ESO

Data & Technology Advisory Group

Meeting 5 Minutes

Date:	15/11/2023	**Location:**	Virtual
Start:	13:00	**End:**	15:00

Participants

Attendee	Organisation
Sebastiaan Van Dort (Chair)	BSI – British Standards Institute
Jamie Crawford	Wales & West Utilities
Tom Pollock	Northern Gas Networks
Dr Priya M Bhagavathy	Power Networks Demonstration Centre
Erwin Frank-Schultz	IBM
Prof Gareth Taylor	Brunel Institute of Power Systems
Abbas Mahmood	Energy Networks Association
Ankit Patel	Arup
Maria Kordoni	ESO
Jonathan Barcroft	ESO
James Edwards-Tombs	ESO
Divya Mahalingam (Facilitator)	ESO

Agenda

1.	**Apologies for absence**
2.	**Discussion: Programme strategy update**
3.	**Discussion: Technical alignment with national digital twin programme & digital spine**
4.	**Discussion: Managing security**
5.	**Next meeting**
6.	**AOB**

Discussion and details

1. Apologies for absence

- No absences

2. Discussion: Programme strategy update

Revised mission statement:

- Creating the common data sharing infrastructure to enable an ecosystem of connected digital twins that will facilitate the transition to net zero.

Reflection Points

- ***Do you have any feedback on the updated mission statement?***
- ***Is the overall purpose and objective of the milestone plan clear, does the format convey it clearly?***
- ***Are there any other enablers and decisions that should be included?***

Discussion

- The group liked the revised mission statement, it was mentioned that affordability, reliability and fair for all are significant elements which were in one of the previous mission statements, but unable to be included in the final version.
- ESO confirmed that affordability was considered but has different meaning to different groups of people.
- It was agreed to clarify and include clear scope/role of Minimum Viable Product (MVP) and Future System Operator (FSO) in the milestone plan.
- It was suggested to include dependencies for the enablers and to highlight them in different colour to separate their requirements for the VirtualES programme development.
- It was discussed that MVP gives the ability to gather users' feedback in the early stages to help focus continued development on users' needs for the VirtualES programme.
- The group asked whether data sharing infrastructure will be applicable for real time data. ESO confirmed the plan is to extend that beyond MVP through use cases. The initial strategic plan for the MVP will be looking at longer term data and slower frequencies.
- It was proposed to consider delivering the MVP earlier then given timeline, allowing enough time to test and rethink on some important technical aspects - different code models, architecture approach or ontology for the next round.
- The group questioned, do we want to call it MVP or Pilot. A pilot study gets a core digital product or service out in the ecosystem in a controlled way.
- It was suggested to keep the MVP to a minimum and focus only on the functional requirements of the product. This way, you can plan and budget it better.
- It was advised that before creating an MVP, consider what you want to achieve with your product and its target uses.
- It was discussed to collaborate with some related governance framework, such as National Underground Asset Register (NUAR) project, which are built out data governance artefacts with high quality content.
- ESO reassured the group that continuous engagement between ESO and NUAR team is happening and will be used to help baseline MVP testing framework for data governance.
- ESO requested group members to link to any interesting and relevant projects to look at and consider for the programme development.
- It was confirmed that members of the group are involved on different data sharing projects over next year (2024). They are willing to share the information with the group when available.
- It was advised that the proposed MVP does not include some activities needed for sustainable data governance, such as setting up a Data Committee; creating policies and supporting documentation; or putting in place a controls and assessment environment. It was suggested we do need them, but not just yet.

- It was concluded that don’t just settle on one MVP, as there are chances that if it fails, you may have to go back to the drawing board. Keep multiple options for fallback if the current MVP doesn’t plan out well; and
- Keep all the stakeholders - this includes network companies, end-consumers, suppliers, generators, system operators, government, regulators, representatives of relevant organisations and other bodies, as well as investors, on the same page. It helps them understand how their contribution fits the large picture, and they collaborate better with the VirtualES programme.

3. **Discussion: Technical alignment with national digital twin programme & digital spine**

Definitions of the following concepts.

- Data sharing infrastructure: the digital services, standards and tools that support the exchange of data between participants across the sector.
- Common Digital Assets: include the common energy digital tools, services, and infrastructure that are created, deployed, and used across the energy sector.

Reflection Point

- ***Are these definitions clear and is anything missing?***

Discussion

- It was suggested that graphical view of how these concepts all relate to each other would be very useful for the industry at large and what are the dependencies, such as, potential, hard dependencies for data sharing and digital assets.
- It was shared that Ofgem published data analytical graphs alongside their distributed flexibility market engagement, that picture could be expanded on or updated for data sharing and digital assets.

Prepare-Trust-Share Model

Reflection Points

- ***Does the Prepare-Trust-Share model resonate with you?***
- ***Are there any other aspects of interoperability or alignment that we are missing?***

Discussion

- The Prepare-Trust-Share model resonated well.
- It was recommended that the initial data discovery and identification piece could be useful. For instance, identify requires to be considered before preparing, where you work backwards from the use cases and what you're trying to achieve to identify the data sets, before you start to Prepare-Trust-Share them.
- It was agreed among the group that extra steps or expansion of the model will be beneficial.
- ESO acknowledged group feedback and confirmed to furthering the Prepare-Trust-Share model.
- It was explained that the data producers will need to prepare their data for sharing by transforming it to an agreed standard, and understanding their data licensing conditions, metadata, and security permissions.
- It was described that a trust framework will ensure that only verified and validated participants can exchange data. This also includes understanding a host of security, compliance, regulatory, governance, data licensing agreements and legal implications for sharing that data, as the correct controls will need to implement as part of the ’Publish‘ step.
- It was mentioned to bring some approaches to interoperability testing and conformance to give people an opportunity to understand what data is expected with correct controls and standards.
- It was considered that standardising the data to an agreed format will enable interoperability of data throughout the energy sector and beyond. It will also enable key software / analysis packages to standardise on import / export functionality.

Data preparation and sharing

Reflection Points

- ***Is there any functionality in this data preparation step that you feel is critical to energy and needs to be considered?***
- ***Are there any constraints to the deployment of this functionality within different organisations?***

Discussion

- Defining the appropriate characteristics of the data is essential and will make the data understandable, useful and self-describing. This, alongside the security & governance controls will ensure that the data is treated as a product as it contains all the required components and characteristics for sharing.
- ESO explained that the data sharing in the VirtualES will function through approved protocols such as Application Programming Interface (API) endpoints. The data exchange will need to accommodate sharing of both static and dynamic data, between multiple producers and consumers - depending on the use-case.
- The adoption of approved and secure API will ensure that data is shared securely, and effectively through a data exchange method that is most suited for the dataset and the use-case.
- It was agreed that trusted and secure APIs will ensure that the producers are registered with the trust framework and are trusted participants. This will enable the application of security and governance controls to the data as it is exchanged using the VirtualES.
- It was explained that people being able to reuse data easily enhances innovation, but data not made available because it's not in agreed format might hinder innovation.
- Group discussed that if data sharing infrastructure is controlled by standards and format, many network operators who have their own data format will stop publishing data in open because the cost of converting to required format could be high.
- ESO reassured, the goal is to design a data sharing infrastructure that can support the effective and secure operations of the VirtualES.
- Based on the research conducted by the VirtualES, and the work conducted by the data sharing architecture industry collaboration group, a distributed data sharing architecture has been considered as the most appropriate for the VirtualES infrastructure.
- The goal of distributed data sharing is to enable the seamless access to data for multiple users, regardless of its physical location. The data is decentralised i.e., it is not stored in a centralised repository with a central owner but rather the locality and ownership of the data lies with the organisations providing that data.

Technical alignment

Reflection Point

- ***Are there any other topics that should be considered in this alignment exercise?***

Discussion

- ESO explained that the digital spine feasibility study also concluded that these functional components could be delivered by existing in-sector and cross-sector programmes, namely the National Digital Twin Programme (NDTP) as “Prepare”, Open Energy as “Trust”, and Virtual Energy System as “Share”.
- The objective of the technical alignment in the VirtualES is to understand the technical design and development maturity of the data sharing infrastructure component parts with respect to interoperability, and to identify the integration dependencies between the NDTP, Virtual Energy System and Open Energy.

- It was mentioned to consider a range of potential data that can be shared, specifically in the digital twin space. In an industry like this, data could be complex and different technical solutions might require for sharing.
- It was advised to add the National Digital Twin Programme (NDTP) updates in the next briefing.
- ESO confirmed that NDTP and ESO are collaborating to build an understanding of what technical arrangements required to know:
  - Is the product already out there available to be deployed?
  - Does it need developing?
  - How many suppliers can install such a thing?

Action

- ESO to share more information on NDTP and ESO findings on technical alignment.

4. Discussion: Managing security

- Across the energy sector there is wide-spread recognition that digitalisation of the sector brings in new risks and opportunities for the security and resilience of the overall system. Being security-minded and embedding digital security principles is recognised as essential to enabling safe digitalisation at scale.

Reflection Points

- ***What are some key principles that should underpin the decisions made to define security parameters?***
- ***Are there existing frameworks that can support definition of security best practices and protocols?***
- ***What are potential risks to consider at this stage in the programme, associated to managing security?***

Discussion

- It was discussed that it is important to:
  - Collaboratively identify the security best practices and protocols to be adhered to, aligned to National Protective Security Authority (NPSA).
  - Carry out an assessment of the potential security risks created and identify core security requirements.
  - Test possible resolution and mitigation assumptions. ESO confirmed engagement with NCSC on this matter.
- It was agreed that being security-minded and embedding digital security principles is recognised as essential to enabling safe digitalisation at scale.
- It was discussed that an organisation should always make a cautious decision in align with audit when it comes to sharing data.
- It is important to regularly review and assess all data-sharing-related policies, procedures, and technologies within the organisation. The cybersecurity landscape, laws, and regulations change, and so do cyberthreats. Thus, assessing the effectiveness of implemented security controls should be a regular practice.
- Projects like Cyber Assessment Framework from the National Cyber Security Centre can support definition of security best practices and protocols.
- It is important to avoid breaching any element of General Data Protection Regulation (GDPR), which can result in severe fines. Create and deploy a thorough data sharing protocol.
- It was advised in the next step is to implement suitable security measures – depending on the level of sensitivity, each data group might require different security controls. The right tool or a set of tools should offer a variety of technical controls, including:
  - Robust end-to-end encryption
  - Access controls
  - Various authentication methods (passwords)

5. **Next meeting**

- The next meeting will be held on Wednesday 24th January from 13:00 to 15:00.

6. **AOB**

- The Chair thanked the group for their attendance and contribution.