ONENET
one network for Europe

Report on the second GRIFOn Meeting

D12.3

Authors:

Nadja Novak (ELES)

Sebastian Vogel (E.DSO)

José-Pablo Chaves Ávila (Comillas)

Ivelina Stoyanova (RWTH Aachen)

Ioannis Theologitis (ENTSO-E)

Responsible Partner	10 – ELES
Checked by WP leader	Padraic McKeever (Fraunhofer), 15.03.2023
Verified by the appointed Reviewers	Carmen Gutiérrez Moles (IDAE), 24.03.2023 Václav Janoušek (CEZ DISTRIBUCE), 27.03.2023
Approved by Project Coordinator	Padraic McKeever (Fraunhofer), 30. 03.2023

Dissemination Level	
PU	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	31.03.2023
Actual date of delivery	30.03.2023

Version	Date	Author(s)	Notes
0.1	16.01.2023	Nadja Novak	Initial draft version
0.2	31.01.2023	Sebastian Vogel	Updates in Ch. 3
0.3	02.02.2023	José-Pablo Chaves Ávila	Updates in Ch. 3
0.4	03.02.2023	Ivelina Stoyanova	Updates in Ch. 3
0.5	21.03.2023	Nadja Novak	Ready for review
0.5	22.03.2023	Ioannis Theologitis	Updates in Ch. 3
0.6	27.03.2023	Padraic McKeever	Updates acting on review comments

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.

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

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 optimises 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 fully centralised to a highly decentralised system, grid operators must 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 seventy 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 standardised 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 organised 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

List of Abbreviations and Acronyms

Acronym	Meaning
ACM	Authority for Consumers and Markets
ADMS	Advanced Distribution Management System
AMI	Advanced Metering Infrastructure
API	Application Programming Interface
CGMES	Common Grid Model Exchange Standard
CIM	Common Information Model
DER	Distributed Energy Resources
DR	Demand Response
DSO	Distribution System Operator
EEBUS	Protocol suite for the Internet of things that aims to standardise the interface between electrical consumers, producers, storages and (logical) managing entities.
EMS	Energy Management System
eTOM	enhanced Telecom Operations Map
EU	European Union
FSP	Flexibility Service Provider
GDPR	General Data Protection Regulation
GPRS	General Packet Radio Service
GRIFOn	Grid Forum
ICT	Information and Communications Technology
IoT	Internet of Things
IT	Information Technology
MDM	Mobile Device Management
OT	Operational Technology
RES	Renewable Energy Sources
SAREF	Smart Applications REFerence
SCADA	Supervisory Control and Data Acquisition
TSO	Transmission System Operator
UBA	User Behaviour Analytics
WP	Work Package

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

Executive Summary

GRIFOn is an innovative approach to generating European-wide consensus about OneNet proposed solutions by integrating external stakeholders in developing key solutions. GRIFOn is implemented via workshops on specific project-related topics. Deliverable 12.3 is the report on the second GRIFOn workshop, which took place virtually on 16th May 2022 on the platform Wonder. The focus of this workshop was on "TSO-DSO-Customer Interoperability and Integration." Ninety people registered for the workshop, and forty attended the event.

The workshop participants participated in the group sessions on topics related to the TSOs, DSOs and end customers. Each group discussed several pre-defined questions on interoperability, cybersecurity, and how to integrate flexibility. In addition, there was a focus on getting the participants' views on where the problems, barriers and gaps lie.

Some of the key outcomes were:

- Regarding interoperability, it was agreed that developing common standards for data exchange (of grid data, electricity data, real-time data, etc.) is vital, both between TSOs and DSOs and between DSOs and customers. This goes hand in hand with both the need to share data between authorised stakeholders and being able to address that need.
- The groups considered the barriers to data exchange from DSO-TSO, DSO-Consumer, and Consumer-market standpoints. The technical, regulatory and standardisation barriers are common to these pairs. However, where customers are involved, there are additional privacy considerations, data ownership, monetary compensation, motivation, and trust. Additionally, the issues of GDPR being transposed differently in different countries, the need to harmonise data models and the need for data quality rather than sheer quantity was highlighted.
- The complexity and breadth of cybersecurity in electricity grids are highlighted by the different but interlinked facets of the problem. Cybersecurity was brought up by the discussions in the different groups, ranging from the security of the grid components and systems to the need for data governance – both as an enabler of cybersecurity and also to provide a stable business environment, to the need to ensure the privacy of customer data.

This second GRIFOn workshop was held about six months earlier than initially foreseen in the OneNet project plan. Nevertheless, its results have been available to, and have been used by, the project's "horizontal" work packages dealing with market structures, network operation and IT solutions.

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

1 Introduction

The Grid Forum (GRIFOn) is an initiative launched by OneNet to promote and facilitate the creation of a community of stakeholders interested in collaborating and actively tackling the most pressing issues regarding the future European electricity markets. It will leverage different mechanisms of inclusion tailored to each stakeholder group to ensure their engagement over the project's lifetime and beyond. GRIFOn will create a unique European-wide consensus and acceptance of OneNet's proposed concepts and solutions.

GRIFOn has three main objectives:

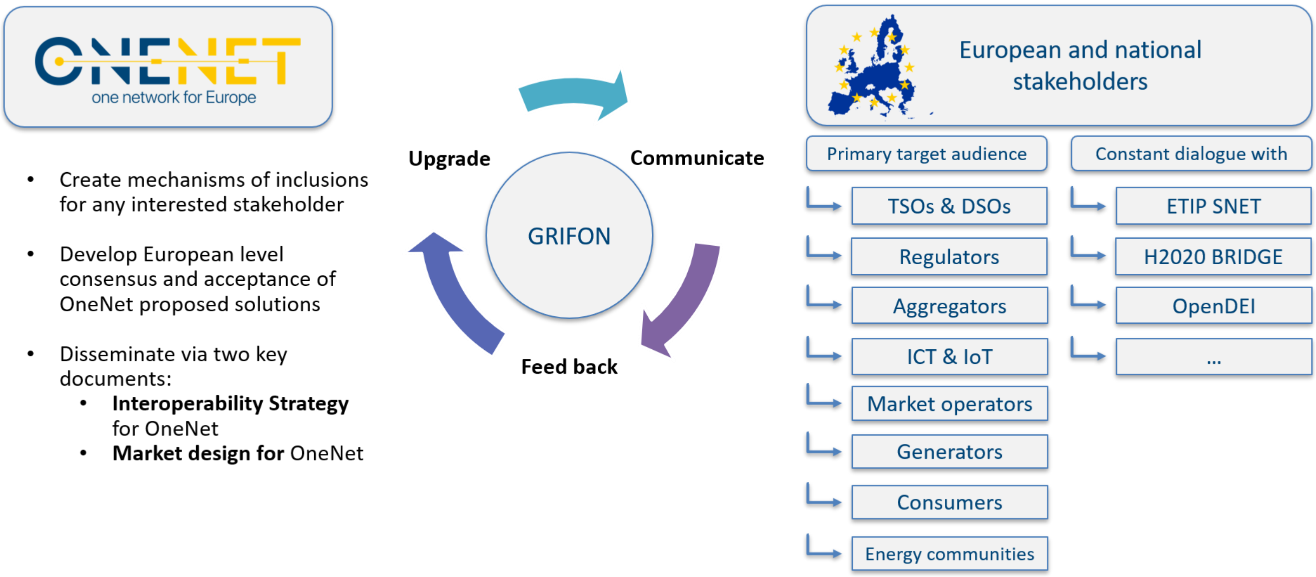
1. Co-determination OneNet's project results through the participation of all relevant stakeholders.
2. Europe-wide knowledge sharing on how to shape an integrated European energy market.
3. Consolidation of a shared vision of the European energy markets and systems by building consensus of OneNet proposed solutions among both project- and non-project parties.

In the context of the OneNet project, GRIFOn's primary outcome will be two whitepapers at the end of the project. The first document is titled **Interoperability Strategy for OneNet,** and the second is **Market design for OneNet.** Both papers will summarise some of the key results of the OneNet project.

1. **Interoperability Strategy for OneNet:** An essential aspect of an integrated European electricity system that considers the regional differences of the Member States is interoperability between its stakeholders and their systems. Following the system-of-system approach, the document will outline the path towards an interoperable and federalised European electricity market.
2. **Market design for OneNet:** GRIFOn will foster the development of a fragmented electricity market landscape (particularly for balancing and non-frequency ancillary services) towards an integrated pan-European one. This document will provide a comprehensive overview of the current situation and outline the next steps for a unified European electricity market design.

The OneNet consortium concludes that interactive/engaging workshop formats are the most promising for knowledge exchange between the project consortium and external stakeholders in the framework of the GRIFOn. Alternative ways of knowledge exchange, like surveys and open consultations, may be used to support the workshop format. The OneNet project welcomes all stakeholders to create a European consensus on operating the electrical system as one system based on a combination of existing and new concepts and solutions. GRIFOn may primarily address and encourage TSOs & DSOs, regulators, aggregators, ICT & IoT companies, market operators, energy suppliers, energy communities and consumer organisations to engage with GRIFOn.

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



- Create mechanisms of inclusions for any interested stakeholder
- Develop European level consensus and acceptance of OneNet proposed solutions
- Disseminate via two key documents:
  - **Interoperability Strategy** for OneNet
  - **Market design for** OneNet

Figure 1.1: GRIFOn organisation

GRIFOn enables OneNet to continuously dialogue with external stakeholders by allocating dedicated resources to this task. But it is still challenging to implement a constant communication flow between a large group of stakeholders. OneNet tackles this challenge with the support of the entire project consortium. To communicate the GRIFOn idea, OneNet created Figure 1.1, which visualised the continuous GRIFOn circle. In addition, GRIFOn provides us with a communication forum which leads to feedback on OneNet's working topics, which allows us to upgrade our project results if necessary. The following report describes our approach to implementing GRIFOn, focusing on our second GRIFOn workshop on TSO-DSO-Customer Interoperability and Integration, which took place on the Wonder Platform in May 2022.

This report consists of four chapters. Chapter one provides information on GRIFOn. Chapter two introduces our approach to implementing the second GRIFOn workshop and presents background information on defining topics, stakeholders, and workshop design. Chapter three reports on the results of the second GRIFOn workshop. Chapter four summarises our plans for the next GRIFOn activity based on the learnings from the past two workshops and presents our conclusions.

2 The GRIFOn approach

The OneNet consortium identified early that a structured process is necessary to manage an activity like GRIFOn. Therefore, we defined a method to help us implement a GRIFOn activity/workshop. This process follows a 6-step approach.

1- **Identify topic:** Identify concrete OneNet-related outcomes/deliverables that can benefit from external feedback (what, by when is the input required).

2- **Identify stakeholders:** Identify the type of stakeholder and the individual stakeholders/associations from whom feedback can be valuable.

3- **Preliminary planning:** Decide on the form in which this feedback is ideally received (I.e., survey, workshop, track-changes review of deliverables, or a mixture of these…).

4- **Detailed planning:** Define responsible OneNet partner and organise stakeholder engagement action with GRIFOn lead.

5- **Implementation and promotion:** Carry out stakeholder engagement action.

6- **Feedback:** Feed the outcome of the stakeholder engagement action into the relevant living document.

The following subsections describe how we followed this process to implement the second GRIFOn workshop.

2.1 Step 1: Identify the topic

The OneNet project can be roughly separated into three phases that largely overlap and interchange. These phases are:

- developing new flexibility products, services and associated market setup;
- development and implementation of the OneNet IT system and verification of the concepts and solutions proposed by OneNet in a set of large field tests;
- gathering data and evaluating the project outcome.

In the second year of OneNet, the WP4 project partners stressed their work would benefit from obtaining stakeholder feedback. As a result, WP12 concluded that GRIFOn should organise the second workshop, which will focus on "TSO-DSO-Customer Interoperability and Integration."

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

2.2 Step 2: Identify stakeholders

During the dedicated GRIFOn Stakeholder Task Force meetings, project partners discussed the feedback on OneNet's activities/proposals/findings from which stakeholder groups are needed. As a result, project partners identified seven relevant stakeholder groups:

- Transmission and Distribution System Operators.
- Regulators.
- Aggregators.
- Market Operators.
- Industrial and Residential Consumers Organisations.
- Energy producers Associations.
- ICT/IoT providers/platforms.

Each stakeholder group was further segmented, and a detailed list of individual stakeholders within each relevant stakeholder group was made. The list was the basis on which GRIFOn Task Force determined from which stakeholders' feedback at the second workshop was wanted. They identified the following stakeholder groups as the most important:

- Transmission and Distribution System Operators.
- Regulators.
- Industrial and Residential Consumers Organisations.
- Energy producers Associations.
- ICT/IoT providers/platforms.
- Data exchange experts.
- Representatives of other relevant Horizon projects.

2.3 Steps 3 and 4: Planning the second GRIFOn event

During the discussion at the dedicated GRIFOn Task Force meeting, it was agreed that the most urgent stakeholder feedback is needed for Task 4.1 (Flexibility services integration and data exchange at TSO level for interoperability towards the distribution system) and Task 4.2 (Flexibility services integration and data exchange at DSO level for interoperability towards the transmission system). Therefore, the second GRIFOn event took place on 16 May 2022 as an online workshop.

After the first workshop, the GRIFOn task force evaluated the organisation and implementation of the event. The organisers were satisfied with the number of participants and a little less with the interactivity of the discussion. Therefore, the Task Force started to explore different options for encouraging two-way

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

communication with the stakeholders and making webinars more interactive. Various virtual conference systems were in the discussion - Zoom, MS Teams, and Wonder, that should be combined with web applications such as Miro, Slido, Mentimeter and others. Finally, the Task Force decided on the Wonder conference system combined with the Miro web application for the breakout sessions.

Project partners decided that the workshop should be organised as follows:

- Plenary session with the general presentation of the OneNet project, GRIFOn and the introduction to the tools used at the event: The plenary session aimed to present the OneNet project's vision and demonstrations that will test the developed market concepts in real life. Stephan Gross from Fraunhofer Institute presented the vision and three thematic pillars, the four demonstration clusters that will test new market concepts in real-time, and the idea behind the GRIFOn platform. After the introduction, the technical moderators introduced the tools used at the event, and the participants left the plenary session and joined one of the nine discussion groups. At the end of the group discussions, the participants re-joined the plenary session, where the moderators presented the key results of each thematic pillar.
- Breakout sessions – discussions in the TSO, DSO and Customer subgroups: We defined three thematic pillars for the group discussions - TSO, DSO, and Customers. Each thematic pillar was divided into three sub-groups. For each sub-group, three questions for the debate were prepared. Each sub-group used a Miro board for gathering feedback.

  In the beginning, moderators explained to the participants they would have to write down their ideas and thoughts on a set of questions on the Miro board. They stressed that participants must also formulate their comments/answers in a way understandable to others. During the sub-group discussions, moderators shared their screens with the Miro board. Every question started with 5 minutes of silent brainstorming, where everyone in the group added sticky notes in the section "Things considered" on the Miro board. This was followed by a 10-minute discussion. Finally, the moderators asked for feedback on the sticky notes in the area Things considered and wrote sticky notes in the section Discussion and agreements and Arguments beyond question/topic. In the end, the moderators closed the group discussion and announced a short break. The moderators then moved to the help section to form a circle with all the other moderators, where they prepared conclusions for each thematic pillar. After that, participants moved back to the plenary session circle.

- A plenary session with the presentation of the summaries from the breakout session.

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

The agenda of the workshop is presented in Table 2.1.

Start time	Stop time	Timeframe	Comment	Speaker
9:30	9:40	00:10	Welcome and Introduction of OneNet and GRIFOn	Stephan Gross
9:40	9:55	00:15	Introduction to the tools and moderators of the event	Technical moderators
9:55	10:00	00:05	Splitting up into discussion groups	Participants
10:00	11:00	01:00	Breakout sessions 1. TSO 2. DSO 3. Consumers	Moderators
11:00	11:30	00:30	Break and Networking	Participants
11:30	12:15	00:45	Summary session 15min per topic with a chance for further feedback and comments from the participants	Moderators + Participants
12:15	12:30	00:15	Closing words	Stephan Gross

Table 2.1 Agenda of the second GRIFOn workshop

2.4 Step 5: Implementation and promotion

The project partners disseminated information about the workshop to various stakeholders and tried to attract them to participate. Therefore, they prepared a dedicated sub-page on the OneNet project website[1], where the invitation to participate in the event, agenda and registration link were published. Additionally, the registration form was prepared on the Eventbrite platform for user-friendly registration to the event.[2] Furthermore, news about the workshop was published on OneNet's web page and social media channels. Also, all project partners were asked to share information about the workshop on their digital communication channels and among their connections from the pre-defined stakeholder groups.

2.5 Feedback

The last step of the GRIFOn event circle is to collect the feedback received during the GRIFOn workshop and to utilise it for further developments of the OneNet project results. The discussion results find their way directly back into the work of Tasks 4.1 and 4.2.

[1] https://onenet-project.eu/the-grid-forum-grifon-on-tso-dso-consumer-data-exchange/

[2] https://www.eventbrite.fr/e/onenet-the-grid-forum-grifon-on-tso-dso-consumer-data-exchange-tickets-323250108777

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

3 Results of the second GRIFOn workshop

3.1 TSO group discussion

Three questions were prepared for each sub-group for the discussion in the TSO thematic pillar. However, participants interested in the topics important from the transmission system operators' point of view participated only in the two sub-groups, so the questions from the sub-group TSO 3 were not debated.

Sub-group TSO 1	Sub-group TSO 2	Sub-group TSO 3
What are the best TSO-DSO and Customer Interoperability approaches to consider?	What are the most pressing gaps that should be addressed regarding data exchange and interfaces?	To what extent the current CIM standards should be adapted to cover data related to energy forecast, DER and flexibility?
How to overcome existing barriers for TSO-DSO data exchange: country restrictions, data restrictions, legal issues, agreements, etc.?	Which common standards should be prioritised to improve interoperability?	What are the best TSO-DSO and Customer Interoperability approaches to consider?
Which are the cybersecurity challenges when interfacing IT with OT?	In your opinion, which systems are of the highest priority when implementing new cybersecurity measures?	What do you consider to be the greatest security risk in the future?

Table 3.1 TSO sub-groups questions

3.1.1 Sub-group TSO 1

Question 1: What are the best TSO-DSO and Customer Interoperability approaches to consider?

The box below records the outcome of the Miro board session, After the box is a summary of the subsequent discussions. We followed the same approach also in the following sub-chapters.

Discussion and agreements

- Develop role models at the European level.
- TSOs and DSOs should also raise awareness among customers about changes in the energy sector.
- Increase information exchange in an automatic mode.
- Develop common standards for data exchange.
- TSOs need more data from DSOs as RES is increasingly connected to the distribution grid.

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

- Create a data hub or central exchange platform between TSO and DSO.
- Note the increased need for two-way transport/ communication as RES is integrated into small scales.

Arguments beyond question/topic

- Use of the Blockchain - to give restricted access to selected data.
- Share relevant data with each stakeholder, including other stakeholders such as certification parties.

The topics debated in question 1 covered standardisation, open data exchange and IT support.

Standardisation was seen as key to ensuring interoperability. There is a need to develop common standards for open data exchange and increase the automatic exchange of information. This approach allows all parties to access the same data in real time, facilitating better decision-making and reducing the risk of errors. Open data exchange (of grid data, electricity data, real-time data, etc.) requires using a common data model. Blockchain technology was highlighted as a method for data access control, i.e., ensuring that only authorised people can access data. Relevant data should be shared with each stakeholder, including other stakeholders such as certification parties.

The development of role models at the European level was considered important. Role models can showcase best practices and standards for interoperability, promote collaboration and knowledge-sharing among TSOs, DSOs, and customers, be used as a benchmark to measure the performance of TSOs, DSOs, and customers in terms of interoperability, as well as providing support for policy development at the European level.

As more DERs are integrated into the grid, TSOs need more data from DSOs to manage the system effectively. DERs' management systems should be designed to enable communication and coordination among all parties, with real-time bi-directional data exchange and control to the extent necessary for ensuring the system's optimised and safe operation. Therefore, it is necessary to create a data hub or central exchange platform between TSOs and DSOs.

Additionally, TSOs and DSOs or any other competent authority, e.g. the national regulator or ministry, need to raise customers' awareness about changes in the energy sector.

Question 2: How can we overcome existing barriers for TSO-DSO data exchange: country restrictions, data restrictions, legal issues, agreements,…?

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

Discussion and agreements

- Writing common exchange specifications and common EU legislation.
- Agreements are necessary regarding data models, communication protocols, data formats, tools, etc.
- Standards must be agreed upon at a European level - which may take time to integrate into existing systems—understanding TSO, DSO, and customer requirements.

Arguments beyond question/topic

- Data exchanges in the boundary and specific areas should be clarified.
- Some large customers may influence cross-border flexibility.

Overcoming existing barriers for TSO-DSO data exchange requires a multi-faceted approach that addresses technical, organisational, and regulatory issues. Here are some ways to overcome these barriers:

1 <u>Technical Solutions</u>: Technical solutions such as standardised communication protocols, data models, tools and data dictionaries can help to facilitate data exchange between TSOs and DSOs.

2 <u>Organisational Collaboration</u>: Collaboration between TSOs and DSOs is crucial for effective data exchange. Establishing joint teams or working groups to identify common goals and better understand TSO, DSO and customer requirements and needs; developing common standards at a European level, which may take time to integrate into existing systems; establishing common processes can help to promote cooperation and trust.

3 <u>Legal Framework</u>: A clear legal framework that establishes the rights and obligations of TSOs and DSOs concerning data exchange is essential. This framework should address data ownership, liability, protection, and confidentiality issues. Harmonisation of legal requirements across different countries can help to remove legal barriers to data exchange. There is already a sound basis for the legal framework (Network Codes and/or Guidelines), which must be enhanced and detailed in respective methodologies according to the different requirements.

4 <u>Regulatory Framework</u>: The regulatory framework should support data exchange by setting clear rules for data access, sharing, and protection. The regulatory framework should also provide incentives for TSOs and DSOs to share data, such as regulatory requirements or financial incentives. It was remarked that some large Customers might influence cross-border flexibility.

5 <u>Data Governance</u>: Clear data governance structures and processes can help ensure data is exchanged securely and efficiently. Data governance should address data quality, accuracy, completeness, and security issues. It should also establish clear roles and responsibilities for data owners, users, and custodians.

Question 3: Which cybersecurity challenges are you experiencing when interfacing IT with OT?

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

Topics considered

- Potential impacts → areas.
- Identify critical assets.
- Energy systems operational technologies (technical security controls and techniques).

Discussion and agreements

- Loss of production units, market disruption and loss of potential revenue for generators and impact on demand non-supplied.
- Impact on the availability of Web Platforms.
- Problems with Energy Management Software.
- Interrupted control functions, remote access to primary equipment for the attackers, and loss of revenue.
- Interrupted Databases and client data.
- Unavailability to access various systems.
- Meter tampering, the possibility of faulty controls, breach of data privacy for customers.

Arguments beyond the proposed question/topic

- Energy systems operational environments (organisational and procedural security controls).
- Interrupted system operation and control, power outages and possibility for cascading effects.
- User Behaviour Analytics (UBA).
- Mobile Device Management (MDM).
- General IT security reflecting business requirements.

Participants highlighted the identification of critical assets and energy systems operational technologies (technical security controls and techniques) as areas to focus on in the discussion.

Some of the challenges are:

- IT and OT systems are part of the critical infrastructure; therefore, cyber-attacks on these systems can have severe consequences on the functioning of the electrical grid. As a result, TSOs and all relevant technology and asset providers must ensure their systems are secure and resilient against cyber-attacks. Cyber-attacks can lead to severe consequences: loss of production units, market disruption, loss of revenue, unavailability of Web Platforms, interrupted databases and client data, unavailability to access various systems, problems with Energy Management software and interrupted control functions and loss of revenue. Additionally, there is the threat of meter tampering, the possibility of faulty controls, and the data privacy breach for customers. Finally, potentially interrupted system operation and control can lead to severe consequences such as power outages and the possibility of cascading effects.

- Ensuring cybersecurity also means addressing the energy systems' operational environments, including organisational and procedural security controls. It must be discussed on a general (holistic) level, but the IT and OT security must also reflect the business requirements.
- The overall topic of cybersecurity in the electricity/energy system has been highlighted over the last years with a dedicated network code in the drafting phase and several national initiatives to ensure a safe system operation.

User Behaviour Analytics (UBA) and Mobile Device Management (MDM) were also opened in the discussion.

3.1.2 Sub-group TSO 2

Question 1: What are the most pressing gaps that should be addressed regarding data exchange and interfaces?

Topics considered

- Examples
- Privacy

Discussion and agreements

- Gaps depend on the region
- User data model
- User privacy
- Grid data model
- IT security
- Standard for interfaces

Although the gaps depend on the region, the following areas were seen to be relevant:

1. Standardisation: There is a lack of standardisation in data exchange interfaces between TSOs and other stakeholders, such as DSOs, generators, and consumers. Standardisation of interfaces and data models can improve interoperability and reduce the complexity of data exchange interfaces.
2. Data Quality: The quality of data exchanged between TSOs, and other stakeholders can be inconsistent, incomplete, or inaccurate. This can lead to errors in operational decision-making and hinder the integration of renewable energy sources into the electrical grid.

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

3. Cybersecurity: The data exchange between TSOs and other stakeholders can create cybersecurity risks. These risks can be mitigated by implementing security controls, such as encryption and access controls, and by ensuring that all parties follow best practices for cybersecurity.
4. Data Privacy: Data exchange between TSOs and other stakeholders can also create privacy risks. TSOs must ensure that they comply with relevant privacy regulations and that sensitive data is protected from unauthorised access.
5. Scalability: The increasing complexity and volume of data exchanged between TSOs, and other stakeholders can create scalability challenges. TSOs must ensure that their data exchange interfaces can handle large volumes of data and are flexible enough to adapt to changing requirements.
6. Interoperability: Interoperability between different data exchange interfaces can be challenging, primarily when stakeholders use different systems or protocols. TSOs must ensure their data exchange interfaces are interoperable with other systems to facilitate seamless data exchange.

Question 2: Which common standards should be prioritised to improve interoperability?

Discussion and agreements

- Market & product related
- CIM
- CGMES

The participants thought that market and product-related standards should be prioritised. They identified CIM and CGMES where several harmonisation and implementation developments have been performed in the system operation environment and system development. These enable exchanges of the data necessary for regional or pan-European grid development studies and system operation processes required by the network codes. The standards are continuously evolving to meet the changing requirements for data exchange, which are increasing in frequency and type, with higher RES integration and the introduction of smart grids.

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

Question 3: In your opinion, which systems are of the highest priority when implementing new cybersecurity measures?

Topics considered

- All have the same risk.

Discussion and agreements

- SCADA systems
- Electricity production units
- Monitoring and dispatch systems
- Digital interfaces
- Smart metering systems
- Billing systems

The participants thought that all systems, tools and assets have the same risk. Several examples have been mentioned during the discussion:

- SCADA systems
- Electricity production units
- Monitoring and dispatch systems
- Digital interfaces
- Smart metering systems
- Billing systems

The European cybersecurity law aims to address the cybersecurity challenges in the energy sector. It addresses the need for more IT and tools, more data exchange, more overall security requirements (beyond any local rules) and interoperability which, of course, increase the level of vulnerabilities and the risks for cyber threats. The coming EU network code will enable sufficient cybersecurity across the European power system, set up common criteria for cross-border risk assessment, collect and share essential information on a broader area more securely, and enable effective crisis management to handle cyber incidents.

3.2 DSO group discussion

Three questions were also prepared for each of the three DSO sub-groups. The questions from sub-group DSO 3 were not debated since there were few participants, and due to time constraints, the questions of group 3 could not be tackled by the other sub-groups. However, the discussions of both groups provided insightful exchanges.

Sub-group DSO 1	Sub-group DSO 2	Sub-group DSO 3
Most pressing gaps to be addressed in terms of data access (observability of data from external parties/ resources connected to the grid) for DSO?	What are the 3 most concerns for DSOs regarding data exchange when integrating flexibility?	What are the current barriers to DSO-TSO coordination regarding data exchange? How can they be solved?
What are the current barriers to DSO-Consumer interaction regarding data exchange? How can they be solved?	Can data models and protocols be standardised at DSO level? If not, what are the barriers for this? (e.g. CIM)	The CIM data model is used mainly by TSO, but it is not a widely adopted DSO. What is needed to enhance the use of CIM by DSOs?
In your opinion, which systems are of the highest priority when implementing new cybersecurity measures?	Do you think that an information risk-management strategy is essential for every organisation?	What do you consider to be the greatest security risk in the future?

Table 3.2 DSO sub-groups questions

3.2.1 Sub-group DSO 1

Question 1: What could be the most pressing gaps to be addressed in terms of data access (observability of data from external parties/resources connected to the grid) for DSO?

Topics considered

- Lack of data
- Interoperability
- Missing data
- Standards ambiguity

Discussion and agreements

- Very country specific legislation, rules, and acts
- GDPR
- Time and resources – we are so focused on projects.
- Harmonised data format

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

- Data models
- Common data formats, including APIs.
- Data exchange standards (common process models, widely approved and recognised (see eTOM for telco)
- Not plug-and-play solutions
- Identification of data streams
- Missing proper data exchange
- Interfaces for exchange
- Clear specifications: what can of data, in which format
- Data validity/quality
- Skills in data analytics

The participants came up with four main topics to be discussed: (1) access to available data, (2) barriers to interoperability, (3) gaps by missing data, and (4) ambiguity of specific standards. As expected, all points pivot around data and interoperability.

The breakout room participants discussed the topics, which led to the depicted sticky notes on the Miro board. They can be clustered into legal requirements, data models, and data utilisation.

First, European Member States have transposed EU legislation to different forms and extents. This leads to uncertainty about applicable law in different regional areas. While the GDPR, as a regulation rather than a directive, is directly applicable in Member States, it caused high burdens on involved stakeholders. Such obligations include time and personnel resources that cannot be put into innovation simultaneously.

Second, data models need to be harmonised. Common data formats, including APIs and connectors, should be used in various projects and countries. An uptake of data exchange standardisation is required to account for new but already widely recognised process models (see eTOM for the telecommunication industry). However, it must be noted that data models are no plug-and-play solutions but require specific use cases and extensions. Data streams must be identified to evaluate gaps and respective interfaces.

Finally, the focus should be on data quality rather than sheer quantity. Data sources and processes need to be validated, which requires computational resources, business use cases, and skills in data analytics. Therefore, in line with the previous point and to ease this work, precise specifications of data and formats are needed.

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

Question 2: What are the current barriers to DSO-Consumer interaction regarding data exchange? How can they be solved?

Topics considered

- Data sovereignty

Discussion and agreements

- Lack of motivation from consumer side (knowledge regarding the energy system).
- Consumer is sceptical about DSO. Not aware of data usefulness.
- Consumers are reluctant to provide data.
- Engagement Strategies.
- DSO vs Retailer.
- Lack of standards on consumer side (devices behind the meter can make it a barrier, like PV and batteries).
- Bad reputation on DSO side.
- Road map smart meters: The level of smart meter implementation. Generation of smart meters. New ones have longer lifespans and functions.
- Aggregation vs Individual.

For the second question, only one topic was identified - Data sovereignty, which includes the aspects of data ownership and processing responsibilities.

The discussants identified various topic areas, mainly available knowledge and aggregating data.

There needs to be more motivation from the consumer side. This might be caused by insufficient engagement strategies and lacking knowledge regarding the overall energy system, for instance, the separation of the DSO and retail business. In addition, consumers are sceptical about providing data to DSOs, which is reinforced due to the unclear business use cases of providing data to them.

Aggregating consumer data might be a solution to this generic problem. However, individual consumers have higher barriers to adopting existing standards, such as devices behind the meter (e.g., batteries and PVs). Furthermore, the slow roll-out of smart meters creates an additional obstacle to implementing coherent solutions across the EU. By now, we are already looking at the next generation of smart meters with longer lifespans and additional functions. Therefore, market entry issues might increase more for individuals than aggregators. This might not be the right direction considering public calls for democratising the energy sector.

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

Question 3: In your opinion, which systems are of the highest priority when implementing new cybersecurity measures?

Discussion and agreements

- SCADA / ADMS
- Master Data (systems for grid, customer, meters and more)
- Databases
- Self-service systems (customer facing)
- EMS (Energy management software)

Due to a lack of time, the brainstorming session was skipped for this section, and the discussion started right away. The DSO was identified as the leading actor, which could be due to the focus of the sub-group.

Energy management software (EMS), like Supervisory Control and Data Acquisition (SCADA) and Advanced Distribution Management System (ADMS), are at the core of tackling cybersecurity challenges. These systems, on the one side, link to databases and, on the other side, to self-service systems. Databases include master data, e.g., grid systems, customer, and meter data), which is highly sensitive. On the other hand, self-service systems on the consumer side touch on the same data but increase the surface for attacks.

3.2.2 Sub-group DSO 2

Question 1: What are the 3 most common concerns for DSOs regarding data exchange when integrating flexibility?

Discussion and agreements

- IT-security
- Consent Management
- Small FSP, opening structure to more stakeholders... maybe they are new vulnerabilities?
- Hacking many FSPs could be danger to grid?
- The more data is exchanged, the more threats are possible.
- GDPR
- Data privacy and security.
- Consent Management: business information could be attacked (cyber security), and not all data must be disclosed. Data comes from individuals.
- DSOs must protect data.

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

- Customer data/security of the system.
- Data interoperability.
- Harmonisation of data exchange between stakeholders.
- Reliability of flexibility activation.
- Data scalability.
- Coordination with TSOs.
- Data from different sources requires different data (planning).
- Where is flexibility coming from, how long, etc.? TSO coordination is essential.
- Grids are separated; exchange is needed to some extent.
- Data accuracy and reliability are important.
- Data must be ready for scalability.

The answer was split into three main fields: security, privacy, and data. All of them are closely interlinked while taking a slightly different perspective.

First, the existence and involvement of small FSPs open the structure of the energy sector up to new stakeholders. This could open doors for new vulnerabilities and eventually cause issues for electricity grids. The more data there is, the more threats are possible. The discussion showed that these serious issues require more attention from the involved actors.

Second, consent management is essential to ensure the privacy of consumers and businesses. While not all data must be disclosed to other actors, it certainly must be managed securely and adequately. DSOs are responsible for protecting grid and customer data and ensuring the system and supply security.

Finally, planning must account for different data use cases and data sources. Thereby, TSO-DSO coordination rather than interoperability of services is essential. Furthermore, customer and DSO grid data must not damage transmission systems. Therefore, planning data usage should account for the continuing separation of grids while ensuring the exchange of coordination plans. This requires business needs and solutions, as developed by OneNet. Such solutions must eventually be ready for scalability and replicability by maintaining high levels of data accuracy.

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

Question 2: Can data models and protocols be standardised at DSO level? If not, what could be barriers for this (e.g. CIM)?

Discussion and agreements

- Data models should be easy and fast to integrate.
- Protocols may be hard to adopt by small parties.
- It depends on the stakeholder.
- CIM is a great candidate, but the migration process requires a lot of resources and expertise that should be shared between operators as much as possible.
- Too many different DSOs, and thus data models, to reach an agreement.
- Barrier: Complexity of semantic models' reference tools missing, incompatibility issues between commercial tools.
- Hard to integrate. Many small ones with small IT departments.
- Participation should be incentivised, not made more complex.
- If it's already hard for TSOs...
- Data models must be easy to understand.
- CIM is a good candidate but requires many resources.
- Development should be shared between stakeholders.
- Process of importing data for tools.
- Consistency of exchanges is important.
- Expertise should be shared as well.
- Standards should look at the implementation of import/export.
- Many DSOs have different data models, and it is difficult to agree.
- Different stakeholders have different knowledge.
- Reference tools are missing, causing incompatibility issues between commercial tools.

Large data models like CIM are hard to integrate for smaller entities like DSOs, particularly since smaller companies often have smaller IT departments. On the other hand, data models should be easy to understand, and the utilisation should be incentivised by supporting DSO developers. Nevertheless, it appears as if CIM is growing increasingly complex. Therefore, it is a good candidate for modelling the communication between TSOs and DSOs but requires many resources to implement.

Hence, developing data models and protocols should be a joint venture between various stakeholders. Important aspects are the process of importing and exporting data into systems as well as the consistency of

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

exchanges. Aligning diverging perspectives on these aspects is a prerequisite for making tools work as efficiently as expected. To achieve this, expertise must be shared and standards developed together.

Therefore, the knowledge of different stakeholders must be brought together. This could be done by developing and providing reference tools for upcoming developments, avoiding compatibility issues. Data models and protocols solve different needs on different levels, but interfaces and extensions can be created to build bridges in between.

Question 3: Do you think that an information risk-management strategy is essential for every organisation?

Discussion and agreements

- With an increase in digitalisation, it is essential.
- For vulnerabilities from cyber-attacks and poor data security.
- Information risk management strategies are essential.
- High costs for smaller companies. For instance, German DSOs are generally very small.
- Guidelines as assistance? Facilitate cooperation with templates (by EDSO?).
- Develop common broad strategies. Start from a common view instead of individual ones (top-down approach).
- Harmonise processes.
- GDPR made companies stricter, hindering innovation.
- More barriers decrease flexibility for exploring new activities.
- But it's for the well-being of customers.
- Related to data exchanges!

There was no debate about the apparent "yes" to the question; however, the participants were eager to point out several aspects by underlining some of the issues related to data exchanges.

First, information risk management strategies are essential for every organisation. However, they pose higher costs for smaller companies due to limited resources, which we can observe with smaller DSOs in Germany. Guidelines could be developed by more prominent DSO associations, like E.DSO, to facilitate their cooperation. Such guidelines or templates should include GDPR issues, which made companies act more strictly towards the freedom of innovation. Developers must account for additional barriers to explore new activities, for instance, related to flexibility services. While it is clear that this happens for customers' well-being, a balance with innovation actions should be found. This aligns with developing common, broad information risk-management strategies, which should start with a top-down approach. Processes need to be harmonised with high-level goals in mind and work downwards to more specific use cases.

3.3 Customer group discussion

For this group discussion, three sets of questions were prepared for each sub-group. However, participants interested in the topics important from the distribution system operators' point of view participated only in the two sub-groups (1 and 3), so the questions from the sub-group Consumer 2 were not debated. Customers include aggregators, large customers and households.

Sub-group Customer 1: Data Exchange and Interfaces	Sub-group Customer 2: Customer integration	Sub-group Customer 3: Interoperability
Which are the three most important barriers in terms of data exchange among customer and market? How can they be addressed?	Which are the main challenges for the integration of the customer into the energy market from technical and legal perspective?	Which are the data models and ontologies most used in the interaction with the consumer or flexibility provider? Which gaps and barriers are there?
Which are the three most important barriers in terms of data exchange among customer and DSO? How can they be addressed?	Which are the main enablers for customer integration? Please include examples for best practices and the corresponding key factors.	Which actions can support the interoperability? Standardisation, legal actions, cyber-security, AI?
Which are the most important technical or legal gaps related to Cyber-security?	What role do data privacy and data security play in customer engagement? Are there socio-cultural aspects that have to be considered?	Where do you see the most growth in security threats?

Table 3.3 Customer sub-groups questions

3.3.1 Sub-group Customer 1

In the sub-group Customer 1, the participants debated only questions 1 and 2.

Question 1: Which are the three most important barriers in terms of data exchange among customer and market? How can they be addressed?

Discussion and agreements

- Interfaces are not unified.
- Proprietary data models and a lack of standardised communication protocols limit the interoperability of the solutions.
- Privacy regulations limit the development of specific business models. However, a balance must be reached.
- A regulatory framework for data access of third parties is essential to enable innovative business demos.
- There is a lack of knowledge of final customers about flexibility markets.
- In the Netherlands, the Authority for Consumers and Markets (ACM) ensures fair competition between businesses, and they want to protect consumer interests. The availability of smart meter data serves the

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

interest of prosumers. The conditions for data access need to be defined at technical and regulatory dimensions. Procedures for consent mechanisms for 3rd party data sharing should be established to enable innovative business models.

- There is a lack of standardised communication protocols for customer devices and interfaces with TSOs and DSOs. Missing communication standards and data models to enable communication becomes a barrier to providing flexibility services. Open standards favour the broad adoption of solutions.
- With digitalisation, the exclusion of specific customer groups needs to be monitored. Not everyone can join all solutions.
- Smart-meter deployment increases the observability of customer impacts and new business demos. However, some barriers exist to the smart grid deployment; approximately 2% of the Dutch smart meter population is not working due to technical problems such as a failing GPRS data connection.
- Intermediate actors connecting customers to the market will play a key role in enabling customer participation.

Barriers in terms of data communication between customers and the market can be grouped into three main categories: technical, regulatory, and communication and standardisation. In addition, numerous aspects must be clarified on the customer side, such as data ownership, legal rights and obligations, monetary compensation, and fees. This would further increase customer participation and related business models.

Question 2: Which are the three most important barriers in terms of data exchange among customer and DSO? How can they be addressed?

Things considered

- Data privacy

Discussion and agreements

- If smart meter data isn't available, the solution is in the hands of the DSO. Unfortunately, it is hard for a customer to know which one to reach.
- In the Netherlands, the 'Energy Suppliers Model' is used. This means that one receives one bill for the energy costs, in which both network management and delivery costs are processed, and you pay both to your business energy supplier.
- Single point of contact + better coordination & uniform solutions between supplier & DSO (access smart meter data via supplier vs DSO website).
- Solutions to data privacy are expected from the interoperability acts (1st one on data sharing and on general approaches dealing with privacy).

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

- The functionalities of the meters and overall smart meter environment provide alternatives for providing system services.
- The regulatory framework on clear cost distribution and answer to the question of who pays for devices that are clearly needed to reach climate and sustainability targets is required.
- Data from customers are mainly used for billing purposes only, while these data can be used to assess the flexibility potential. In some countries, there is resistance to smart meter roll-out, and smart meter roll-out lags (Germany).
- The setup of the data management model in some countries is not complete (e.g., data hubs in the Nordics have not yet been established in all countries). Therefore, no single solution exists, and alternative options can be adopted.

Arguments beyond the question/topic

- There is a concern about unclear cost distribution (who pays for the home energy management system) in the light of new (needed) services, i.e., demand-side flexibility.

The main barriers to data exchange between customers and DSOs are data privacy and regulatory issues. Regulatory work should offer guidelines on cost distribution, data ownership and billing.

3.3.2 Sub-group Customer 3

Question 1: Which are the data models and ontologies most used in the interaction with the consumer or flexibility provider? Which gaps and barriers are there?

Things considered

- Individual approach to each customer (big units) cannot be generalised to small units.
- Custom web-based models for each vendor/aggregator can potentially limit solutions' interoperability.
- Challenge: different technologies to interact with customers.
- Barrier: Interoperability with an in-house system of FSPs (or aggregators).
- Diverse, including tailor-made and/or vendor-specific solutions and/or not open source. And this is what makes it challenging for interoperability which is required to scale up specific solutions.

Discussion and agreements

- CIM data models are currently mainly used for large FSPs.

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

- OpenADR Alliance can be a reference for standardising, automating, and simplifying Demand Response (DR) and Distributed Energy Resources (DER) specifications.
- It was suggested the use of Smart Applications REFerence ontology (SAREF) for customer applications.
- Internally developed data models limit the interoperability of the solutions.
- There are barriers to FSP's capacity to interact with certain systems due to complexity and individual restrictions per location.
- TSO's strict data requirements become a barrier for small units.
- It seems like there is an opportunity for an operator of data as a service for customers so that other parties can offer services based on the data - flexibility markets, diagnostics, equipment performance, etc.

Arguments beyond the question/topic

- In the US, Green Button is used for sharing customer AMI data.
- EEBUS: open, two-way information model designed to facilitate information exchange primarily in-home but also with external stakeholders.

Question 2: Which actions can support the interoperability? Standardisation, legal actions, cyber-security, AI?

Things considered

- Cybersecurity is an increasing concern and highly needed.

Discussion and agreements

- A common data model for customer systems like CIM would be defined for each potential resource (storage, smart inverter, EV charger, heat pump, water heater, etc.)
- A reference framework/model to which each model used in real life could be mapped.
- European energy data space was presented as a good reference in dealing with data.
- EU network Codes could help to overcome some barriers.
- The data model would have to incorporate security and privacy elements.
- Clear, unified data structure for TSO/DSO connected flexibility units.
- Ensuring the implementation of the principle of easy access to data and data sharing by customers/data owners.

Arguments beyond the question/topic

- Blockchain approaches for the registration of resources for a variety of use cases.

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

Standardisation appears essential in customer integration, the full exploitation of flexibility, and interoperability. While at higher grid levels, such as TSO and partially DSO, CIM is a widely used solution, and communication is often not automated enough; proprietary and data models and solutions are applied at the customer level. Here, standardisation is necessary, e.g., the extension of CIM or the application of standard solutions such as SAREF or OpenADR. Furthermore, data models should be extended by cyber security aspects to reflect the current challenges in customer integration better.

Question 3: Where do you see the most growth in security threats?

Things considered

- Customer consumption data can make it easy to determine households away for holidays.
- The connection between aggregators and TSO/DSOs should be maximum secured.
- Customer data that could reveal personal information and status.

Discussion and agreements

- As it is more and more about private data (personal, commercial), strict rules and tools for respecting privacy need to be in place.
- A clear split between regulated in the commercial domain is also needed from the data management perspective.

Arguments beyond the question/topic

- Decentralised and communities' requirements? Looser requirements?
- Control of widespread customer devices (IoT).

Energy consumption data can provide conclusions on user behaviour and private information about the customer, such as presence, daily and weekly patterns, status, etc. Therefore, strong measures on data privacy, rights, and ownership issues must be developed and integrated into the system operation.

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

3.4 Evaluation and summary of the results

There are several common themes in the questions discussed in the TSO, DSO and Customer groups: interoperability, barriers to or gaps in data exchange, gaps in data exchange and cyber-security risks.

Regarding interoperability, the development of common standards for data exchange is vital, both between TSOs and DSOs and between DSOs and customers. This goes hand in hand with both the need to share data between authorised stakeholders and being able to address that need.

The groups considered the barriers to data exchange from many standpoints: DSO-TSO, DSO-Consumer, and Consumer-market. The technical, regulatory and standardisation barriers are common to all these pairs. Where customers are involved, there are additional privacy considerations, data ownership, monetary compensation, motivation, and trust. Additionally, the issues of GDPR being transposed differently in different countries, the need to harmonise data models and the need for data quality rather than sheer quantity was highlighted.

The complexity and breadth of cybersecurity in electricity grids are highlighted by the different but interlinked facets of the problem. They were brought up by the discussions in the different groups, ranging from the security of the grid components and systems to the need for data governance both as an enabler of cybersecurity and to give a stable business environment to the need to ensure the privacy of customer data.

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

4 Conclusions

To strengthen the consensus about OneNet's proposed solutions, GRIFOn will engage with as many external stakeholders as possible. The feedback from these stakeholders will find its way back into the proposed solutions. By allowing each stakeholder to provide their opinion, feedback, and expertise on OneNet's solutions, GRIFOn provides a forum for stakeholders to discuss OneNet solutions and reach an unprecedented European consensus about our project results.

The second GRIFOn workshop continued the approach already tried in the first workshop, again engaging with many external stakeholders. The technical solution used for the virtual meeting (Wonder.me conference system and Miro web application for the breakout sessions) worked well, enabling direct exchange with external stakeholders. The results of the discussions demonstrated a broad consensus among the stakeholders on how to address interoperability and data exchange. The WP4 representatives were satisfied with the event's organisation and participant feedback and used it in their future work. In addition, the event format proved successful in encouraging the discussion. Therefore, task forces for the organisation of future workshops now have a proven concept. Still, they will individually decide if the format suits them or if they would prefer something else.

In future GRIFOn workshops, the overall outcome and experience of the participants could be improved by additionally making recordings of the discussions. However, due to the advantage of hosting many participants without requiring them to be physically present, the remaining GRIFOn workshops are expected to be organised as virtual events.

For the GRIFOn activities in 2023, the representatives of the OneNet project defined three possible topics for future workshops:

- The third GRIFOn workshop is planned on **market design** in collaboration with WP3 at the end of Q2 2023. For the organisation of this workshop, the dedicated GRIFOn Task Force will be formed.
- The fourth GRIFOn workshop is planned on **OneNet connector** in collaboration with WP6 at the end of Q3 2023. For the organisation of this workshop, the dedicated GRIFOn Task Force will be formed.
- The fifth GRIFOn workshop is planned on **the main results of OneNet demonstrators** to derive recommendations for the EU-wide implementation of coordinated market schemes and interoperable platforms for standardised system products in collaboration with WP11 in Q3 2023. For the organisation of this workshop, the dedicated GRIFOn Task Force will be formed.

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