About the IET

The IET is a trusted adviser of independent, impartial, evidence-based engineering and technology expertise. We are a registered charity and one of the world's leading professional societies for the engineering and technology community with over 155,000 members worldwide in 148 countries. Our strength is in working collaboratively with government, industry and academia to engineer solutions for our greatest societal challenges. We believe that professional guidance, especially in highly technological areas, is critical to good policy making. For further details on the evidence submitted, please contact policy@theiet.org.

Executive Summary

The IET welcomes the opportunity to provide input on the AI Technical Sandbox, and we support the overall proposal. The production of an AI Technical Sandbox overseen by Ofgem is an ideal opportunity to demonstrate best practice of AI development.

AI is influencing how businesses, industries and technologies operate now and in the future. However, AI in all its encompassing forms, is not infallible and must be applied diligently, and appropriately. Digital technologies can help bolster resilience across a range of sectors by providing a greater insight into scenario modelling and provide insightful data analytics to help inform decision making. As with any other technology, it can also pose its own risks, and it is important to be aware of vulnerabilities that digital technologies may introduce to a system of systems. AI solutions must be aligned, encompassed, and influenced by software engineering, software architecture, management, governance, technology operations, and service delivery / service management. By showing how AI can be used successfully, it will encourage other sectors to adopt AI. A sandbox will help achieve this level of robustness before deploying to a real-life scenario.

A 2023 report by the EU found that regulatory sandboxes are useful, and enable the creation of new products and services, supporting innovation (Source: European Commission: Regulatory sandboxes in the energy sector – Final report). The report found that sandboxes can support technological experimentation in areas such as dynamic pricing models, demand forecasting and consumer energy management systems.

It is important, however, to consider the differences between a regulatory and a technical sandbox:

- A regulatory sandbox can create controlled environments where systems can be developed and tested with regulatory guidance before market release as it allows for processing of personal data and facilitates market access for SMEs and startups.
- A technical sandbox is a secure, isolated environment used for testing software, code, or applications without affecting the main system or network. It acts like a digital playground where potentially harmful or untested code can be run without risk of causing damage to the actual system.

Whilst the rules that Ofgem can afford to relax in the regulatory sandbox are relatively straightforward, utilising a technical sandbox for testing AI in a safe environment requires appropriate digital twin models to exist. It is important for the sandbox to have access to representative data of the energy system to ensure accuracy of modelling. In future, it should aim to be compatible with existing digital twins within the national energy system. Having

appropriate digital twin models enables effective testing of AI behaviours, for example, discovering if the AI model drives undesirable outcomes as well as desirable ones.

Digital twins are widely used across different sectors to test decisions before we make them and understand how different actions might have real life implications. However, they are often not used to their full potential, particularly as they are excellent models for systems that have complex requirements such as the energy sector. The availability and quality of data is important as poor data quality or insufficient data can lead to inaccurate simulations and therefore misguided insights and suboptimal decisions. If the sandbox is to integrate with a digital twin in future it will need to be able to work with real representative data. It will also need to be cross-checked over time, for example, verifying that it is still a faithful representation of the real-world energy system.

A major concern surrounding the implementation of AI is the lack of information and trust in it. IET research has found that 29% of engineering employers surveyed had concerns on the lack of information around AI (Source: The IET, Artificial Intelligence behind 3 times more daily tasks than we think). When developing AI, it is imperative that there are strong data foundations, competency and full transparency, as this will enhance the national public trust and uptake of AI.

Recommendations

- **Energy system data modelling** – The sandbox needs to be designed to run projects more efficiently using up-to-date information throughout the process, leading to improved productivity both now and in the future. It should draw on real time data from the energy system, possibly through existing digital twins. It's a data resource that can improve the design of a new asset or understanding of existing asset condition. This has the potential to vastly reduce errors, reduce system maintenance down time and discontinuities present in more traditional methods of information management.
- **Raising awareness of carbon efficient AI models** – As AI models have very large compute and storage demands, there will be a need for new data centres. There needs to be a comprehensive understanding of the energy consumption of data centres when using AI and to recognise carbon efficient AI models as a way to mitigate impact. The IET recommends a bronze, silver, gold standard for the approval of new data centres in the UK, based on a sustainability rating. This would emphasise the moral responsibility surrounding data centre energy consumption.
- **Regulation** – AI safety and the assessment of risk must go beyond the physical, to look at financial, societal, reputational and risks to mental health, amongst other harms.
- **Data Governance** – There should be firm rules on which data can and cannot be used to train AI systems. The AI Technical Sandbox is a good way to establish high quality and use of data.

Resilience

Digitalisation is central to innovation and key to the energy transition. There have been many successes in Ofgem sandboxes around digitalisation, including the 2022 Secure Data Exchange Sandbox and the Energy Market Challenge (Source: GOV.UK, Projects lay the groundwork for a future of robolawyers and flying cars). This shows that there will only be an increase in digitisation, increasing the risk to national infrastructure.

Strengthening the resilience and security of critical national infrastructure such as the electricity generation, transmission and distribution system is a key priority. As the UK progresses towards its Net Zero targets there will be changes to the energy supply mix and demand. Attempting to achieve this transition without the appropriate strategy in place could

prove costly for the UK. A brittle infrastructure can induce a negative chain reaction throughout the wider system. To create resilience, there needs to be a technical understanding of the issues, processes, and interdependencies there are when assessing risks with a whole system engineering perspective informing decisions.

The risk of energy infrastructure failing due to AI misinformation or cyber security attacks can be quite significant. With an increase in the number of devices connected by digital networks (Source: DCMS committee, Connected tech: smart or sinister?) including in energy infrastructure, it exposes the grid to new risks. Misinformation can be a tool of cyber attackers aiming to disrupt grid operations. AI-driven malicious misinformation campaigns could mislead operators or automated systems, causing disruptions and outages. An AI system manipulated by false data could also open vulnerabilities that hackers could exploit, such as misleading data analysis and faulty decision making.

In order to minimise this risk, it is imperative to develop a better, broader definition of safety and risks of AI tools, this will also help AI developers ensure their product is safe and fit for purpose before going to market. This should include guidelines and criteria for developers to assess their products against.

High quality and real time data

The IET recommends designing the sandbox so that it can access representative data. This will position the sandbox to interact with digital twins in future and make the testing more robust. The use of digital twins, as a combination of technologies, can help support greater resilience across sectors. It's a data resource that can improve the design of a new asset or understanding of existing asset condition. This has the potential to vastly reduce errors and discontinuities present in more traditional methods of information management.

The need for an AI sandbox in the energy sector

AI can transform the energy efficiency of other carbon-intensive industries, such as modelling buildings to predict energy use (Source: European Cluster Collaboration Platform, Artificial Intelligence improves the energy efficiency of buildings). Sandbox testing could allow innovators to trial AI models that optimise energy consumption without risking real-world disruptions. It could also help assess the energy impact of AI systems, including how they interact with grid infrastructure and renewable energy sources. This is especially relevant for testing load balancing algorithms, predictive maintenance, and smart grid technologies. The rise of AI data centres and AI chip production is placing significant strain on global energy grids (Source: Global energy grids strained by surge in AI data centres and chip production.)

However, the difference in energy consumption between different AI models is significant, for example between a Large Language Model (LLM) and a simple AI app. There needs to be more communication on the difference between data centres and AI, which are often conflated. It is also pertinent to communicate that cost is not only quantified in terms of financial return as the cost to the environment and the impact that climate change has on health must also be considered. There needs to be a comprehensive understanding of the most carbon efficient AI models, and the offsetting powers of technology. **The IET proposes a 'bronze, silver, gold' standard for data centres: bronze for excessive energy consumption which is harmful to the environment**, silver for less harmful, and gold for environmentally sustainable operations (Source: The IET, The cloud is not in the sky: why the energy consumption cost of AI models is not equal and what this means for sustainability). This would emphasise the moral responsibility surrounding data centre energy consumption.

Barriers and enablers to AI innovation

There are a number of enablers for innovation in AI, including the use of sandboxes as controlled environment for testing AI solutions that can help innovators navigate legal and ethical challenges while engaging with regulators and other innovators.

It is critical that the appropriate legal and regulatory structures are in place to allow AI's safe development and use but also do not stifle innovation. It needs greater transparency around the training and operation of AI systems. Although the onus is on developers to prove that the product is fit for purpose and has no unintended consequences, further guidelines and standards around how this should be reported would support a regulatory environment that is pro-innovation and provides safeguards against harm. As AI models have very large compute and storage demands, there will be a need for new data centres. **The IET recommends that AI safety and the assessment of risk must go beyond the physical, to look at financial, societal, reputational and risks to mental health, amongst other harms.** There is concern over the lack of broader understanding and information surrounding AI, the data used to train the models and ethical considerations. AI has created a discussion around the ownership of data needed to train these algorithms, as well as the impact of bias and fundamental data quality in the information they produce. As AI spans every sector, it is imperative that regulation is coordinated, so there is consistency and clarity.

It is necessary to ensure AI is used safely and to help prevent incidents from occurring, and it is fundamental to maintaining public trust, which underpins the economic and social benefits AI can bring. A sandbox provides an opportunity to achieve this, however, there needs to be clear governance frameworks set and this sandbox is a great opportunity to spearhead this.

However, there is a clear gap in the ecosystem that needs to be addressed with regards to supporting best practice for development and adoption, ensuring that knowledge is not lost along the pipeline. A clear example of this is in products such as AI, where product development knowledge is not passed onto product users and maintainers in a robust way. The Responsible Handover of AI report (Source: Sense about Science) highlights this example specifically as a break in the pipeline for information / knowledge handover.

Data governance

The AI Technical Sandbox is a good way to establish high quality and use of data.

There is concern over the lack of understanding and information surrounding AI, the data used to train the models and ethical considerations. This has given rise to a discussion around the ownership of data needed to train these algorithms, as well as the impact of bias and fundamental data quality in the information they produce. It is imperative that regulators co-operate globally, so there is consistency, clarity and sharing of best practice.

There needs to be greater clarity on the legal use of data in the research and development of AI systems. Many developers do not understand their legal obligations in terms of permission to use data, or taking decisions based on that data. This lack of clarity hinders research and innovation. While there is much openly accessible data that could be used to 'train' and test algorithms in their early stages, it is unclear the extent to which such data is legally allowed to be used, especially when the data is not accompanied by explicit terms and conditions. Greater legal clarity on these issues would give researchers and companies more confidence to develop AI systems, supporting the UK's pro-innovation approach.

The IET recommends that there should be firm rules on which data can and cannot be used to train AI systems.