators

Component	Implemented in the demos	Demos adopting	Common (incl. open) vs Proprietary
Exchanged data	The following types of data are used: • Market data: Prequalification results, Auction data, Market results, Settlement data • Resource data: FSP data, Technical and location attributes, Metering data, Flexibility potential	ALL	Proprietary (i.e., with restrictions/limited access, can be made open if aggregated, anonymized and/or based on consent)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

	• Operational and planning data: Maintenance plans, Flexibility needs, Consumption and generation forecasts, short-circuit contributions, Estimated curtailed energy, Real-time data on operational conditions, System operation historical data		
Data models	ENTSO-E outage planning coordination model; CIM; ISO8601; ESMP (IEC 62325-503)	FR, SL, CZ, NO	Common
	Custom-based (i.e., tailor-made models)	NO, CY, GR, PT, ES	Proprietary
Communication protocols	IEEE C37.118; Modbus TCP; HTTPs; FTP; MQTT; AMQP; OpenAPI 3.0; SMTP; GMS; REST APIs	ES, CY, GR, SL, PL, NO, PT, FR, CZ	Common
Data exchange formats	JSON, XML, CSV, NETCDF	ALL	Common
Cybersecurity measures	HTTPS; TLS encryption; SCRAM-SHA 512; OIDC; Firewall IP rules	PT, ES, FR, CY, SL, NO	Common
	Token-based authentication tools, specific digital authentications; two-factor authentication	PT, ES, FR, SL, CZ, NO	Proprietary
Market algorithms	Market optimization tools/algorithms; Flexibility needs assessment	CY, GR, HU, NO, ES	Proprietary
	Flexibility needs assessment	NO	Not classifiable
System operations	Technical coordination platforms, e.g. Flexibility Register; SOs tools, e.g., flexibility needs assessment, operational planning, forecast,	PT, ES, FR, CY, GR, NO	Proprietary

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

	energy not served; Local Market platforms		
	Shared ledger for RES curtailment management (STAR), OneNet System[5]	FR, CY, GR	Common

Reflecting this categorisation and mapping of the OneNet solutions, Figure 5.1 portrays the number of common and proprietary solutions used by the OneNet demonstrators, for each group of data category.

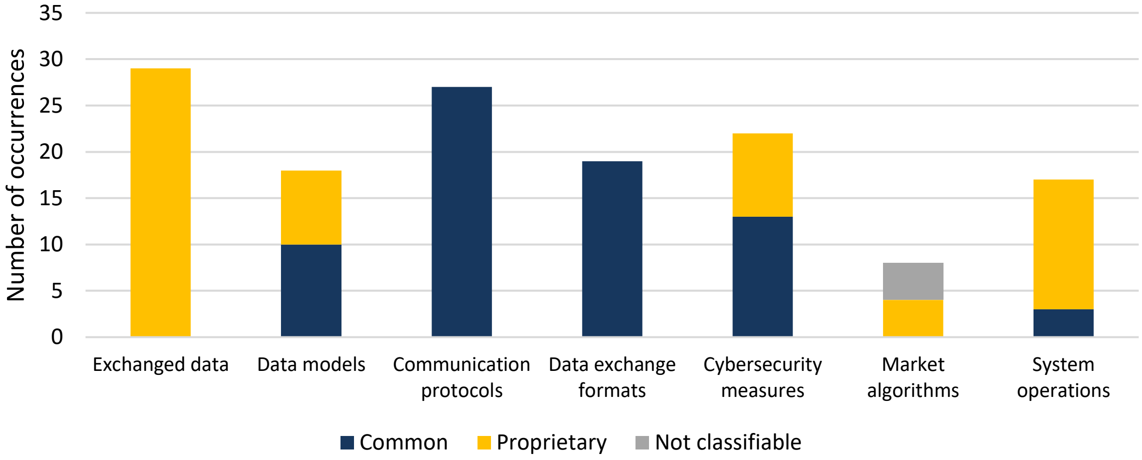

Figure 5.1 - Total number of common and proprietary solutions used by the OneNet demonstrators, grouped by data category

In accordance with Table 5.2, all the Exchanged data and Market algorithms solutions used by the different demos are classified as proprietary. In the case of the Exchanged data category, three sub-categories were identified: market data, resource data, operational and planning data. It is expected that more than one category is needed for the purpose of the demonstrators, thus increasing the overall number of occurrences in comparison to the other categories, making the Exchanged data category the one with the largest number of proprietary solutions. Note, however, that for this category, the proprietary categorization was determined in cases where there are restrictions in data access, meaning the data can't be completely open source unless anonymized, aggregated, or based on consent. These restrictions are not necessarily related to the willingness of the parties to share the data but can also be related to privacy reasons. As for the market algorithms, since the majority is built to fit not only the specific purpose of the demonstrator but also the country's reality, they

[5] In this case, the OneNet system is applied only for system operation, in other demos the OneNet system is being applied also for market processes.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

are mainly marked as proprietary. However, there are certain cases, such as the Northern Cluster demos, where it is too early to say whether it can be defined as proprietary or common. This is due to the fact that these algorithms are already applied in four countries. Therefore, it is commonly used even if making it open source depends mostly on the willingness of the development partner.

On the opposite side, both Data exchange formats and communication protocols categories have only common solutions identified, also as mentioned in Table 5.2, showing that, for the purpose of the OneNet demonstrators, there was no need to adopt any proprietary data formats or existing protocols, which are typically owned and controlled by specific organizations or companies.

In the remaining four categories both common and proprietary solutions were identified. Generally, for Data models and Cybersecurity measures, the common solutions are more widely adopted, whereas for the System operations, OneNet demos mainly opt for proprietary solutions. This also proves that, similarly to the market algorithms, solutions that tend to be more specific to the environment/country where they are deployed tend to be proprietary, which is the case for the system operations solutions, where the used tools have built-in features to fit the needs of the user.

Figure 5.2 to Figure 5.5 following figures present the number of common and proprietary solutions, by category, used for each cluster.

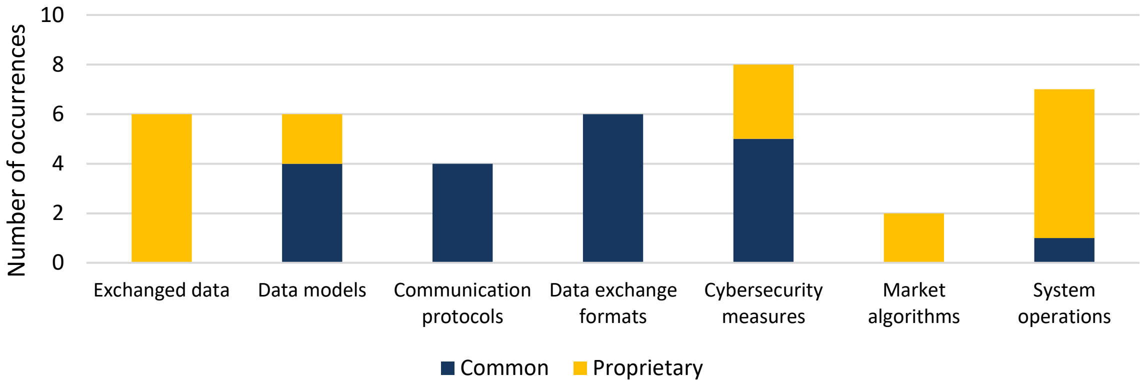

Figure 5.2 - Number of common and proprietary solutions used by the Western cluster, grouped by category

Figure 5.2 also shows that only common solutions are used for Data exchange formats and communication protocols, where common standardized solutions such as RESTful APIs are used. On the other hand, only proprietary solutions were adopted for Exchanged data, following the same reasoning that the data exchanged requires some sort of anonymization, aggregation or consent to be shared, since it contains private and/or confidential information. Since the Spanish demo integrates a market, it is the only demo from the Western Cluster resorting to market algorithms.

In what concerns the System operations, the Western cluster follows a similar tendency to the one presented in Figure 5.1, by having a higher representation of proprietary solutions. This is due to the usage of technical coordination platforms and SO tools that are used by all the demos in the cluster. Only France uses a common solution on this category, which is the STAR platform.

Regarding Cybersecurity measures adopted, the Western cluster shows a higher occurrence of common solutions. Nonetheless, Portugal and France use Token-based authentication tools, whereas Spain uses a Digital certificate authentication provided by OMIE, which consist of proprietary solutions.

Although the majority of the used data models are common, Portugal uses a proprietary one, which is a custom-based data model. However, it is important to highlight that although being tailor made, the data model was completely adapted from a common and open language and is made accessible to third parties [21].This can indeed be regarded as a sub-category from the proprietary one, i.e., proprietary and open source.

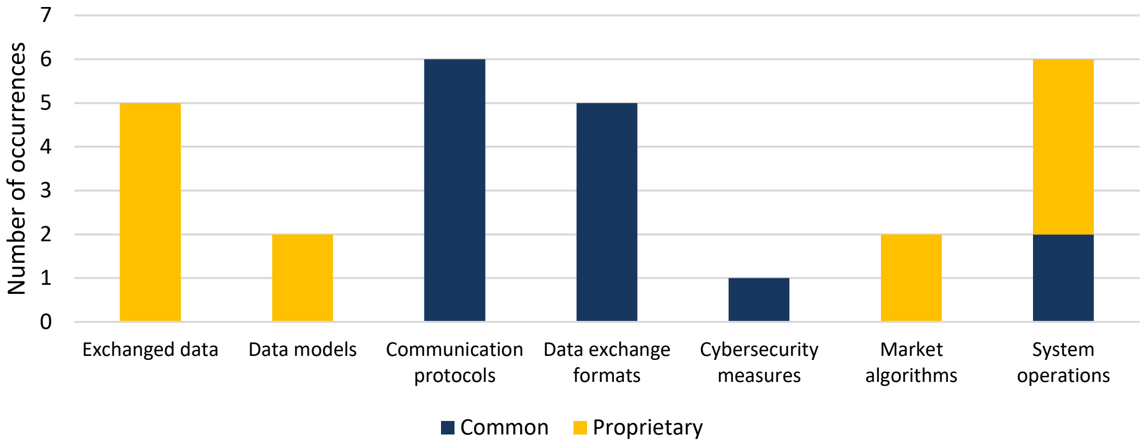

Figure 5.3 - Number of common and proprietary solutions used by the Southern cluster, grouped by data category

When looking at Figure 5.3, the first thing catching attention is the reduced number of Data models and Cybersecurity measures used. Regarding Data models, both Greece and Cyprus use a single custom-based data model, that is considered to be a proprietary solution.

Concerning Cybersecurity measures, it was curious to notice that in most of its SUCs, the Cypriot demo has not seen the need to adopt any measures, because a Digital Twin was being used, already comprising a good level of cybersecurity. The Greek demo has used Requested User login and password hashing to use F-channel platform, which is not classifiable as common or proprietary, as it is more a built-in feature.

The number of common and proprietary solutions adopted for the Exchanged data and Data exchange formats, respectively, are aligned with the trend presented in Figure 5.1 for all the clusters, with Exchanged data being fully private and Data exchange formats fully open. The same can be seen for the number of common and

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

proprietary solutions adopted for Communication protocols. Both the Cypriot and Greek demos make use of REST APIs, which are based on the RESTful common architecture.

Each one of the demos uses one market algorithm for assessing the flexibility needs, which is a unique feature of the Southern cluster, according to the answers provided by the demo leaders.

Finally, when it comes to the system operations, the Southern cluster is the only one that declared to use the OneNet System for that purpose, which is a common solution, used for both its demos. Apart from that, this cluster makes use of some proprietary solutions for its system operations, as well, similarly to what was verified for the Western cluster.

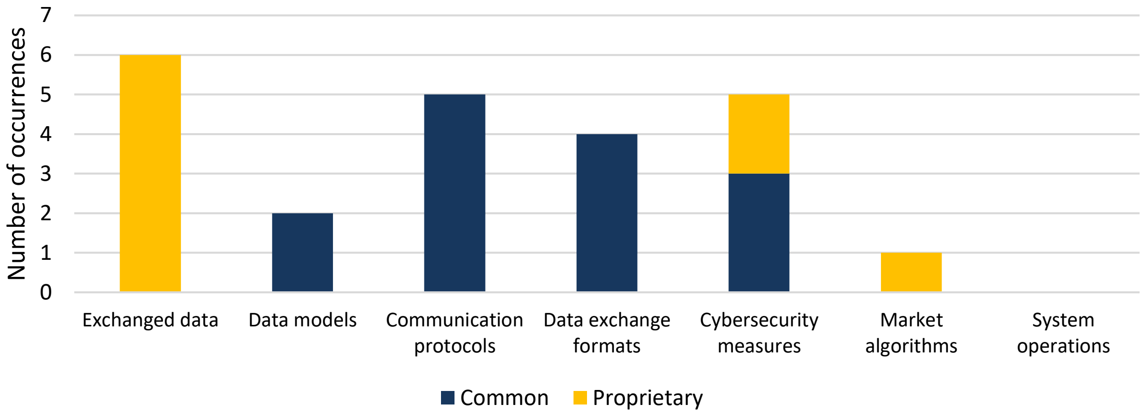

Figure 5.4 - Number of common and proprietary solutions used by the Eastern cluster, grouped by data category

Figure 5.4 illustrates that, for three categories, the Eastern cluster has only used common solutions. Concerning Data exchange formats, it is in line with Figure 5.1, but when it comes to Data models, it is the only cluster that does not use any Custom-based data models, thus being the unique that does not adopt proprietary solutions on this data category. As for the Communication protocols, apart from the RESTful APIs used by Czech demo, other common solutions are used, such as HTTP, MQTT, SMTP and GMS. Regarding Cybersecurity measures, one type of proprietary solution is used: Token-based authentication tools. In addition, three other common solutions were adopted by the Eastern cluster, similarly to what was verified in other clusters.

Apart from the Southern cluster demos, the Hungarian demo was the only one using a Market algorithm, for optimization purposes. Finally, no specific tools for system operations were reported to have been used in this cluster.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

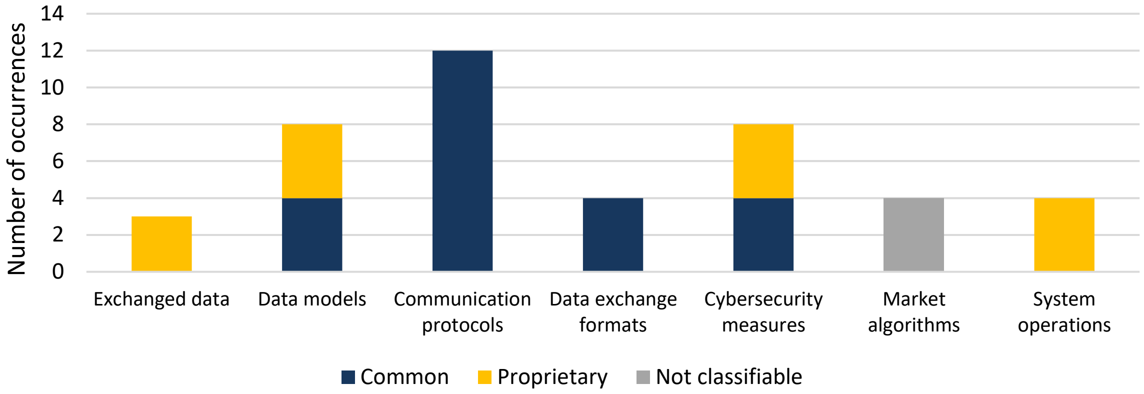

Figure 5.5 - Number of common and proprietary solutions used by the Northern cluster, grouped by data category

Since the Northern cluster represents four country-specific demos, i.e., Finland, Estonia, Lithuania and Latvia, all demonstrating the complete end-to-end process of market-based flexibility uptake by TSO-DSO pairs following a same approach, the number of occurrences is indeed high, resulting from the replicability of the implemented solutions throughout the demonstrators. The usage of common versus proprietary solutions is split in half for the data models category. Apart from resorting to CIM, the Northern cluster uses a MO-specific data model, that can be regarded as a custom-based solution, that will vary between market operators.

Concerning cybersecurity, while the majority of the demos have adopted more common than proprietary solutions, each Northern demonstrators have adopted one common and one proprietary solution: HTTPS and token-based authentication tools, respectively. As for market algorithms, since the ones used are already applied in four countries, it is still too early to say whether it can be defined as proprietary or common, as making them open source depends mostly on the willingness of the development partner.

Regarding Data models and Data exchange formats, all the SUCs used CIM and JSON, respectively, which consist of common solutions. A REST API was used as a communication protocol, apart from three other common solutions adopted for this category. Finally, all three of the Data exchange categories were used within the Northern cluster, thus including market data, resource data and operational and planning data.

5.1.3 Main reflections from adoption of common and proprietary solutions

As described in section 5.1.1, Common solutions are accessible to everyone and not controlled by a single entity. They can be project/community open source or Commercial Open-Source Software (COSS). Some examples include Linux, MySQL, and the CIM data model. Usually, these solutions offer flexibility, scalability, and allow for a higher level of interoperability among different systems.

On the other hand, proprietary solutions are owned and controlled by specific organizations with exclusive rights. Some examples are Microsoft's Windows and Apple's iOS. Proprietary solutions offer tailored

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

features and better integration with specific systems compared to open-source alternatives but may come with associated costs and lack of flexibility.

By gathering the answers to the questionnaires provided by the OneNet demonstrators, presented in section 4, it was possible to map the common and proprietary solutions adopted, by each type of category, as can be seen in Table 5.2. Subsequently, a statistical analysis was performed, as shown in Figure 5.1 to Figure 5.5, in order to understand the tendencies and choices of each cluster, when it comes to adopting Common and/or Proprietary solutions.

It was clear that, depending on the data category, the occurrence of common and proprietary solutions used by the OneNet demonstrators was significantly different. For example, Exchange data category only comprises proprietary solutions, given that, not only all the data exchanged is very specific and unique for each demo, but it also has some degree of privacy and/or confidentiality that requires anonymization, aggregation or consent for it to be shared, thus having limited access. This is also the case for the Market algorithms used for the different demos, that are generally customized for the purpose of the use cases and to fit the different operational realities. On the other side of the coin, the Data Exchange formats are all made of common solutions, which is a good indicator for interoperability within the different SUCs among the different demos and clusters. The same happens with the Communication protocols, which fully consist of common and standardized solutions, such as RESTful APIs.

Regarding the Data models used by the OneNet demonstrators, they are almost evenly split between common and proprietary, with a slightly higher weight from the common solutions. The proprietary solutions are especially custom-based models that are made adaptable to the demos' reality. Nonetheless, it's important to highlight that these are constructed based on an open-source environment some are even made accessible to third parties.

When it comes to the implementation of Cybersecurity measures or System operations, there are both Common solutions and Proprietary solutions. Thus, it might be interesting to understand the differences between them and the main reasons for the demo partners to have used Proprietary solutions, instead of Common solutions and in what terms does that affect interoperability.

In what concerns Cybersecurity measures adopted, the most common proprietary solution are Token-based authentication tools, that are used by three demos. Spain makes use of a Digital certificate authentication provided by OMIE, which is also a proprietary solution.

Finally, when considering System operations, only two types of Common solutions were identified by the demos' answers: STAR platform, used by the French demo and the OneNet System, adopted by the Cypriot and Greek demos. It might be interesting to see how these types of Common solutions could be used in other demos, as well, specially the OneNet System, that was created within OneNet project and should, ideally, provide interoperable solutions, possible to use in several clusters.

5.2 Barriers and limitations

In the following paragraphs, the reasons for the choice of the demos to deploy common or proprietary solutions are analysed to understand the main barriers and limitations for the comprehensive deployment of common solutions and to formulate recommendations for the harmonization of data exchange solutions.

5.2.1 Proprietary solutions

From section 5.1, we were able to see that proprietary solutions are the most chosen option when speaking about exchanged data, market algorithms and system operations (Figure 5.1). To better understand the rationale behind this choice a consultation moment was done with OneNet demonstrators, to understand their opinion on two open questions: *(1) What are the reasons for opting for proprietary solutions in the demo? (2) How do you see that opting for proprietary solutions would affect interoperability of the developments?* Below, a discussion around each of these questions, with opinions gathered from the demonstrators is presented.

(1) What are the reasons for opting for proprietary solutions in the demo?

Similarly, as done in previous sections, the analysis will be segmented into the different demonstration clusters, also considering the difference in scope between them.

Western cluster

Before diving into the analysis, it is important to recall the options taken by the Western cluster in what regards to common and proprietary solutions. Both the exchanged data, the communication protocols and the system operations are majorly addressed by proprietary solutions, while categories such as the data models, the data exchange formats, and cyber security measures are mostly common. On this note, it’s important to highlight the scope of the cluster, that is more related to the technical coordination between system operators, instead of flexibility markets development, which is only the case of the Spanish demo.

Answering to the question itself, the **Portuguese demonstration**, which has a core focus on the operational planning of the electricity network, points out several reasons for this choice such as the fact that proprietary solutions are built with additional layers of security, thus, being able to guarantee resilience and security of the overall system. Also, these solutions are tailor made, making them easier to use and more compatible with the internal systems of the network operators. Having access to dedicated and timely support is also an important aspect, especially when considering critical infrastructures, where promptness of response is vital. One final argument is related to the associated costs. In fact, what could initially be thought to be the most expensive option, proprietary solutions can be cheaper if the organisation requiring the solutions has resources with

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

technical expertise to build the solutions, instead of using an open-source solution that requires several adaptations to fit the needs of the user.

As for the **Spanish demonstration**, it differs significantly in scope in comparison to the Portuguese demonstration, as it develops a flexibility market platform. Nonetheless, also from the demo perspective, opting for proprietary solutions enables an easier process for the Iberian market participants, creating services and procedures as similar as possible to the systems that are currently in production and at the same time try to avoid entry barriers (i.e., avoiding new developments for participants). That is why communication protocols, proprietary certificates and other proprietary solutions have been adapted.

The **French demonstration** has a strong focus on the STAR platform, which is used to simplify and optimize the management of renewable production curtailments. The whole platform source code will be open source and is based on open source blockchain technology, being one of the very few common solutions used for the System operations category. A specific REST API is used as a communication protocol because a project of the STAR platform done a few years ago implemented these APIs and proved to interact efficiently with the HyperLedgerFabric blockchain so it continued being used. This was the recommended option by the development team regarding the optimization of the blockchain platform's performance which was French demo's main concern. As a cybersecurity measure, the French demo has adopted a token-based authentication, which is relevant for a decentralized permissioned blockchain and enables to give different reading and posting rights among participants.

Southern cluster

In the case of the **Cyprus demo**, they mostly resort to proprietary solutions in the demo since they have implemented new market frameworks from the ground up, which could not be implemented using common solutions. Furthermore, different tools were accommodated in the two platforms, such as grid monitoring and coordination of flexible resources, a research work carried out in University of Cyprus (UCY), that was also implemented from zero. The proprietary solutions in the Cyprus demo provided more flexibility to demonstrate the scenarios, and since the demo is built in a simulation framework, the goal was to prepare solutions associated with the hardware in the loop environment that has been created for the demo. Hence, the main reason for opting for proprietary solutions falls to technical reasons.

As for the **Greek demo**, the reasons for opting for proprietary solutions instead of common ones are related to the technical nature of the platform, which indicated that a custom-tailored platform needed to be made to include all the aspects aimed for within the platform. This tailor-made creation could not be done by using the open source pre-made solutions. Apart from that, maximum levels of data security and confidentiality were aimed for, hence the partners opted to go forward with solutions that were sure to fit those criteria.

Eastern cluster

The **Hungarian demonstrator** has identified that generally proprietary solutions are easier to implement since the nature of cloud-based existing services that can be utilized is very well-defined. The platform works within the ecosystem of the DSO, hence the proprietary solutions fit into that IT ecosystem.

The **Czech demonstrator** has implemented proprietary solutions due to the creation of a "traffic light scheme", which was, then, incorporated into real operation. To this end, there was a need for more robust and reliable tools in terms of grid operation and cybersecurity. The second phase of the demonstration project consisted of a platform for non-frequency services, which occurred only for testing purposes (and immediately after the test the platform was dissolved). Therefore, a less extensive approach was implemented.

<u>Northern cluster</u>

The NOCL uses proprietary data models for some use cases, depending on the existing internal IT systems of the different stakeholders. As an example, the market operator Nord Pool has its existing proprietary communication data model and changing it was neither in the scope of the project nor the objective of the Nord Pool itself. Similarly, the TSO Elering has existing IT system, however supporting standard CIM communication. Based on this, the flexibility platform software solution created during the project was able to utilize the existing system operator IT system. In a nutshell, Northern cluster solution developed the capability to demonstrate flexibility use cases for communicating with platforms that are implementing not only standardized but also proprietary IT systems. However, preference would be to use standardized CIM format whenever it is possible.

The reasons for several proprietary solutions are derived from the needs of demo partners' existing systems. Each of the systems needs to be interfaced separately which diminishes common interoperability of the platform. To resolve this barrier the existing systems should implement some common data structure standard.

(2) How do you see that opting for proprietary solutions would affect interoperability of the developments?

Similarly, as done in previous sections, the analysis will be segmented into the different demonstration clusters, also considering the difference in scope between them.

<u>Western cluster</u>

From the **Portuguese demonstration** perspective, some of the use cases are in fact based on open standards, which is the case for the ENTSO-E outage planning coordination model, although incorporating some adaptations, with the remaining being custom-based. This can indeed affect interoperability, as the standards used are not open, however, opting for proprietary solutions allows for higher security and resilience, which is core for SOs activities, especially taking into account the scope of the demonstration, that is targeting the technical coordination between TSO-DSO for operational planning.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Regarding the **Spanish demonstration**, they refer that their systems and procedures are already interoperable with other NEMOs and standardized protocols since they are interconnected with Europe since 2014 for the Price Coupling of Regions (PCR) project and 2018 for the Cross-Border Intraday (XBID) project [27]. One of the main interests was to create new markets that can be integrated with existing ones. Although the market solutions may be proprietary, they are ready to share standardized information using common methods.

Concerning the **French demonstration**, since the code of the STAR platform is open source and the objects exchanged in the REST APIs are described by a data model relying on CIM standards, interoperability might be ensured. Nonetheless, the interoperability may be limited by the blockchain architecture itself, since although accessing the platform is possible for new producers, it has been designed to give access to one TSO and one DSO.

Southern cluster

For the **Greek demonstration**, when it comes to the system operations, they claim the interoperability of the solution would not be affected by using the proprietary solutions, since the modifications from the common tools were relatively minor and would be simple to make in order to fit any system or situation where the platform could be used. In fact, it would make the interoperability even easier, as the changes were made in cooperation with the system operator, so the platform could fit their needs even more than the commonly used tools.

When it comes to the **Cypriot demonstration**, the adoption of proprietary solutions might impact interoperability with other common solutions. However, this is not a major issue since middleware components can be used to achieve the interoperability with common solutions. These middleware components can be easily developed by knowing the input/output requirements (such as data format, data type) in order to achieve the seamless communication of the developed proprietary solutions with the common solutions.

Eastern cluster

As for the **Hungarian demonstrator**, since there are no M2M communications outside of the DSO's system, it is hard to make a case for interoperability issues arising from the proprietary solutions.

Northern cluster

By applying and implementing both common and some proprietary solutions, the Northern cluster has acquired necessary capability in cross-platform communications in the flexibility value-chain. Considering this, Northern cluster has achieved a fair level of interoperability in the developed coordination platform software. Further proprietary systems can be interfaced with a reasonable effort.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

5.2.2 Common solutions

In this section, we aim to determine what hinders demonstrators from adopting common solutions. Similarly, as in previous subsection the demonstrators were asked to identify the possible barriers for applying common solutions in their demos. Below, the answers gathered from the demonstrators are presented. The results are segmented into the different demonstration clusters.

<u>**Western cluster**</u>

As for the **Spanish demo**, the reasons for not adopting common solutions are related to the technical nature. They point out that the principal barrier could be for participants who probably would have two different solutions to participate in electricity markets coexisting at the same time. From the demo perspective, also the propriety solutions are more adaptable to the systems that are currently in use.

For the **Portuguese demo**, applying more proprietary solutions instead of common ones can bring more benefits. They point out several technical reasons for this choice such as that common solutions are not tailor-made, making them not so user friendly and less compatible with the user's internal systems. Also, these solutions might have more vulnerabilities which lead to the resilience and security issues. Additionally, they often lack dedicated and timely support and mostly rely on the community support, which may not always provide accurate and timely solutions.

From the **French demo** perspective, they don't see any barriers to adopt common solutions. They point out only one technical reason that could be considered as a barrier that could have some impact on the STAR platform performance. The latter is based on open source blockchain technology and could be challenging to adapt to ensure the privacy of commercially sensitive data.

<u>**Southern cluster**</u>

In the case of **Cyprus demo**, they refer that the technical particularities of the simulation framework prevent their demo to adopt common solutions. The non-existence of an established regulatory framework for provision of ancillary services by distributed energy resources in the country, as well as the non-existence of an established market, which is currently under development, are also reasons for opting proprietary solutions instead of common ones.

Similar to the Cyprus demo, the **Greek demo** also points out that the technical nature of the platform indicated that the custom-tailored platform needed to be made in order to include all the aspects that they wanted to use within the platform, which can't be done by using common solutions. The desired maximal level of data security and confidentiality is another reason for not opting common solutions. They also identified some barriers from the point of current situation and legislation in the country, like the lack of regulation regarding a flexibility market operation, non-existence flexibility market, lack of submetering regulatory framework as reasons for not adopting common solutions.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Eastern cluster

Regarding the **Hungarian demo**, no barriers for applying common solutions existed.

The **Czech demo** has identified the lack of regulation regarding the flexibility market as a possible reason for not using the common solutions. They also point out that there is an ongoing debate concerning national framework for the flexibility market. The framework covers all types of services and must be convenient for all market participants, notably aggregators and network operators. Until the debate is concluded, they currently can't foresee which approach will be adopted at the national level.

Northern cluster

From the Northern cluster perspective, introducing more common solutions are mainly associated with internal motivations of the relevant stakeholders. The common solutions are not tailored made and may have compatibility issues with other software or hardware. All changes that require shifting to common solutions in the stakeholders' systems need resources that are always limited.

5.2.3 Barriers and limitations of common and proprietary solutions

To understand the reasons behind the demonstrators' choices on common and proprietary solutions and to understand what barriers and limitations exist for implementing more common solutions, demonstrators were asked to provide their opinion on three questions, which answers were then segmented into the different demonstration cluster.

1. *What are the reasons for opting for proprietary solutions in the demo?*
2. *How do you see that opting for proprietary solutions would affect interoperability of the development?*
3. *What are the main barriers for adopting more common solutions?*

Based on the answers of the demonstrators, it's clear that the **technology** is the most significant reason for adopting proprietary solutions instead of common ones. As for the Spanish demo, opting for proprietary solutions is related to their flexibility platform. These solutions are more adaptable to the systems that are currently in use, while avoiding new developments for participants. Similar to the Spanish demo, also the Portuguese demo and the Northern cluster pointed out that proprietary solutions are tailored made, making them easier to use and easier to implement, since they are more compatible with their internal software and hardware. Dedicated and timely support, which can quickly and efficiently address any issues or concerns is also an important reason.

In the case of Southern cluster, both demonstrators refer that technical particularities of their simulation framework and platform, which are custom made, prevent them to adopt common solutions.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Unlike other demonstrators in Western cluster, the French demo refers that they don't see any barriers to adopt common solutions. Their platform STAR, which is based on open-source technology, is one of the very few common solutions. They also specify that platform STAR is using specific REST API, which is proprietary solutions, as a communication protocol.

Analysis of demonstrators' responses revealed that **cybersecurity** is also a significant barrier. The desired maximal level of data security and confidentiality is very important, and this can't be achieved by common solutions. In fact, proprietary solutions are built with additional layers of security, so they can ensure resilience and security of the overall system.

Another barrier is related to the **economic** reasons. Portuguese demonstrator and Northern cluster refer that all changes to the common solutions require several adjustments to fit the systems and need resources that could be limited. Even though proprietary solutions can be initially expensive option, they can be cheaper if the organization has resources with technical expertise to build the solutions.

From the analysis of demos' responses, we can identify also **regulatory framework** as a barrier. As for the Greek demo, as well as the Cyprus demo, the lack of regulation regarding a flexibility market operation, non-existence flexibility market, lack of the submetering regulatory framework are also reasons for not adopting common solutions.

5.3 Harmonization: outline

This section analyses the issue of standardisation and interoperability in the solutions developed in the OneNet demos. While the analysis is to a large extent based on the work done in OneNet WP4 [23] [24] [25] (Integrated Systems Operation for OneNet), this deliverable goes further in analysing not only data exchanges, but also solutions for cyber security and market algorithms. Moreover, another exercise in collecting up-to-date information at the time of the project finalisation was done to capture the final decisions made in the demos.

The analysis has shown that there is no clear consensus on using common solutions when implementing the demonstration solutions. The reasons for using proprietary solutions listed by demos mainly concern:

- Path dependency: it is easier to develop proprietary solutions compatible with the existing systems. This can save financial expenditure, as well as the time and human resources invested.
- Cost of adoption: even for systems developed from scratch (and therefore not impacted by path dependency), developing a proprietary solution can prove to be simpler and less costly than implementing existing common solutions (that might be overly complicated for the particular use case and might require further adaptations anyway).
- Existing common standards do not offer viable solutions for the particular demo needs, therefore dedicated solutions are the only option.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

- Network operators are concerned about the security of the common solutions.

It should be noted that these arguments were named by a group of specific actors in the electricity sector and therefore this perspective might be more representative of the views of network operators. From a more systemic and long-term perspective, the higher cost of adoption of common solutions for network operators could be offset by lower cost of adoption for other actors in the system. This kind of systemic planning however cannot be done by the network operators alone, as they are obliged to focus on reduction of network operating costs. Therefore, additional support from regulators and policy makers would be necessary to adapt more holistic consideration of potential benefits.

Based on the findings of this chapter, the recommendations to harmonise TSO-DSO-customer interactions to achieve wide-scale interoperability are:

- Acknowledge that there will remain a certain level of variety in the implemented solutions, due to cost considerations, path dependency or simply because development of standards takes time and cannot always catch up with the dynamic developments in electricity grids.
- The actors implementing proprietary solutions should make sure that the solutions make sense also in a long-term perspective and taking into account the whole energy system.
- If proprietary solutions are implemented, they should be designed in such a way, that the interoperability to the rest of the system is not impaired. This could be through adequate interfaces, standardized communication solutions, etc. While it might be still difficult for other actors to adapt to the proprietary solution, at least this way there will be an avenue how to do so, and it will help to remedy some of the drawbacks of proprietary solutions, such as vendor lock-in and software opacity.
- Develop further the common standards for data exchange (or make them more flexible/simplified) so that they can offer a working solution for the needs of newly developed use cases.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

6 Evaluation of harmonization actions

6.1 Methodology

The methodology for the evaluation of harmonization actions for data exchange and interfaces is outlined in section 2.2, in this section it is presented in detail. Here, numerous harmonization measures from various aspects of data exchange and interfaces are collected, evaluated and prioritized according to their potential EU impact, timeline and cost as illustrated in Figure 6.1.

First, several EU initiatives were reviewed to apply an established methodology for the evaluation of the impact of harmonization measures at EU level as presented in chapter 3 of this document.

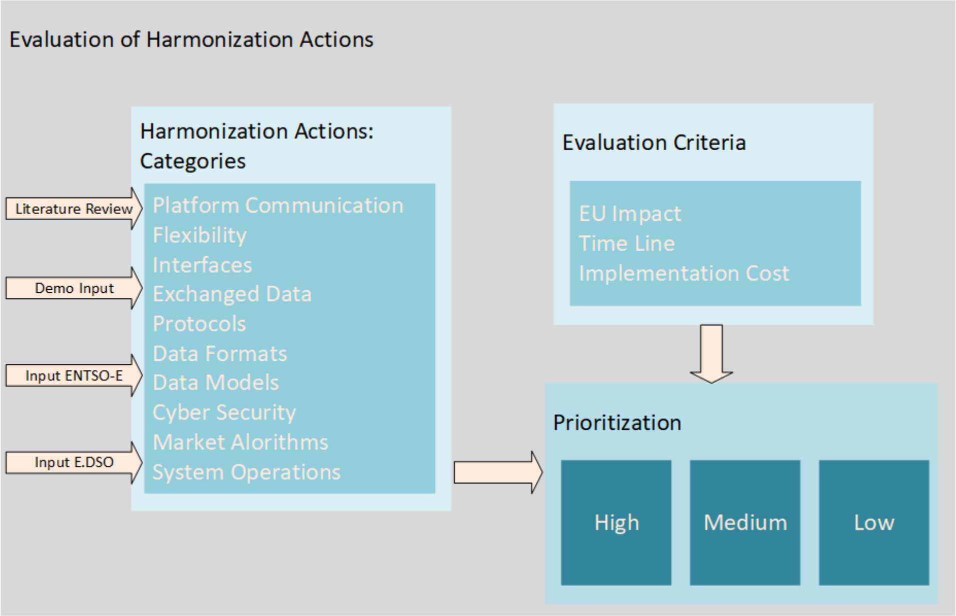

Figure 6.1 Methodology for the evaluation and prioritization of harmonization actions of data exchange and interfaces

To improve interoperability among platforms at EU level, the demos were asked to provide their input on possible harmonization measures which would be useful and applicable from their point of view. Furthermore, input from ENTSO-E and E.DSO has been included to add the perspective of organizations active at EU level. Here, a broad range of harmonization actions, such as the unification of a communication protocol or the definition of minimal cyber security requirements, were reviewed with the support of the demo leaders and the TSOs and DSOs involved in OneNet. The collected harmonization actions are evaluated according to the identified criteria such as expected EU impact, urgency and timeframe as well as implementation cost. Finally, the suggested harmonization measures have been evaluated according to their potential and cost, in order to

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

set the basis for final conclusions and an action plan in terms of interoperability in T11.7 to enable the integration of flexibility, improve the interoperability and enable active interaction among all grid actors.

6.2 Harmonization actions

6.2.1 Platform communication

Communication Infrastructure

The aspects encompassed within this group of actions revolve around bolstering communication infrastructure within the operational framework. This includes standardizing interfaces, integrating OneNet middleware, employing pre-filled communication formulas, and ensuring robust cyber protection for all communication channels.

A critical aspect is the establishment of a standardized communication interface, notably the use of REST API. This interface standardization allows seamless communication between various components and systems, promoting interoperability and efficient data exchange.

Incorporating OneNet middleware is essential for facilitating smooth interactions between disparate systems. The OneNet System acts as an intermediary, ensuring effective integration and communication flow between different platforms, thereby enhancing the overall operational efficiency, as the data exchange happens in a decentralized end-to-end way, without a further intermediary.

Additionally, leveraging pre-filled communication formulas streamlines the data transmission process, providing a predefined structure for exchanging information. This ensures consistency and accuracy in the conveyed data, thereby contributing to a more organized and efficient communication system.

Cybersecurity is a paramount consideration. Protecting these communication channels is imperative, and integrating cyber protection measures is crucial. This ensures that sensitive information remains secure during transmission, safeguarding the integrity and confidentiality of the data exchanged across the network.

Platform and Data Handling

These aspects pertain to platforms and efficient data management within the operational infrastructure.

The central platform is at the core of this category, serving as a pivotal hub for various operational activities. This centralized platform acts as a focal point for collating, processing, and managing critical data and information that are essential for the smooth functioning of the system.

For example, a specific platform, MARI, was chosen to address the requirements of the manual Frequency Restoration Reserve (mFRR) mechanism. MARI, as an mFRR platform, plays a crucial role in managing and ensuring the availability of reserves to restore the system frequency within predefined limits, thereby enhancing the overall stability of the grid.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Furthermore, data hubs dedicated to managing the metering data are integral components of this domain. These hubs efficiently handle large amounts of metering data generated by smart meters. By centralizing and organizing these data, hubs facilitate better analysis, decision-making, and operational planning within the distribution network.

6.2.2 Flexibility

Communication and information exchange

Communication and information exchange play pivotal roles within an aggregator's operational framework. The dynamic and interconnected nature of the market requires seamless communication and information flow among stakeholders. One key facet of this communication is the effective exchange of information between market operators and FSPs. This exchange ensures that the aggregator can respond adequately to market dynamics and needs.

A common format for information exchange is crucial to maximize the integration of flexibility. Establishing a standardized, shared format ensures that all stakeholders operate on a level playing field and promotes a harmonious flow of information. This common format further underscores the importance of flexibility in a dynamic market environment, which fosters collaboration and innovation among stakeholders.

Definition and methodology

The establishment of structured methodologies, frameworks and approaches is at the core of integrating flexibility in the operational dynamics. This forms the foundation for assessing the flexibility potential and addressing imbalances effectively. The first step involves defining a comprehensive methodology to assess the flexibility potential. This methodology should encompass an in-depth analysis of the available resources, technological capabilities, and market conditions. By gauging the potential for flexibility, stakeholders can develop targeted strategies to harness and optimize these resources.

A crucial aspect is the definition of a common framework for imbalance settlement. A standardized approach ensures that imbalances are handled uniformly across the board, promoting fairness and transparency within the system. The framework should address factors such as pricing mechanisms, dispute resolution, and collaboration protocols, to ensure a cohesive and efficient process for settling imbalances.

In essence, embracing flexibility requires a structured approach that encompasses methodologies to evaluate the potential and frameworks to handle imbalances. These elements collectively contribute to a more agile and adaptive operational environment, aligning stakeholders towards a more sustainable and responsive market. Through these defined methodologies and frameworks, the potential for a more resilient and dynamic market landscape can be achieved.

Aggregator and Flexibility

The aggregator is a cornerstone for delivering adaptability and responsiveness to the market. This role manifests in two primary facets: the technical API/UI components provided by the aggregator and its central position as the primary unit for flexibility provision.

First, the aggregator employs a sophisticated API that enables seamless communication and interaction between the aggregator and FSPs. This API facilitates the exchange of data and commands and streamlines the process of flexibility provision. It acts as a bridge, allowing FSPs to efficiently integrate their systems and offerings into the aggregator's ecosystem.

In conjunction with the API, the aggregator also presents an FSP aggregator UI (User Interface). This interface serves as a user-friendly platform, offering an intuitive and accessible means for FSPs to interact with an aggregator's system. The UI provides a visual representation of flexibility options, allowing FSPs to navigate, customize, and tailor their offerings based on market demand and operational requirements.

At its core, the aggregator functions as the primary unit of flexibility. Its pivotal position is to aggregate, orchestrate, and optimize flexibility resources from various FSPs. By consolidating these resources, the aggregator enhances the overall flexibility potential of the market. It acts as a focal point, effectively managing and deploying flexibility to match real-time demand and ultimately contributing to a more agile and responsive market.

6.2.3 Interfaces

Communication interfaces

Communication interfaces are fundamental pillars that facilitate seamless interaction among diverse stakeholders. These interfaces and channels play vital roles in connecting and engaging various entities, such as TSOs, DSOs, FSPs, MOs, and more.

One pivotal implementation is the harmonization of communication interfaces utilizing technologies such as REST APIs, specifically designed to foster effective communication among stakeholders. The use of a standardized interface facilitates the exchange of information, resulting in improved interoperability and operational efficiency.

Moreover, the communication interface between the MO and the stakeholders is of paramount importance. This interface facilitates a direct and structured flow of information, enabling the MO to effectively coordinate with market participants.

Additionally, interfaces such as T&D-CP – SO and T&D-CP – MO provide dedicated channels for communication between dedicated TSO-DSO Coordination Platform (T&D-CP) and System Operators (SO) and

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

MOs, respectively. These interfaces enhance coordination and ensure a smooth flow of information between different layers of infrastructure.

A common interface acts as a unifying entity, streamlining the participation of stakeholders. This standardizes the process, making it easier for entities to engage in and contribute to a flexible system.

6.2.4 Data exchange

Communication and standards

Efficient communication, data exchange, and processes are essential and involve multiple stakeholders, such as TSOs, DSOs, market operators, flexibility providers, and various platforms. The primary objective is to synchronize the interfaces, formats, schemas, and processes to facilitate effective communication and seamless data sharing.

Effective communication between MOs and market participants is vital. Setting up efficient communication channels in both directions enables real-time market updates and requirements, resulting in better synchronization of flexibility provisions.

Another key aspect of data exchange is the pre-agreed format and schema, representing the data model, between DSOs and TSOs. Aligning with a standard format and schema ensures smooth data exchange, providing a common understanding and structure for shared information. Defined schedules for data exchange aligned with market results and timely and synchronized data exchanges based on market outcomes allow for quicker adjustments and decision-making, contributing to efficient operation.

Implementing a standardized process, for example to share market results akin to the OneNet Connector, offers a structured and consistent approach for disseminating critical market information. This approach enhances transparency and facilitates collaboration among stakeholders, ultimately promoting an agile and responsive sector.

Market-related Data Exchange

A multitude of data flows through market processes, encompassing bids, flexibility parameters, schedules, metering data, tenders, purchase offers, and market results. The focus here lies in establishing robust schedules and efficient processes for the seamless exchange of data and optimizing market activities.

The requirement to optimize the flow of crucial data groups, such as bids, flexibility parameters, schedules, metering data, tenders, and purchase offers, lies at the heart of this matter. Implementing a structured data-exchange method for these vital components is essential to ensure that the market operates smoothly and effectively.

One actionable step involves defining clear schedules for data exchange that are meticulously aligned with market results. This alignment ensures that data are exchanged at strategic junctures, allowing stakeholders to make informed decisions and adapt their strategies in real time, ultimately enhancing the market's effectiveness.

It is imperative to create a standardized process for disseminating market outcomes along with well-defined schedules. By taking inspiration from systems such as the OneNet Connector, this standardized process facilitates the efficient and consistent dissemination of critical market insights. This process serves as a key component in ensuring that market results are communicated in a transparent, easily understandable, and uniform manner.

Achieving full integration entails harmonizing the schedules of these processes with those of the other markets.

TSO-DSO collaboration

Central to efficient operation is the seamless exchange of data and collaboration, particularly between TSO and DSO. This collaborative effort focuses on crucial aspects, such as registration, prequalification, bid optimization, flexibility activation and settlement, but also managing outages and establishing a unified register for flexibility services and associated identification.

Addressing outages is part of this data exchange effort. Ensuring smooth communication and coordination between TSOs and DSOs regarding outages is essential to maintain a reliable energy supply. These include timely reporting, updates, and resolution plans.

An element of this collaboration involves creating a common register that encapsulates flexibility services and their identification. TSOs and DSOs collaborate to define and maintain this register, which acts as a centralized hub for all contracted flexibility services. Standardized identification protocols and data structures within this register enhance operational efficiency and streamline the utilization of flexible resources.

6.2.5 Protocols

Operations rely heavily on standardized communication protocols. These protocols serve as the backbone for seamless data exchanges and interactions within the landscape. One protocol in this domain is Hypertext Transfer Protocol Secure (HTTPS).

HTTPS is a communication protocol that ensures secure and encrypted data transmission over a network. Encrypting data enhances security and privacy, making it significantly more challenging for unauthorized entities to intercept or manipulate the information being exchanged. It is imperative to establish standardized communication protocols across various systems. These protocols define the rules and conventions for data exchange and provide a common language that facilitates seamless communication and integration among different components.

Incorporating HTTPS as a standard communication protocol enhances cybersecurity. By adhering to standardized communication protocols such as HTTPS, a robust foundation for secure, efficient, and reliable data exchange can be established.

6.2.6 Data formats

Specification of different formats

The specification of various data exchange formats is an aspect of modern operations. Among these formats, XML and JavaScript Object Notation (JSON) are particularly important. JSON, for example, provides a lightweight and standardized format for data interchange, facilitating easy parsing and human-readable data representation.

These formats enhance the interoperability and data integrity, enabling integration across diverse energy systems and platforms. XML enables facilitates the comparison and aggregation of data, is open and extensible, while JSON offers a structured and standardized way to represent data, streamlining data processing and utilization.

Supporting these formats in different applications is essential. Various applications within the energy domain, such as energy management systems, grid monitoring tools, and customer-facing platforms should be designed to interact using XML and JSON. This ensures a cohesive system in which data can be exchanged, processed, and utilized seamlessly across different facets of energy operations.

Enhancing accessibility by supporting these formats through user-friendly interfaces, such as Web User Interfaces (WebUI) and email, is significant. WebUI allows users to interact with data easily through web-based interfaces, thereby promoting intuitive data exchange. Simultaneously, integrating these formats with email facilitates efficient communication and data-sharing.

6.2.7 Cyber security

Authentication and authorization

Ensuring cybersecurity of systems involves implementing diverse methods and processes for robust authentication and authorization. The objective is to ensure that only authorized users or systems can securely access and interact with platforms or components within the infrastructure.

A fundamental aspect is identification/authentication, which establishes secure user identity. This includes employing authentication mechanisms to validate the identities of users and systems seeking access.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

One effective approach is to adopt token-based authentication. This method involves generating and validating unique tokens for users and enhancing security by reducing the need to transmit sensitive information for every interaction.

By employing digital certificates, the system can verify the authenticity of users or entities that attempt to access critical energy components, thereby fortifying the security posture.

JSON Web Tokens (JWT) enable secure sharing of authorization data between parties, ensuring that only those with appropriate permissions can access designated resources.

Finally, integrating human-based user authorization processes strengthens security measures. By carefully defining and controlling the permissions granted to individuals based on their roles and responsibilities, the system can effectively manage access to sensitive information and functionalities.

Secure data transmission

Secure data transmission encompasses safeguarding communication within individual entities and across different layers; this concept is known as cross-layer communication. Employing HTTPS and related security protocols is fundamental to guaranteeing the secure transfer of data.

One key action is to establish cyber-protected communication within an entity's platforms or components, such as ensuring secure communication channels between TSOs and DSOs. Additionally, it enables secure communication between DSOs and FSPs, thus contributing to a fortified cybersecurity architecture.

Data privacy and consent management

Cybersecurity adeptly manages and secures various types of data to uphold privacy and to adhere to consent compliance requirements. The two key categories of data that demand particular attention are metering and bidding data.

Metering data, which is highly sensitive, requires stringent security measures to protect against unauthorized access and potential breaches. Furthermore, ensuring compliance with consent regulations is important because explicit permissions are obtained from individuals or entities before using their data. This ensures that the metered data are handled responsibly and in line with privacy regulations.

Bid data is an area that necessitates robust cybersecurity measures. Bid data provide valuable insights into market behavior and strategies. Consequently, safeguarding bid data against unauthorized access, manipulation, and theft is required to maintain the integrity and competitiveness of the energy market. Implementing encryption, access controls, and monitoring mechanisms are actions used to fortify bid data security.

6.2.8 Market algorithms

Market clearing algorithm harmonization

Effective market operation and optimization rely on the harmonization and optimization of market-clearing algorithms. Specifically, this effect aligns algorithms to enhance market efficiency and effectiveness, with a keen focus on synchronization between TSOs and DSOs.

The development of a joint TSO-DSO optimization-based market-clearing algorithm aims to create a collaborative approach in which TSOs and DSOs work in tandem to optimize market-clearing processes. By leveraging their respective expertise and data, this joint algorithm facilitates efficient resource allocation and ensures a well-coordinated and optimal energy market.

Harmonization of market-clearing algorithms achieves a standardized and consistent approach across market operations. This harmonization simplifies interactions and transactions between various entities, leading to a more cohesive and efficient market.

Specific market algorithm

Understanding and potentially implementing specific market algorithms, such as Adaptive Group Notification (AGNO) [28], Deadline Guarantee and Influence-Aware scheduling (DGIA) [29], and Process-Based Cost Modeling technique (PBCM) [30], optimizes efficiency. These algorithms are specialized approaches in the market context.

The AGNO algorithm, for instance, stands as a unique framework designed to enhance grid operations and energy distribution. By comprehending the intricacies of AGNO and its applications, market operators can leverage its capabilities to optimize grid management and ensure a reliable and stable energy supply.

Similarly, the DGIA algorithm, denoting a specific approach to distributed generation integration, has great potential in shaping the energy market. Acquiring a comprehensive understanding of DGIA enables stakeholders to effectively incorporate distributed generation sources and promote sustainability and resilience.

The PBCM algorithm, which focuses on price-based congestion management, offers a method for alleviating congestion and optimizing energy flows within the market. Exploring and implementing PBCM allows for efficient management of energy distribution and pricing, ultimately benefiting both providers and customers in the market.

6.2.9 System Operations

Monitoring and forecasting

Operational planning activities depend on forecasting and monitoring accuracy. To accomplish this, there is harmonization and frequent information exchange between DSOs and TSOs. This synergy aims to optimize the precision of forecasts, ultimately improving operational planning.

Aligning the methodologies and tools used by both DSOs and TSOs ensures a unified and standardized approach to data analysis. This harmonization promotes consistency and accuracy in forecasting, laying a strong foundation for more effective operational planning.

Daily information exchanges between DSOs and TSOs facilitate the frequent sharing of crucial information regarding load patterns, system statuses, and other pertinent data, which can enhance operational planning activities.

Settlement and activation

Efficient system operation necessitates well-structured settlement and activation mechanisms facilitated by the platform. These mechanisms encompass the essential operational processes involved in settling transactions and activating services within a system.

The foundational action lies in establishing an integration of settlement and activation processes within the market platform. This integration increases the efficiency of the flow of transactions and services, reduces delays, and enhances the overall system efficiency.

Automation significantly expedites settlement processes by reducing manual intervention and potential errors. It allows swift and accurate financial transactions and ensures timely compensation.

Embedding real-time monitoring and reporting features within a platform is paramount. Real-time monitoring provides instantaneous insights into the settlement and activation processes, enabling prompt identification and resolution of anomalies. Concurrently, comprehensive reporting facilitates transparency and accountability and enhances the system’s credibility.

Integrating smart contracts into settlement and activation mechanisms can revolutionize the process. Smart contracts are executed automatically based on predefined terms, confirming an efficient and error-free settlement and activation. This automation minimizes the administrative workload and mitigates the risk of disputes.

6.3 Evaluation of harmonization measures

6.3.1 Criteria for the evaluation of harmonization measures

6.3.2 EU impact

The EU impact denominates the impact which the corresponding harmonization measure is expected to have for the improvement of the interoperability and the TSO-DSO-customer coordination at EU level.

6.3.3 Time scale

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

The criterion time scale expresses the urgency for the deployment of the harmonization measure and the adequate time scale. For example, the deployment of unified cyber security standards is significantly more urgent than the introduction of a unified data model. On the other hand, the time scale also includes the aspect, that the deployment horizon of certain measures might be specific and dependent on the introduction of technology or the development of the concrete field. Furthermore, certain solutions might have to be deployed in parallel with grid reinforcement to avoid additional cost at a later point in time.

6.3.4 Implementation cost

The aspect implementation cost addresses the fact that any modifications of the existing IT infrastructure, platforms and environments will cause additional expenses for the adaptation to the new solution, for example for the implementation of interfaces, adaptors or the switching to a completely different solution such as an alternative data model.

6.3.5 Prioritization of harmonization measures

To outline a possible trajectory in the harmonization of data exchange, possible harmonization actions were discussed, and a questionnaire was circulated among the demo clusters in order to collect the opinion of the corresponding demo on harmonization measures, which would be helpful from the perspective of their requirements and circumstances. To derive a comprehensive and nuanced rating system for the self-assessment of the particular demos, the authors devised a structured approach encompassing two distinct ratings. The first rating comprised a straightforward sum of self-ascribed values attributed to the following categories: EU impact, implementation cost, and timeframe. Each category's value is based on an evaluation of the impact of the action at EU level, the financial cost associated for example with its implementation, the management of legacy system, etc., and the anticipated duration for its successful realization. Thus, we differentiate between the recommended and expected timeframes. In the following, this simplified rating is referred to as *basic rating.*

The second component of this rating system introduces a weighted summation, where the EU impact and urgency are accorded heightened significance through a multiplication factor of 1.5. This augmentation aims to underscore the pivotal roles that the EU’s impacts and urgency play in the overall assessment. This rating is referred to as *weighted rating*.

The resultant rating, thus amalgamated, bifurcates into distinct tiers of significance: high, medium, and low. Assignments of high, medium, or low ratings were contingent upon the cumulative values accrued and categorized within predefined ranges of 15–10 for high, 10–5 for medium, and 5–0 for low.

The rationale behind this approach is rooted in the belief that the EU’s impact and urgency are paramount considerations in evaluating potential effectiveness and immediate pertinence within the European context. Consequently, affording these aspects greater weight in the rating system ensures a more nuanced appraisal.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

6.3.5.1 Platform communication

In the context of the basic rating presented in Table 6.1 - Platform communication harmonization measures evaluated with the basic rating based on EU impact, implementation cost and the expected timeframeTable 6.1, the classification of the initiative is founded on commonalities across categories, primarily focusing on the communication infrastructure and platform data handling. The high-rated elements in this rating encompass the utilization of the OneNet Connector, specifically in Hungary and Portugal, indicative of a strong EU impact and favourable recommended timeframe. The medium-rated aspects emphasize the communication infrastructure through OneNet Middleware and cyber-protected communication in Cyprus, reflecting a moderate level of EU impact and expected timeframe.

Then, the weighted rating elevates the urgency of implementation, shifting the emphasis towards prompt and efficient execution of the initiative as illustrated in Table 6.2. The high-rated elements in this rating align with those in the basic rating, accentuating the use of the OneNet Connector and cyber-protected communication. Medium-rated components maintain a similar trend, with a focus on OneNet Middleware and REST API communication.

Table 6.1 - Platform communication harmonization measures evaluated with the basic rating based on EU impact, implementation cost and the expected timeframe

basic rating	categories based on commonalities	specification of harmonization action	DEMO
high	Communication infrastructure	Usage of OneNet Connector	Hungary
		Cyber-Protected communication	Cyprus
		Standardized communication interface	Portugal
		Implementation of OneNet Connector	
		Usage of OneNet Connector	Poland
	Platform and data handling	mFRR platform (MARI)	Northern
		Datahubs of DSO metering data	
medium	Communication infrastructure	OneNet Middleware	Northern
		Communication on platforms through REST API	Cyprus
		Standardized communication protocol	Spain
		Central platform	Czech
		Pre-filled communication formulas	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Table 6.2 - Platform communication harmonization measures evaluated with the weighted rating

weighted rating	categories based on commonalities	specification of harmonization action	DEMO
high	Communication infrastructure	Usage of OneNet Connector	Hungary
		Cyber-Protected communication	Cyprus
		Standardized communication interface	Portugal
		Implementation of OneNet Connector	
		Standardized communication protocol	Spain
	Platform and data handling	mFRR platform (MARI)	Northern
		datahubs of DSO metering data	
medium	Communication infrastructure	OneNet Middleware	Northern
		Communication on platforms through REST API	Cyprus
		Central platform	Czechia
		Usage of OneNet Connector	Poland
low	Communication infrastructure	Pre-filled communication formulas	Czech

6.3.5.2 Flexibility

With the basic rating in Table 6.3, the evaluation revolves around the commonalities between aggregators and flexibility, communication and information exchange, and definition and methodology. The high-rated elements emphasize the utilization of a FSP aggregator API. Medium-rated facets underscore the significance of the FSP aggregator UI and the defined format for communication in Poland and Portugal, respectively.

In the case of weighted rating in Table 6.4, high-rated elements, in alignment with the basic ratings, the utilization of the FSP aggregator API and UI, as well as effective communication with flexibility providers, are underscored. Additionally, the presence of a defined common format is indicative of a proactive approach to EU impact and urgency. Medium-rated facets highlight the significance of aggregator-provided flexibility and defined communication formats in Poland and Portugal.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Table 6.3 - Flexibility measures evaluated with the basic rating for the recommended timeframe

basic rating	categories based on commonalities	specification of harmonization action	DEMO
high	Aggregator and flexibility	FSP aggregator API	Northern
	Communication and information exchange	Communication between operator and FSP	Cyprus
		Communication with flexibility providers	
medium	Aggregator and flexibility	FSP aggregator UI	Northern
		Aggregator provides flexibility	Poland
	Communication and information exchange	Definition of format to exchange	Portugal
		Definition of a common format	Spain
	Definition and methodology	Definition of a methodology	Portugal
		Definition of a common framework	Spain

Table 6.4 - Flexibility harmonization measures evaluated with the weighted rating for impact and urgency

weighted rating	categories based on commonalities	specification of harmonization action	DEMO
high	Aggregator and flexibility	FSP aggregator API	Northern
		FSP aggregator UI	
	Communication and information exchange	Communication between operator and FSP	Cyprus
		Communication with flexibility providers	
		Definition of a common format	Spain
	Definition and methodology	Definition of a common framework	Spain
medium	Aggregator and flexibility	Aggregator provides flexibility	Poland
	Communication and information exchange	Definition of format to exchange	Portugal
	Definition and methodology	Definition of a methodology	Portugal

6.3.5.3 Interfaces

In the context of the basic rating in Table 6.5, the evaluation centres on commonalities concerning communication interfaces, emphasizing their harmonization action. The high-rated elements underline the presence of robust communication interfaces that facilitate interactions between diverse stakeholders, notably

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

in the Northern DEMO. In addition, the middleware functionality interfacing different platforms in Cyprus is highlighted. The medium-rated aspects accentuate standardized and harmonizing communication interfaces in Hungary and Spain, respectively, suggesting a moderate EU impact and a balanced recommended timeframe.

The high-rated elements in weighted rating in Table 6.6 align with those in the basic ratings, emphasizing the importance of standardized and harmonizing communication interfaces, inter-stakeholder interaction, middleware functionality, and web user interfaces (WebUI). The emphasis on these high-rated elements indicates a proactive approach toward EU impact and urgency. Medium-rated facets highlighted the significance of a common flexibility interface in Spain and the unification of communication channels in the Czech DEMO, signifying a moderate EU impact.

Table 6.5 - Interface harmonization measures evaluated with the basic rating

basic rating	categories based on commonalities	specification of harmonization action	DEMO
high	Communication interfaces	Interface between different stakeholders	Northern
		Middleware between different platform	Cyprus
medium	Communication interfaces	Standard Harmonizing communication	Hungary
		Common flexibility interface	Spain
		Unify communication channel	Czech
		WebUI	Poland

Table 6.6 - Interface harmonization measures evaluated with the weighted rating

weighted rating	categories based on commonalities	specification of harmonization action	DEMO
high	Communication interfaces	Standard Harmonizing communication	Hungary
		Interface between different stakeholders	Northern
		Middleware between different platform	Cyprus
		WebUI	Poland
medium	Communication interfaces	Common flexibility interface	Spain
		Unify communication channel	Czechia

6.3.5.4 Exchanged data

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

With the basic rating in Table 6.7, the high-rated elements underscore the creation of common definitions and data structures in Poland and the collaboration between TSO and DSO in Cyprus. The latter aspect highlights the efficient communication channels from operators to FSPs and market operators with providers. The medium-rated aspects highlight harmonizing communication interfaces in Hungary, along with market-related data exchange encompassing bids, flexibility, schedule, and metering data in the Northern DEMO. Low-rated elements emphasize market-related data exchanges with pre-agreed formats and schemas in Portugal.

In weighted rating in Table 6.8, the high-rated elements align with those in ratings 1 and 2, emphasizing the importance of harmonizing communication interfaces, standardizing communication structures, and efficient market-related data exchange. The emphasis on these high-rated elements indicates a proactive approach toward EU impact and urgency. Medium-rated facets highlight the significance of market-related data exchange, focusing on pre-agreed formats and schemas in Portugal, and the alignment of schedules with market results.

Table 6.7 - Data exchange harmonization measures evaluated with the basic rating for the recommended timeframe

basic rating	categories based on commonalities	specification of harmonization action	DEMO
high	Comm. interface and standards	Creation of common definitions and data structures	Poland
	TSO-DSO collaboration	Communication of operator to the FSPs	Cyprus
		Communication of market operators with providers	
		Communication of operators' providers	
medium	Comm. interface and standards	Harmonizing communication interface	Hungary
	Market-related exchange	Bids, Flexibility, Schedule, Metering data, etc.	Northern
		Standardized process for sharing market results	Spain
		Schedule of processes with energy markets	
low	Market-related exchange	Pre-agreed format and schema	Portugal
		Definition of schedules aligned with market results	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Table 6.8 - Data exchange harmonization measures evaluated with the weighted rating

weighted rating	categories based on commonalities	specification of harmonization action	DEMO
high	Communication interface and standards	Harmonizing communication interface	Hungary
		Creation of common definitions and data structures	Poland
	Market-related exchange	Bids, Flexibility, Schedule, Metering data, etc.	Northern
		Standardized process for sharing market results	Spain
		Schedule of processes with energy markets	
	TSO-DSO collaboration	Communication of operator to the FSPs	Cyprus
		Communication of market operators with providers	
		Communication of operators' providers	
medium	Market-related exchange	Pre-agreed format and schema	Portugal
		Definition of schedules aligned with market results	

6.3.5.5 Protocols

With the basic rating in Table 6.9, the evaluation is centred on commonalities concerning standardized communication protocols and their harmonization actions, with an emphasis on demonstration (DEMO). The high-rated element underlines the definition and establishment of standardized communication protocols, particularly within the context of Cyprus. Medium-rated aspects extend the theme of secure communication by highlighting protocols that prioritize security through the utilization of HTTPS in Portugal, Spain, and Poland.

In weighted rating in Table 6.10, the high-rated elements align with those in the basic ratings, emphasizing the importance of standardized communication protocols and secure communication through HTTPS. The emphasis on these high-rated elements indicates a proactive approach toward EU impact and urgency. Medium-rated facets highlight the significance of secure communication through HTTPS in Portugal and Poland.

Table 6.9 - Protocol harmonization measures evaluated with the basic rating

basic rating	categories based on commonalities	specification of harmonization action	DEMO

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

high	Standardized communication protocols	Define standardized communication	Cyprus
medium	Standardized communication protocols	Secure communication through HTTPS	Portugal Spain Poland

Table 6.10 - Protocol harmonization measures evaluated with the weighted rating

Weighted rating	**categories based on commonalities**	**specification of harmonization action**	**DEMO**
high	Standardized communication protocols	Define standardized communication	Cyprus
		Secure communication through HTTPS	Spain
medium	Standardized communication protocols	Secure communication through HTTPS	Portugal Poland

6.3.5.6 Data formats

With the basic rating, the evaluation revolves around commonalities pertaining to the specification of harmonization actions and different data exchange formats. The medium-rated element emphasizes the specification of various data-exchange formats in Cyprus. Low-rated elements underscore the specification of diverse formats and data-exchange mechanisms supported by WebUI and email in Poland.

In the weighted rating in Table 6.12, the medium-rated elements reiterate the significance of specifying diverse data-exchange formats in Cyprus, aligning with the previous ratings. Additionally, data exchange mechanisms supported by WebUI and email in Poland are highlighted.

Table 6.11 - Data format harmonization measures evaluated with the basic rating for the recommended timeframe

basic rating	**categories based on commonalities**	**specification of harmonization action**	**DEMO**
high		json	Hungary
medium	Specification of different formats	Specification of different data exchange formats XML, json XLS, TXT XLSX	Cyprus Portugal Spain Poland

low	Specification of different formats	Data exchanges supported with Web UI and email	Poland

Table 6.12 - Data format harmonization measures evaluated with the weighted rating

weighted rating	categories based on commonalities	specification of harmonization action	DEMO
high		JSON	Hungary
medium	Specification of different formats	Specification of different data exchange formats	Cyprus
		Data exchanges supported with WebUI and email	Poland
		XML, JSON XLS, TXT	Portugal Spain
low		XLSX	Poland

6.3.5.7 Cyber security

In basic rating in Table 6.13, the medium-rated elements underline the importance of authentication and authorization mechanisms, notably, the implementation of token-based authentication, digital certificate authentication, and authorization with JSON Web Tokens in Portugal, Spain, and Poland, respectively. Moreover, secure data transmission is emphasized through the adoption of cyber-protected communication and the use of HTTPS for secure communication in Cyprus and Portugal. These low-rated elements emphasize human-based user authorization and secure data transmission through the HTTPS protocol in Poland and Spain.

The implementation of token-based authentication, digital certificate authentication, and authorization with JSON Web Tokens are highlighted in Portugal, Spain, and Poland, respectively, with ratings of 2. Additionally, secure data transmission through the use of HTTPS and Cyber-Protected communication, as well as the HTTPS protocol, underscores a comparable level of EU impact and a balanced expected timeframe. Low-rated elements indicate a reduced sense of urgency and EU impact within this categorization.

The medium-rated elements in the weighted rating in Table 6.13 emphasize the significance of authentication and authorization mechanisms, such as human-based user authorization, in Poland. In addition, secure data transmission through the use of HTTPS and the HTTPS protocol is reiterated, highlighting their importance.

Table 6.13 - Cyber security measures evaluated with the basic rating

basic rating	categories based on commonalities	specification of harmonization action	DEMO

medium	Authentication and authorization	Implementation of token-based authentication	Portugal
medium low	Authentication and authorization Secure data transmission	Digital certificate authentication	Spain
		Authorization with JSON Web Tokens	Poland
		Cyber-Protected communication	Cyprus
	Secure data transmission Authentication and authorization	Use of HTTPS for secure communication	Portugal
		Human-based user authorization	Poland
low	Secure data transmission	HTTPS protocol	Spain

Table 6.14 - Cyber security harmonization measures evaluated with the weighted rating

weighted rating	categories based on commonalities	specification of harmonization action	DEMO
high	Authentication and authorization	Implementation of token-based authentication	Portugal
		Digital certificate authentication	Spain
	Secure data transmission	Cyber-Protected communication	Cyprus
medium	Authentication and authorization	Human-based user authorization	Poland
	Secure data transmission	Use of HTTPS for secure communication	Portugal
		HTTPS protocol	Spain
low	Authentication and authorization	Authorization with JSON Web Tokens	Poland

6.3.5.8 Market algorithms

In terms of market algorithms, the high- and medium-rated components remained consistent through the different ratings in Table 6.15 and Table 6.16.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The high-rated elements underscore the harmonization of market-clearing algorithms, particularly focusing on joint transmission system operator–distribution system operator (TSO-DSO) optimization in the Northern DEMO. Moreover, particular market algorithms, such as AGNO, DGIA, and PBCM in Poland, are spotlighted. The medium-rated aspect emphasizes the importance of harmonizing market-clearing algorithms in Cyprus.

Table 6.15 - Market algorithm harmonization measures evaluated with the basic rating

basic rating	categories based on commonalities	specification of harmonization action	DEMO
high	Market clearing algorithm harmonization	Joint TSO-DSO optimisation	Northern
	Specific market algorithm	AGNO, DGIA, PBCM algorithms	Poland
medium	Market clearing algorithm harmonization	Harmonization of market clearing algorithms	Cyprus

Table 6.16 - Market algorithm harmonization measures evaluated with the weighted rating

weighted rating	categories based on commonalities	specification of harmonization action	DEMO
high	Market clearing algorithm harmonization	Joint TSO-DSO optimisation	Northern
medium	Specific market algorithm	AGNO, DGIA, PBCM algorithms	Poland
	Market clearing algorithm harmonization	Harmonization of market clearing algorithms	Cyprus

6.3.5.9 System operations

The medium-rated elements emphasize the harmonization of accuracy in forecasting within Cyprus, implying a moderate EU impact and a recommended timeframe for implementation in Table 6.17. Furthermore, the importance of information exchange between DSO and TSOs in Portugal is underlined. Low-rated elements suggest a focus on the settlement and activation processes through market platforms in Poland, implying a relatively reduced EU impact.

For the weighted rating in Table 6.18, the medium-rated facets echo the importance of accuracy in forecasting, emphasizing its harmonization within Cyprus. Additionally, the significance of information exchange between the DSO and TSO in Portugal is reiterated. Low-rated elements hint at a reduced sense of urgency and EU impact within this categorization, emphasizing settlement and activation processes through market platforms in Poland.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Table 6.17 - System operation harmonization measures evaluated with the basic rating

basic rating	categories based on commonalities	specification of harmonization action	DEMO
medium	Accuracy and forecasting	Harmonization of accuracy for forecasting	Cyprus
		Information exchange between DSO and TSO	Portugal
low	Settlement and activation	Settlement and activation through market platform	Poland

Table 6.18 - System operation harmonization measures evaluated with the weighted rating

weighted rating	categories based on commonalities	specification of harmonization action	DEMO
medium	Accuracy and forecasting	Harmonization of accuracy for forecasting	Cyprus
		Information exchange between DSO and TSO	Portugal
low	Settlement and activation	Settlement and activation through market platform	Poland

6.3.6 Conclusions

After looking at the various categories individually, in the next step the focus is on how intricately interwoven these categories are to achieve a comprehensive system improvement at EU level. These categories are deeply interconnected and collectively contribute to the overarching goals of efficient communication, enhanced flexibility, robust cyber security, and effective system operations.

The utilization of technologies such as the OneNet Connector in Hungary and Portugal is not just about improving the communication infrastructure but highlights the higher EU goal of achieving a harmonized and integrated system. This integration is critical to ensure seamless data exchange and interoperability across member states. The focus on cyber-protected communication in Cyprus, while rated differently, ties into the larger narrative of ensuring system security and reliability and themes that resonate across other categories.

Flexibility as a category extends beyond the mere use of aggregator APIs and UIs. This encapsulates the EU's vision of a responsive and adaptable energy system. This adaptability is crucial in the face of fluctuating energy demands and integration of renewable energy sources. The importance placed on communication formats and methodologies in Poland and Portugal further underscores the need for a standardized yet flexible approach to data exchange and communication.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The emphasis on interfaces, particularly the harmonization of communication interfaces, goes hand-in-hand with the themes of platform communication and flexibility. The effectiveness of these interfaces in facilitating interactions among diverse stakeholders, as seen in Northern and Cyprus demos, is paramount for creating a cohesive EU-wide energy network. This cohesion is necessary to realize the EU's objectives of energy efficiency and sustainability.

Exchanged data, as a category, highlights the criticality of creating common definitions and structures for data. This is not just a technical requirement, but also a foundational aspect of ensuring that data exchange across different EU regions is coherent and aligned.

The protocols category, emphasizing standardized communication protocols and security through HTTPS, intersects with cybersecurity. These protocols form the backbone of a secure and reliable communication network, which is a necessity in today's digital and interconnected world. The implementation of these protocols demonstrates a commitment to maintaining a high standard of security and reliability across the EU network.

Data models, exchange formats, and cyber security are not just individual components but are part of the larger framework that supports the robust functioning of the EU's energy systems. Specificity in data models, as seen in Hungary, and adaptability in data exchange formats, as exemplified in Cyprus and Poland, are critical for handling the diverse and complex data landscape of the EU. Similarly, the focus on cyber security through authentication and authorization mechanisms is essential for protecting these data and infrastructure from cyber threats.

The market algorithms and system operation categories further illustrate this interconnectedness. The harmonization of market-clearing algorithms and emphasis on forecasting accuracy and information exchange are not standalone objectives. These are integral to ensuring that the EU's energy market operates efficiently and transparently, facilitating optimal resource allocation and system stability.

In conclusion, the different categories, although rated separately, are part of a cohesive and interconnected system. Each category, with its specific focus, contributes to broader EU objectives in terms of energy efficiency, security, and sustainability. The variations in ratings and granularity within the measures highlight the complex nature of these systems and the need for a nuanced approach that considers the unique challenges and opportunities in each demo.

6.4 Further input

The experience of E.DSO and ENTSO-E shows that the introduction of novel concepts and the system-wide deployment requires enormous amount of manpower, time and resources. In the discussed case of the switching to a unified data format, where all power elements had to be modelled according to the new format, even though the harmonization of different standards and solutions is expected to bring significant benefits in terms of interoperability, the IT barriers and the duration of the adaptation exceeded the expectation by far. The hesitation of the involved third parties complicated the procedure additionally.

To summarize the findings, the definition of interoperability is not limited to applying the same solutions, interoperability is rather enabled by harmonization of the applied solutions to be able to interact and exchange data. This can be for example the deployment of adapters between the main solution and previous or local solutions, or the development of adequate interfaces on the side of proprietary solutions. Furthermore, with the advancing decentralization of resources and the increase of flexibility potential on customer side, customers gain more and more significance for the short-term grid operation and their concerns should be included in the data exchange models and standardization.

Particularly ENTSO-E follows a very concrete policy to enable interoperability and support standardization. There is an interoperability maturity model, which defines the main elements of interoperability and enables a certification process for industry. Here, conformity assessment labs are performed for industrial products to confirm that they comply to the standards and can interact through the standard data exchange solution.

In general, the listed challenges are typical and expected for projects of these dimensions, where a new product or standard is introduced into an existing infrastructure with hundreds of thousands of elements and frequent interactions. Therefore, initiatives to improve interoperability have to include geopolitical, socioeconomic and local restrictions, concerns of smaller entities with limited resources, as well as customer concerns to be able to draw the benefits with minimal effect on the stability of a very heterogeneous landscape of stakeholders.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

7 Recommendations and proposal for harmonization of data exchange and interfaces

The analyses presented in the previous sections showcased the various proprietary and common solutions that have been adopted by the several OneNet demonstrators, in the implementation of their tools' development, the pilots and validation processes. In the following, the work and the gained insights are summarized to draw concrete recommendations for the harmonization of data exchange and interfaces.

7.1 Summary

The analysis of OneNet demonstrators shows that, while in several cases the technologies and standards are common, there is yet significant differences among the various solutions, especially among the demos in the different regional clusters. The demonstrations are developed based on the local practices and proprietary solutions that are already commonly used in the TSO-DSO environment. This maintains the existing differentiation in data exchange and interfaces across the countries. A recommendation to this would be to develop more detailed guidelines for data exchange and interfaces to dictate the steps towards data interoperability that will be followed on a pan-European level. Additionally, it would be beneficial to develop a Network Code on Interoperability and Data Exchange for the Electricity networks, which is already existing in the Gas networks.[6] The legal framework for this is already set in the Electricity Market directive[7] and its implementing acts, foremostly the Commission Implementing Regulation on Interoperability Requirements for Metering and Consumption Data.[8]

The customers' flexibility is, at least in the cases of OneNet demonstrators investigated in this deliverable, mainly engaged through aggregated data and not in the form of actual data exchange with each customer. This is an unavoidable result of the low smart meter penetration in several European countries e.g., Greece, which is the main energy data source and non-standardization of data exchange from distributed flexibility assets on customer premises i.e., heat pumps, electric chargers, BMS systems etc. A recommendation that will facilitate harmonization in data exchange would be the large-scale deployment of smart meters across Europe and the standardization of communication among end devices.

[6] https://www.entsog.eu/interoperability-and-data-exchange-nc

[7] EC, 2019. Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0944

[8] EC, 2023. Commission Implementing Regulation (EU) 2023/1162 on interoperability requirements and non-discriminatory and transparent procedures for access to metering and consumption data. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1162#:~:text=This%20implementing%20Regulation%20lays%20down,(EU)%202019%2F944.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Open-source solutions in combination with stronger cybersecurity measures would facilitate the data exchange and interfaces among TSO-DSO-customers, providing opportunities for adaptability, while at the same time cyber-shielding the system operators' activities ensuring the resilience of the energy system. An additional recommendation could be to update/extend the "Network Code for cybersecurity aspects of cross-border electricity flows"[9] to emphasize more the TSO-DSO- customer data exchanges, interfaces and setting the cybersecurity framework that will facilitate/cyber-shielded open-source solutions.

Furthermore, the flexibility markets and business models should provide more incentives to valorize the end-customer flexibility. This would facilitate the use of data exchange and interfaces, and would also strengthen the case for harmonization, making it an enabler of market profitability, increasing liquidity and facilitating market transactions, apart from solely operational needs. This recommendation would certainly be facilitated by the smart meter and communications infrastructure on the grid.

7.2 Recommendations

Based on the analysis of the previous sections, we can draw the main conclusions and recommendations for harmonization in data exchange and interfaces:

7.2.1 Implementation of regulatory framework for interoperability

While the high-level regulatory principles for implementation of interoperability in the energy sectors were set in the European legislation, significant work remains to be done in implementing these principles in EU frameworks, network codes and on national level. It should be ensured that especially the national level legislation comes in a timely manner with a framework that enables existence of flexibility markets and that facilitates interoperability of the adapted solutions.

7.2.2 Standardization and interoperability

Standardisation of data exchange formats and communication interfaces is essential for harmonization of data exchanges in the energy sector. It ensures that different components and systems can seamlessly communicate and exchange data. Energy sector stakeholders should adopt standardized communication interfaces, such as REST API, for effective data exchange. This ensures a common language for communication and promotes interoperability.

[9] https://eepublicdownloads.entsoe.eu/clean-documents/Network%20codes%20documents/NC%20CS/220114_NCC_Legal_Text.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

7.2.3 Cyber security

Cybersecurity is a paramount concern in data exchange. Implementing secure communication protocols such as HTTPS is critical to safeguard sensitive information during transmission. Furthermore, encryption mechanisms should be implemented to protect data integrity and enhance cybersecurity. In terms of data privacy and consent compliance, robust cybersecurity measures should be implemented to protect sensitive data, including metering and bidding data. Compliance should be ensured with consent regulations to uphold data privacy.

7.2.4 Data Exchange in the market process

Efficient data exchange processes are crucial for real-time decision-making. Harmonized schedules for data exchange in the market process and structured processes in general can improve the overall effectiveness of the energy market. Therefore, data exchange schedules should be aligned with market results and real-time requirements. This ensures timely information sharing and enables stakeholders to make informed decisions. In terms of automated data exchange, it could include the use of smart contracts, streamline of settlement and activation processes. This reduces manual intervention and the potential for errors.

7.2.5 TSO-DSO coordination

Collaboration between TSOs and DSOs is vital for efficient data exchange, particularly in managing outages, maintaining a unified register for flexible services or in grid operation and planning. Collaboration between TSOs and DSOs in managing outages and maintaining a centralized register for flexibility services and resources should be fostered, as it improves the efficiency and reliability of data exchange. Here, transparency should be enhanced through real-time monitoring and comprehensive reporting features. This promotes accountability and trust among stakeholders.

7.2.6 Data exchange from FSP to end customer

The implementation of proprietary solutions for data exchange is often a barrier for the communication with the end customer. Here, it would be helpful to manage data exchange through a generic gateway solution able to control many proprietary models of an asset using the same product. The proposed solution not only adds value for on-site automation but could also offer FSP to aggregate flexibility across all similar assets using the same interface. An alternative, more efficient solution requires the resource manufacturer to provide cloud services for individual energy data measurements and possibly aggregation that could be used by a FSP through an API. The latter not only solves standardization issue but also propose an accurate method to tackle energy measurements and post-delivery verification and settlement which has been a hurdle due to lack of standards.

These recommendations and improving standardization, security, and collaboration, the energy sector can achieve harmonization in data exchange and interfaces, leading to a more efficient and responsive market.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

7.2.7 Harmonization actions in terms of communication and data exchange

To advance harmonization actions, it is essential to adopt a strategic approach that acknowledges diverse contexts while striving for greater integration and consistency. The following steps outline a pathway to effectively advance these harmonization actions.

- Foster collaboration and knowledge-sharing

  Encourage collaboration among member states to share best practices, technological insights, and experiences. For instance, countries such as Hungary and Portugal, which show advanced implementation of technologies such as the OneNet Connector, could share their experiences and strategies with others. This collaboration can facilitate learning and accelerate the adoption of effective practices across the EU.

- Tailor approaches to country-specific contexts

  Recognize the unique challenges and strengths of each member state. Customized strategies that consider local regulatory frameworks, technological infrastructure, energy market structures, and cultural attitudes should be developed. For instance, in countries lagging technological infrastructure, initial efforts might focus on building foundational capabilities before implementing advanced systems.

- Strengthening regulatory frameworks and policies

  Work towards developing and harmonizing regulatory frameworks and policies that support the adoption of these actions. This could involve setting EU-wide standards for data exchange formats, communication protocols, and cybersecurity measures while allowing for some flexibility to accommodate national differences.

- Investment in Technology and Infrastructure

  Facilitate investments in technology and infrastructure to ensure that all member states have the necessary tools and systems to implement harmonization actions. This could include financial support for less-developed countries or regions within the EU to help them catch up.

- Enhancing Training and Capacity Building

  Implement comprehensive training and capacity-building programs to ensure that the workforce in each member state is equipped with the skills and knowledge required to implement and manage new systems and protocols effectively.

- Promote Public Engagement and Support

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Engage with the public and stakeholders to build support for these initiatives. Public understanding and support are crucial for the successful implementation of such changes, especially those that directly impact energy consumption and market operations.

- Monitoring and evaluating progress

  Establish robust mechanisms to monitor and evaluate the progress of harmonization actions. Regular assessment and feedback can help identify areas of success and those requiring further attention, allowing for the continuous improvement and adaptation of strategies.

- Leveraging technological innovation

  Innovation should be encouraged in areas such as data analytics, machine learning, and blockchain to enhance the efficiency and effectiveness of energy systems. Innovative approaches can offer new solutions to complex problems, aiding harmonization efforts.

- Ensuring Cybersecurity and Data Protection

  Given the critical nature of energy infrastructure and data, cybersecurity and data protection should be prioritized in all harmonization efforts. This includes the development and implementation of stringent security protocols and ensuring compliance across member states.

- Alignment with Broader EU Objectives

  Ensure that all harmonization actions are aligned with broader EU objectives, such as the transition to renewable energy, sustainability, and reducing carbon emissions. This alignment ensures that harmonization efforts contribute to the overarching goals of the EU.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

References

[1] Schittekatte, T., Reif, V., and Meeus, L., ‘The EU Electricity Network Codes (2020 ed.)’. Online. Available at: https://fsr.eui.eu/publications/?handle=1814/67610.

[2] Reif, V., Nouicer, A., Schittekatte, T., Deschamps, V., and Meeus, L., ‘Report on the Foundations for the adoptions of New Network Codes 1’, INTERRFACE Project Deliverable D9.12/2021. Online. Available at https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5d94418be&appId=PPGMS.

[3] European Parliament and Council (2009), ‘REGULATION (EC) No 714/2009 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 July 2009 on conditions for access to the network for cross-border exchanges in electricity and repealing Regulation (EC) No 1228/2003.’ Online. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32009R0714.

[4] European Commission (2017), ‘REGULATIONS COMMISSION REGULATION (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation.’ Online. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R1485.

[5] ACER, ‘Framework Guideline on Demand Response.’ Online. Available at: https://www.acer.europa.eu/Official_documents/Acts_of_the_Agency/Framework_Guidelines/Framework%20Guidelines/FG_DemandResponse.pdf.

[6] European Smart Grids Task Force Expert Group 1 – Standards and Interoperability, ‘My Energy Data’. Online. Available at: https://energy.ec.europa.eu/system/files/2016-11/report_final_eg1_my_energy_data_15_november_2016_0.pdf.

[7] European Smart Grids Task Force Expert Group 1 – Standards and Interoperability – Working Group on Data Format & Procedures, ‘Towards Interoperability within the EU for Electricity and Gas Data Access & Exchange’. Online. Available at: https://energy.ec.europa.eu/system/files/2019-05/eg1_main_report_interop_data_access_0.pdf.

[8] European Parliament and Council (2019), DIRECTIVE (EU) 2019/944 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (recast). Online. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0944.

[9] European Commission (2023), COMMISSION IMPLEMENTING REGULATION (EU) 2023/1162 of 6 June 2023 on interoperability requirements and non-discriminatory and transparent procedures for access to metering and consumption data. Online. Available at: https://energy.ec.europa.eu/publications/implementing-regulation-interoperability-requirements-and-non-discriminatory-and-transparent_en.

[10] IEC SRD 63200 – SGAM basics. Online. Available at: https://syc-se.iec.ch/deliveries/sgam-basics/.

[11] ENTSO-E, ’The harmonized electricity market role model’ version 2022-01. Online. Available at: https://eepublicdownloads.entsoe.eu/clean-documents/EDI/Library/HRM/Harmonised_Role_Model_2022-01.pdf.

[12] ACER, ‘Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows (NCCS)’, July 6, 2022 –V2.3. Online. Available at: https://acer.europa.eu/sites/default/files/documents/Recommendations/Revised%20Network%20Code%20on%20Cybersecurity%20%28NCCS%29_1.pdf.

[13] European Parliament and Council (2016), DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Online. Available at https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[14] European Parliament and Council (2022), 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 (NIS 2 Directive). Online. Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[15] European Parliament and Council (2019a), REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Online. Available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj.

[16] ENTSO-E: “All TSOs’ proposal for the Key Organisational Requirements, Roles and Responsibilities (KORRR) relating to Data Exchange in accordance with Article 40(6) of Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a Guideline on Electricity Transmission System Operation”. Online. Available at: https://www.cnmc.es/sites/default/files/2282482_21.pdf.

[17] European Commission (2011), ‘Energy Roadmap 2050. Impact assessment and scenario analysis’. Online. Available at: https://energy.ec.europa.eu/system/files/2014-10/roadmap2050_ia_20120430_en_0.pdf.

[18] European Commission (2021), ‘Communication from the Commission to the European Parliament and the Council: Action plan to boost long distance and cross-border passenger rail (COM/2021/810 final)’. Online. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2021%3A810%3AFIN.

[19] Sparc, ‘Robotics 2020 Multi-Annual Roadmap’, The Partnership for Robotics in Europe. Online. Available at: https://old.eu-robotics.net/cms/upload/topic_groups/H2020_Robotics_Multi-Annual_Roadmap_ICT-2017B.pdf.

[20] ONC, ‘Connecting Health and Care for the Nation - A Shared Nationwide Interoperability Roadmap. Final Version 1.0’, The Office of the National Coordinator for Health IT. Online. Available at: https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

[21] Lacerda, M., Silva, C., Glória, G., Toro-Cárdenas, M., Egorov, A., Lucas, A., Pestana, R., 2023. D9.2 - Validation and results of concept test – Portugal. OneNet deliverable. Online. Available at: https://onenet-project.eu/wp-content/uploads/2023/05/OneNet_D9.2_v1.0.pdf.

[22] Zafeiropoulou, M.; Bachoumis, T.; Drivakou, K.; Tzoumpas, A.; Bosco, F., 2021, D5.8 -Report on Cybersecurity, privacy and other business regulatory requirements. Online. Available at: https://zenodo.org/records/5948695.

[23] Bytyqi, A. et. al., 2022, D4.1 - Guidelines for TSO Operation and Guidelines for Data Exchange. Online. Available at: https://www.onenet-project.eu//wp-content/uploads/2022/12/OneNet_D4.1_v1.0.pdf.

[24] Augusto, C. et.al., 2023, D4.2 -Guidelines for DSO operation and guidelines for data exchange. Online. Available at: https://www.onenet-project.eu//wp-content/uploads/2023/09/OneNet_D4.2_v1.0.pdf.

[25] Stoyanova, I., Bytyqi, A., Augusto, C. et. al., 2022, D4.3 - Guidelines for TSO-DSO-customer integration system integration plan. Online. Available at: https://www.onenet-project.eu//wp-content/uploads/2022/12/OneNet_D4.3_v1.0.pdf.

[26] Zafeiropoulou, M., Tzoumpas, A. et.al, 2023, D4.4 - Cybersecurity requirements for Grid Operators. Online. Available at: https://www.onenet-project.eu//wp-content/uploads/2023/06/OneNet_D4.4_v1.0.pdf.

[27] OMIE, "Details of the Intraday Market's Operation". Online. Available at: https://www.omie.es/sites/default/files/inline-files/intraday_and_continuous_markets.pdf.

[28] Tsoumakos, Dimitrios & Roussopoulos, Nick. "AGNO: An Adaptive Group Communication Scheme for Unstructured P2P Networks", Proc. 11th international Euro-Par conference on Parallel Processing, August 2005, Pages 1183–1193. https://doi.org/10.1007/11549468_1291183-1193.

[29] Lin, JW., Arul, J.M. & Lin, CY. "Joint deadline-constrained and influence-aware design for allocating MapReduce jobs in cloud computing systems". Cluster Computing. 22. (Suppl 3), 6963–6976 (2019). https://doi.org/10.1007/s10586-018-1981-x.

[30] Narang, Pankaj and Kumari, Mamta and De, Pijus Kanti, A PBCM Approach Analyzing the Manufacturing Cost of NMC-622 Batteries Using EPQ Model and Genetic Algorithm. Available at SSRN: https://ssrn.com/abstract=4261648 or http://dx.doi.org/10.2139/ssrn.4261648 .

[31] Kapetanios, A., Kotsalos, K., Bosco, F. et al., 2023, D6.1 - Report on decentralized edge-level middleware for scalable platform agnostic data management and exchange. Online. Available at: https://www.onenet-project.eu//wp-content/uploads/2023/02/D6.1-OneNet-v1.0.pdf.

[32] Bosco, F. et al., 2023, D6.3 - Extended Interoperability and Management with FIWARE. Online. Available at: https://www.onenet-project.eu//wp-content/uploads/2023/09/OneNet_D6.3_v1.0.pdf

[33] Bosco, F. et al., 2023, D6.4 - AI, Big Data, IoT Orchestration Workbench. Online. Available at: https://www.onenet-project.eu//wp-content/uploads/2023/09/OneNet_D6.4_v1.0.pdf.

[34] Panagou, E. et al., 2023, D6.6 - Tools for Legal, Regulatory, Privacy and Cybersecurity Compliance. Online. Available at: https://www.onenet-project.eu//wp-content/uploads/2023/09/OneNet_D6.6_v1.0-1.pdf.

[35] Tzoumpas, A., Kapetanios, A. et al., 2023, D6.8 - OneNet Framework and Components Final Release. Online. Available at: https://www.onenet-project.eu/wp-content/uploads/2024/01/OneNet_D6.8_V1.0.pdf.

[36] Bachoumis, A. et al., 2021, D5.1 - OneNet Concept and Requirements. Online. Available at: https://zenodo.org/records/5929318.

[37] Lind, L. et al., 2021, D9.1 - Specifications and guidelines for Western Demos. Online. Available at: https://zenodo.org/records/5948735.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Annex A Demo Questionnaires Evaluation of Harmonization Measures

A.1 Platform communication

DEMO	Harmonization action	Potential local impact (1-5)	Potential EU impact (1-5)	Implementation and adaptation cost: detail (text) and value (1-5)	Urgency (1-5)	Recommended time frame for the introduction (1-5-10 yrs)	Expected time frame for the introduction (5-10-15 yrs)	Potential conflicts
Hungary	Standardized communication interface (REST API) between flexibility platforms and FSPs	5	5	Every platform and FSP shall implement the interface. 5	5	1	5	Existing marker participants (FSPs) has to change their modus operandi
Northern	MARI	5	5	Specific API connection 2	5	1	5	
	OneNet Middleware	2	2	Depends on the business case. 2	2	5	5	
	Datahubs of DSO metering data	5	5	Specific API connection 4	5	1	5	Country specific legal based conflicts
Cyprus	Communication of the platforms for TSO, DSO, Market through REST API	4	4	Cost for make the platforms compatible with REST API 2	3	1	1	Autonomy of the different operators
	Cyber-Protected communication	4	5	Cybersecurity systems for ensuring the protection of the platform communication. 4	4	1	5	
Greece								
France								

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Portugal	Standardized communication interface between the technical coordination platforms (RESP APIs)	5	4	2 (relatively low-cost solution for SOs)	4	1	5	None
	Implementation of the OneNet Connector to allow higher degree of replicability	2	4	2 (relatively low-cost solution for SOs)	2	5	5	
Spain	Standardized communication protocol to interconnect different users (MO, DSOs, FSPs) platforms	4	4	2 (low if the decisions are made before individual developments)	5			
Czech	Central platform for all participant	5	3	Central solution can be implemented into some existing central tool. 3	1	2	2	No
	Pre-filled communication formulas	3	1	User-friendly environ-ment based on previous experience. 2	1	2	2	No
Poland	The usage of OneNet Connector	2	4	Already developed tools to communicate between platforms with known technology. 2	3	5	5	Different requirements regarding the role of ONC
Slovenia								

A.2 Flexibility

DEMO	Harmonization action	Potential local impact (1-5)	Potential EU impact (1-5)	Implementation and adaptation cost: detail (text) and value (1-5)	Urgency (1-5)	Recommended time frame for the introduction (1-5-10 yrs)	Expected time frame for the introduction (5-10-15 yrs)	Potential conflicts (text)
Hungary								
Northern	FSP aggregator API	5	5	FSPs connect platform API. 5	4	1	5	
	FSP aggregator UI	5	5	UI for FSP 3	3	2	5	
Cyprus	Communication of the market operator to the FSPs and vice versa	4	4	Provide a seamless communication infrastructure for facilitating the communication of the FSPs to the market and vice versa. 4	4	5	5	Costly implementation of the necessary infrastructure
	Communication of the operators with the flexibility providers	4	4	Communication infrastructure for sending the flexibility required by the operators to the FSPs. 3	4	5	5	Costly implementation of the necessary infrastructure. A standard communication framework needs to be established to allow FSP to manage their power assets (in line with the manufacturers).
Greece								
France								
Portugal	Definition of the format to exchange flexibility needs (json)	4	2	2 (relatively low-cost solution for SOs)	3	1	5	None
	Definition of a methodology to assess flexibility potential	5	2	2 (relatively low-cost solution for SOs)	3	1	5	The demand profile and restriction vary significantly from type of FSP

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Spain	Definition of a common framework to settle imbalance	5	5	4	5	1-2	3	Depending on the model, there could be potential conflicts between Aggregator and Suppliers
Spain	Definition of a common format of information exchange	4	4	2 (low if the decisions are made before individual developments)	5	Soon	2	none
Czech								
Poland	Aggregator as the main unit to provide flexibility	5	3	Elaboration of rules to cooperate between aggregator and FSP's and how to require flexibility from an aggregator from TSO/DSO perspective. 3	3	1	5	Discussion to find solutions, which will be suitable for all stakeholders regarding flexibility
Slovenia								

A.3 Interfaces

DEMO	Harmonization action	Potential local impact (1-5)	Potential EU impact (1-5)	Implementation and adaptation cost: detail (text) and value (1-5)	Urgency (1-5)	Recommended time frame for the introduction (1-5-10 yrs)	Expected time frame for the introduction (5-10-15 yrs)	Potential conflicts (text)
Hungary	Standard Harmonizing communication interface (REST API) between flexibility platforms and TSO	4	4	Beside existing legacy systems a new protocol has to be maintained. 3	4	3		Various market models could have different take on the protocol
Northern	MO<-> Aggregator (FSP)	5	5	Agreement, remuneration, bids, assets (5)	5	5	5	
	FR – FSP interface							
	FR – MO interface							

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

	T&D-CP – SO interface							
	T&D-CP – MO interface							
Cyprus	Middleware between different platform of energy stakeholders (TSO, DSO, FSP)	3	3	Implementation of standardized middleware that will facilitate the transfer of information between the different platforms in a secured way /3	4	5	10	Autonomy between the different operators
Greece								
France								
Portugal								
Spain	Common flexibility interface to facilitate FSPs/Aggregators participation	5	3	4	3	1-2	Not expected	Conflict with individual company interests
Czech	Unify communication channel (ECP)	5	3	Not easy to implement, due to different IT systems of each participant. 4	1	2	2	No
Poland	WebUI (market platform), where every local stakeholder would have common place to perform actions	5	3	Creation of properly working market platform for satisfying interface for all stakeholders 5	4	1	5	Business requirements might not be suitable for system requirements
Slovenia								

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

A.4 Exchanged data

DEMO	Harmonization action	Potential local impact (1-5)	Potential EU impact (1-5)	Implementation and adaptation cost: detail (text) and value (1-5)	Urgency (1-5)	Recommended time frame for the introduction (1-5-10 yrs)	Expected time frame for the introduction (5-10-15 yrs)	Potential conflicts (text)
Hungary	Harmonizing communication interface (Rest API) between flexibility platforms and TSO	4	4	Besides existing legacy systems a new protocol has to be maintained. 3	4	3	5	Various market models could have different take on the protocol
Northern	Bids Flexibility Schedule Metering data Tenders Purchase offers	5	4	Specific APIs (5)	5	1	5	
Cyprus	Communication of the market operator to the FSPs and vice versa	4	4	Provide a seamless communication infrastructure for facilitating the communication of the FSPs to the market and vice versa/3	4	5	5	Costly implementation of the necessary infrastructure
Cyprus	Communication of the operators with the flexibility providers	4	4	Communication infrastructure for activating the flexibility required by the operators to the FSPs/3	4	5	5	Costly implementation of the necessary infrastructure
	Communication of the operators with the flexibility providers	4	4	Communication infrastructure for sending the flexibility required by the operators to the FSPs. /3	4	5	5	Costly implementation of the necessary infrastructure. A standard communication framework to allow FSP to manage their power assets (in line with the manufacturers). A standard communication framework needs to be established to allow FSP to manage their power assets (in line with the manufacturers).
Greece								
France								

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Portugal	Pre-agreed format and schema (data model) between the DSO and TSO for the data exchange	4	2	1 (the cost is related with the platforms developed not this process)	4	1	5	The data model may differ depending on the data requirements for each specific case (and country). Hence, the purpose is more on the agreement between national SOs.
	Definition of schedules for the data exchange aligned with market results	4	2	1 (the cost is related with the platforms developed not this process)	4	1	5	None
Spain	Standardized process for sharing market results (similar to Onenet Connector)	3	5	3	5	2	5	None
	Schedule of processes harmonized with the other energy markets to be fully integrated	5	5	2	4	As soon as local flexibility markets negotiation starts	1-2	None
Czech	Outages (TSO-DSO)							
	Common TSO and DSO flexibility register – identification, contracted services							
Poland	Creation of common definitions and data structures for stakeholders	4	4	Arrangements and adaption - 3	3	5	5	-
Slovenia								

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

A.5 Protocols

DEMO	Harmonization action	Potential local impact (1-5)	Potential EU impact (1-5)	Implementation and adaptation cost: detail (text) and value (1-5)	Urgency (1-5)	Recommended time frame for the introduction (1-5-10 yrs)	Expected time frame for the introduction (5-10-15 yrs)	Potential conflicts (text)
Hungary								
Northern	HTTPS							
Cyprus	Define standardized communication protocols for the seamless communication of the different platforms/entities	5	5	Define and implement a strategy for making compatible the different devices/platforms in an interoperable environment considering the compatibility of the protocols/5	5	1	5	Autonomy of the different entities. Hard modification of the platforms to new protocols.
Greece								
France								
Portugal	Use of HTTPS for secure communication	4	4	1	4	1	1	None
Spain	HTTPS protocol for secure communication	5	5	1 (very low, broadly used solution)	4	1-2	3	None
Czech								
Poland	Secure communication through HTTPS protocol	3	3	Standard, known technology – 1	1	1	1	-
Slovenia								

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

A.6 Data exchange formats

DEMO	Harmonization action	Potential local impact (1-5)	Potential EU impact (1-5)	Implementation and adaptation cost: detail (text) and value (1-5)	Urgency (1-5)	Recommended time frame for the introduction (1-5-10 yrs)	Expected time frame for the introduction (5-10-15 yrs)	Potential conflicts (text)
Hungary								
Northern	HTTPS							
	JSON							
Cyprus	Specification of different data exchange formats for different applications according to the execution time requirements	2	2	According to the application and its time requirements different data exchange formats should be specified in a local and European level/2	2	5	10	Autonomy
Greece								
France								
Portugal								
Spain								
Czech								
Poland	All data exchanges supported with WebUI and email	1	1	Standard, data exchange through market platform (part of development of market platform) – 1	4	1	1	-
Slovenia								

A.7 Data models

DEMO	Harmonization action	Potential local impact (1-5)	Potential EU impact (1-5)	Implementation and adaptation cost: detail (text) and value (1-5)	Urgency (1-5)	Recommended time frame for the introduction (1-5-10 yrs)	Expected time frame for the introduction (5-10-15 yrs)	Potential conflicts (text)
Hungary	Harmonization JSON data models between flexibility platforms and FSPs	5	5	Every platform and FSP shall implement the interface. 5	5	1	5	Existing marker participants (FSPs) has to change their modus operandi
Northern	CIM-XML							
	CIM-JSON							
Cyprus	Specification of different data models for different applications	2	2	According to the application different models should be specified in a local and European level/2	2	5	10	Autonomy
Greece								
France								
Portugal	XML	5	2	2 (relatively low-cost solution for SOs)	4	1	5	
	JSON	5	2	2 (relatively low-cost solution for SOs)	4	1	5	
Spain	XLS (for downloading market results)	3	3	2	4	1-2	3	None
	TXT (for downloading market results)	3	3	2	4	1-2	3	None
Czech								
Poland	All additional data is exchanged between all stakeholders through XLSX	1	1	Standard XLSX, created during development - 2	1	5	5	-
Slovenia								

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

A.8 Cyber security

DEMO	Harmonization action	Potential local impact (1-5)	Potential EU impact (1-5)	Implementation and adaptation cost: detail (text) and value (1-5)	Urgency (1-5)	Recommended time frame for the introduction (1-5-10 yrs)	Expected time frame for the introduction (5-10-15 yrs)	Potential conflicts (text)
Hungary								
Northern	Identification/ Authentication							
	Metering data - consents							
	Bid data							
Cyprus	Cyber-Protected communication between the platforms /components of the same entity (i.e. TSO, DSO, etc.) as well as the cross-layer communication (TSO-DSO, DSO-FSP, etc.).	4	5	Design and installation of cyber-security systems for ensuring the protection and privacy of the communication between different entities in the power systems/4	4	1	5	
Greece								
France								
Portugal	Implementation of token-based authentication	4	4	2	4	2	5	None

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

	Use of HTTPS for secure communication	4	4	1	4	1	1	None
Spain	Digital certificate authentication	4	4	2	4	1-2	3	None
	HTTPS protocol	5	2	1 (very low, broadly used solution)	4	1-2	3	None
Czech								
Poland	Authorization and tokenization with JSON Web Tokens	2	3	Known technology, easy to implement – 1	5	1	5	
	Human-based user authorization	1	1	Creation a tool for Market Operator to perform registration processes – 2	5	1	5	
Slovenia								

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

A.9 Market algorithms

DEMO	Harmonization action	Potential local impact (1-5)	Potential EU impact (1-5)	Implementation and adaptation cost: detail (text) and value (1-5)	Urgency (1-5)	Recommended time frame for the introduction (1-5-10 yrs)	Expected time frame for the introduction (5-10-15 yrs)	Potential conflicts (text)
Hungary								
Northern	Joint TSO-DSO optimisation-based market clearing algorithm	5	4	5	3	5	5	Integration with other markets (e.g. MARI)
Cyprus	Harmonization of market clearing algorithms	2	2	Develop and adapt the same market clearing algorithms in the pan European grid/2	2	5	5	Autonomy of the different market operators, regulatory barriers
Greece								
France								
Portugal								
Spain								
Portugal								
Spain								
Czech								
Poland	AGNO, DGIA, PBCM algorithms	3	3	Complicated algorithm for providing expected data flows and implementation of the algorithm to the platform – 4	3	5	15	Finding proper structure for the algorithm, which should be fast-compiling, easy to operate and reliable
Slovenia								

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

A.10 System operations

DEMO	Harmonization action	Potential local impact (1-5)	Potential EU impact (1-5)	Implementation and adaptation cost: detail (text) and value (1-5)	Urgency (1-5)	Recommended time frame for the introduction (1-5-10 yrs)	Expected time frame for the introduction (5-10-15 yrs)	Potential conflicts (text)
Hungary								
Northern								
Cyprus	Harmonization of the accuracy of the tools for forecasting and monitoring	3	3	Develop and adapt monitoring and forecasting tools that meet certain specifications and requirements related to the accuracy/2	3	5	10	Autonomy of the different stakeholders.
Greece								
France								
Portugal	Frequent (daily) information exchange between DSO and TSO for better operational planning activities (e.g., increased accuracy of forecasts)	4	2	3 requires process automation	3	1	5	
Spain								
Czech								
Poland	Settlement and activation provided through market platform	2	2	Basic tool to manually fulfill data regarding settlement amount and activated volume – 1	1	1	5	-
Slovenia								

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739