Grant Agreement N°: 956671

Topic: ICT-56-2020

The European IoT Hub

Growing a sustainable and comprehensive ecosystem for Next Generation Internet of Things

D2.3: Expert consultations and dialogue report

Revision: v.0.9

Work package	WP 2
Task	Task 2.3
Due date	31/10/2021
Submission date	29/10/2021
Deliverable lead	BluSpecs
Authors	Brendan Rowan, Dr. Robert Pomohaci (BluSpecs)
Contributors	Dr. Monique Calisti, Dr. Lamprini Kolovou, Katherine Anderson (Martel), Emilie Mathilde Jakobsen (AU), Dr. Rute Sofia (FOR), Tanya Suárez (BluSpecs).
Version	1.0
Dissemination level	PUBLIC

EXECUTIVE SUMMARY

EU-IoT puts in place the mechanisms to enhance the IoT community of researchers and innovators in Europe into an increasingly cohesive, dynamic, participatory and sustainable ecosystem, as an essential part of the Next Generation Internet of Things (NGIoT) Initiative. The aim is to assist stakeholders to engage and create value, as well as set up a self-sustaining European IoT community.

This document brings together the insights and inputs collected from top IoT specialists in Europe as part of the Experts Group, as well as consultations within the NGIoT initiative and the wider IoT community.

The insights are summarised within the EU-IoT framework, which is organised in the vertical dimension along 5 areas between of the human-edge-cloud continuum: Human/IoT Interface, Far Edge, Near Edge, Infrastructure and Data Spaces. In the horizontal dimension, the framework is organised around Technology, Market, Policy & Standards and Skills. Within each of the former three domains (Skills are to be addressed in the final version of this deliverable), this deliverable collects information along three areas: future directions, potential barriers and obstacles, as well as opportunities for Europe.

In terms of NGIoT technologies, the key future directions are:

- Digital sensing through novel interfaces is driving new modes of interacting with technology within the IoT paradigm.
- The shift of intelligence to the Far Edge is the next frontier, and will lead to lower power consumption locally, greater responsiveness with more efficient and higher economic potential applications.
- 5G will transform IoT, not just through faster speeds but also enabling new functions such as orchestration or network slicing to enable applications such as private edges, collaborative IoT and federation of intelligence.
- These applications will enable new modes for data interaction, specifically under the model of data spaces.

The key barriers and obstacles affecting this vision of the NGIoT are vendor lock-in for both hardware and software, power requirements of devices, and policy considerations particularly in the area of interoperability.

Europe is in a good position to overcome these challenges, building on the clear ownership models and their leadership in decentralised and Far Edge technologies.

Four key domain areas for the NGIoT have been identified: Agriculture, Manufacturing, Mobility and Energy, with specific applications investigated in each. There is also the opportunity of applying NGIoT technology in new domains, but barriers such as semantic compatibility of data or the inertia of the current or the dominance of non-European, cloud hyperscalers in the landscape need to be surpassed. Europe has shown industrial leadership across the key domains, particularly in manufacturing, but what is missing is the development of specific products, as well as applying and deploying edge AI technologies and platforms within real word verticals at scale.

Within policy and standardisation, hybrid, decentralised, and privacy preserving IoT architectures are likely to transform the NGIoT, realising the vision of a trustworthy, secure and private European IoT landscape. The key SDOs that are involved in this work include IETF, ISO, ETSI, 3GPP and ITU-T among others. GAIA-X represents a new frontier and will be key to ensuring strategic European autonomy. Obstacles such as closed standards, a lack of skills and a risk-averse culture need to be overcome. There is an opportunity for Europe to take advantage of the current strong attitude and rules around data protection to create an appropriate, European-value-drive data storage and analytics model for IoT and Edge.

The EU-IoT Expert Group currently has 20 members, with broad expertise across the NGIoT landscape. Half of them are affiliated to academia, and a third to industry, with a small share to non-profit organisations. Currently all members are located in Europe, with more experience from outside the continent to be brought through a future expansion of the Group. The Expert Group have already met in two sessions, in March and September 2021, with two further sessions in March and September 2022 planned.

TABLE OF CONTENTS

LIST OF FIGURES

ABBREVIATIONS

AB	Advisory Board
AI	Artificial Intelligence
AR	Artificial Reality
BMI	Building Information Modelling
CB	Coordination Board
CSA	Coordination and Support Action
CTF	Communication Task Force
C&A	Consortiums and Alliances
DEI	Digitising European Industry
DEP	Digital Europe Programme
DID	Decentralised IDentifier
DLT	Distributed Ledger Technology
EG	Expert Group
HEP	Horizon Europe Programme
IA	Innovation Actions
IoT	Internet of Things
JU	Joint Undertaking
M2M	Machine to Machine
ML	Machine Learning
MR	Mixed Reality
NGI	Next Generation Internet
NGIOT	Next Generation Internet of Things
NGO	Non-Governmental Organization
PLC	Programmable Logic Controller
RIA	Research and Innovation Action
R&I	Research and Innovation
SNS	Smart Networks and Services
SoS	System of Systems
SRIA	Strategic Research and Innovation Agenda
VR	Virtual Reality

1 THE NEXT GENERATION IOT LANDSCAPE AND EU-IOT

The EU-IoT project is working to strengthen and coordinate research and innovation Internet of Things (IoT) efforts, supporting the creation of a sustainable and competitive ecosystem embracing European technology and system providers. The purpose is to increase trust and acceptance in **human-centric, secure and privacy-preserving IoT by design** made in Europe. The specific objectives for the project are the following:

1. To support the development of synergies and foster strategic coordination among NGIoT projects and related initiatives in order to drive impact and reinforce the strength of European IoT to achieve Horizon 2020 goals while smoothly and effectively transitioning to Horizon Europe.
2. To ensure the growth of the NGIoT ecosystem by engaging target stakeholders and facilitating participation for newcomers, while fostering collaborations among them and establishing strong liaisons at intra and inter-programme level.
3. To foster the development of business models, innovation activities and skills-building lowering the barrier for adoption and development of IoT-empowered solutions.
4. To support and coordinate outreach and impact-creation activities across the NGIoT ecosystem, by orchestrating communication and dissemination efforts, open calls promotion, events organisation and participation, and contributions to open-source, pre-normative and standardisation initiatives.

One of the key areas of work of EU-IoT is **strategic positioning and road mapping activities** to ensure alignment on a shared vision and common goals to shape the digital future of Europe, particularly in IoT policy. This is achieved through a combined set of activities to ensure alignment at pan-European level with relevant efforts. For this purpose, EU-IoT is engaging with several other prominent representatives in the NGIoT community, via lead and orchestration of:

- **The NGIoT Coordination Board (CB)**, which gathers coordinators of the NGIoT research projects (ICT-56 RIA: ASSSIST-IoT, VEDLIoT, IntellIoT, IoT NGIN, iNGENIOUS and TERMINET) and of the three CSAs (EU-IoT, NGIoT and OPEN DEI), as well as EC representatives.
- **The EU-IoT Advisory Board (AB)**, grouping prominent experts from relevant domains and initiatives such as FIWARE, OASC, AIOTI among others. The advisors offer EU-IoT strategic guidance and policy recommendations.
- **The EU-IoT Expert Group (EG)**, bringing together top IoT experts in Europe and beyond to collect insights on the top trends and future directions in IoT for Europe.

In this deliverable, the focus is on collecting inputs from the EG, as well as consultations with the ICT-56 RIA projects and dialogues with the key European IoT communities and experts on the top trends in technologies, applications and standards that are driving the Next Generation IoT.

The document is divided into the following parts. Section 1 provides an introduction to the document. Section 2 details the EU-IoT framework for collecting these inputs and centralising them. The outputs are then collected in Section 3 within each of the three key areas of Technology, Applications and Standards. Section 4 presents the structure and processes of the Expert Group and the workshops where information was collected, while Section 5 presents the conclusions to this document. Supporting Annexes 1 and 2 present the rough outcomes from the EG sessions as the collaborative Miro boards, as well as the members of the Expert Group.

2 THE EU-IOT FRAMEWORK

The European IoT landscape embraces several initiatives focusing on an increasing number of novel technologies across several verticals that allow for the proliferation of new IoT solutions and services models.

To properly understand and analyse the needs of such a diverse and ever-growing community, EU-IoT has defined a **mapping process and a framework** to capture the core requirements and needs, despite the diversity, while considering the specificity of different NGIoT use cases.

The proposed EU-IoT framework has been validated through consultations with Experts, the Advisory Board and the NGIoT projects. The framework operates along two axes:

The first axis addresses the points of interaction between the physical elements which make up the human-to-cloud continuum, reflecting the current and future structure of the IoT. This axis looks at the **human-device-gateway-networks-cloud** points of engagement and searches for areas and themes of progress between and across them.

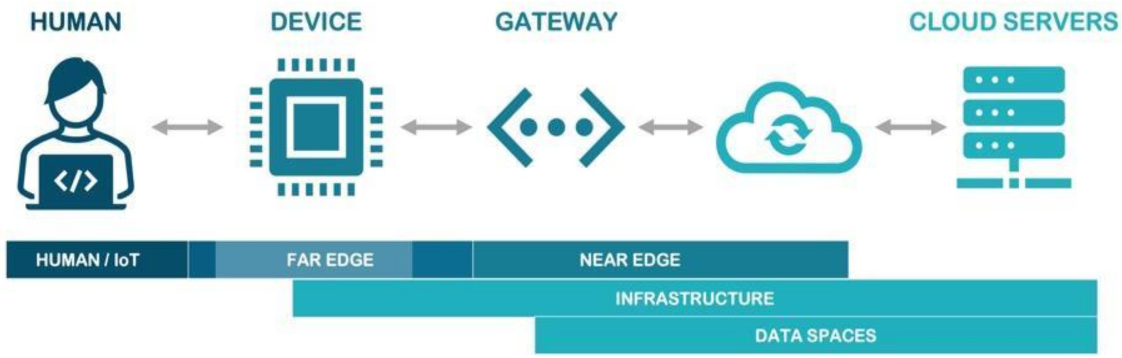

Figure 1: The IoT continuum - from human to cloud and back again with key interfaces

The second horizontal axis refers to key research and innovation areas / technological contexts which can overlap and have a reach across the continuum that EU-IoT will focus. There are five areas of interest: the **Human/IoT interface**, the **Far Edge** (devices level), the **Near Edge** (gateway level), the **Infrastructure** (including networks) and the **Data Spaces,** as displayed in Figure 1 above. Within these five key areas/contexts, which bracket advances, discussions, and debates, EU-IoT addresses four broad main themes grouping important transversal aspects, as shown in Figure 2.

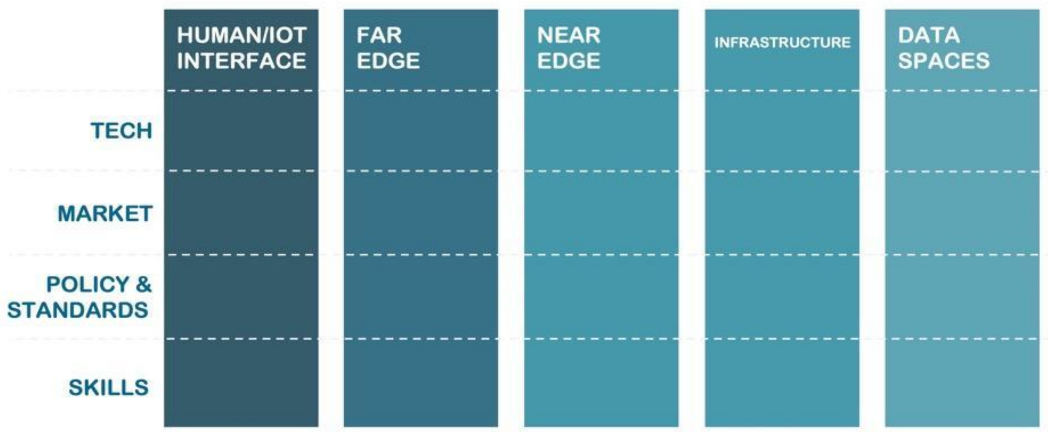

Figure 2: Draft guiding framework of the EU-IoT approach

3 KEY DRIVING TRENDS FOR THE NGIOT

In the following section, we present the key outcomes of the consultations within the Expert Group, as well as with the NGIoT projects, grouped within areas of the EU-IoT framework. Together, these key insights provide a glimpse into the cutting edge of IoT from the players involved and working on bringing these technologies to market. The results are structured according to the three horizontal domains of the EU-IoT framework: Technologies, Application and Standards. For each of these domains we structure the insights along the key directions for the future, barriers and obstacles to achieving this vision, and Europe's position within the global NGIoT landscape. The process of collecting insights on the Skills needs of the NGIoT is ongoing through further consultations with experts, as well as the EU-IoT training activities. These will be summarised in the updated version of this deliverable.

3.1 Technology

3.1.1 Future directions

Digital sensing through novel interfaces

At the human-machine interface, several new technologies will transform the interaction between operators and IoT devices. **Novel dashboards** will improve human sensing, allowing for simultaneous control of multiple devices. These will not necessarily be completely new interfaces; significant value is expected from the reuse of existing interfaces in a novel manner. The **environment will become the interface**, with technology moving beyond legacy devices such as the mouse.

Haptic sensors will allow devices to evolve within context and better fit within their environment. **Autonomous receptive interfaces**, sensing the whole human body and not just hand touch points, as well as **automatic speech recognition and interaction** will allow for a novel and full sensory experience in human-machine communication. This digital sensing will bring new interactions enabled by **virtual reality** (VR), **augmented reality** (AR) or **mixed reality** (MR), with the assistance of artificial intelligence (AI), to improve the current man-machine complementarity.

There is an opportunity for IoT interfaces to evolve in conjunction with the requirements of personal privacy, through the concept of disposable (proofs of) identities or decentralised identifiers (**DIDs**). These are temporary verifiable credentials, anonymous and dynamic, which are discarded after an ID check. A specific application of this is the development by Microsoft in the ION project, removing the need for usernames or passwords for log-ins, instead accessing private areas through a DID-enabled private key.

Intelligence on the Far Edge – the new frontier

Adding intelligence on the Edge will move perception closer to where the data is generated and sensed by IoT devices. This **distribution** of IoT functions to where they are needed will help to better manage data, driving real-time decision making with **efficient ML** where it is most necessary. This reduction in data transfer will enable low connectivity apps and **optimise power consumption**. Intelligence at the Edge will also drive better security and privacy for IoT devices.

However, the synchronisation of data is contingent on efficient communication between devices. **Semantic validation** will be required to make data analysis efficient and reduce uncertainty.

The standard system-on-a-chip approach used previously will need to evolve to reduce the resource use in preparing programmes, **through the use of simulators**. **Microcontroller** units under a function as a service model can also be used to improve processing, through recent advances such as the NVIDIA Jetson[1]. Together **AI hardware accelerators on constrained edge devices is expected to be a major milestone in the integration of intelligence at the edge**. This hardware set-up can support high computational tasks needed for model training at the edge and transfer learning. This will be combined with **advanced optimisation techniques**, to auto-tune the high dimensional space of configuration parameters for Edge Computing to an appropriate value according to the ML framework and its objectives.

In order to scale up the existing pilots for Edge Intelligence, **no or low-code models** are an attractive solution, making the ML selection and data normalisation process more automatic and visual.

ML algorithms can be improved by incremental learning techniques such as **transfer learning**, where new data is used to continuously extend the model knowledge and functions. This way, one can take a reference model and incrementally augment it.

The fuzzy edge – near or far?

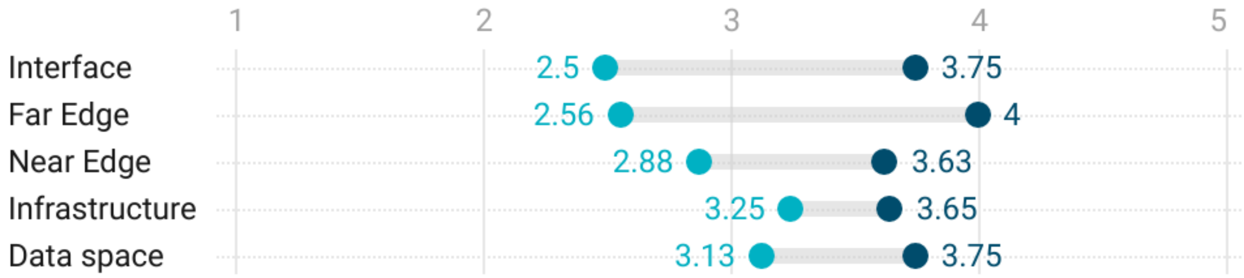

Figure 3: Relative maturity (green) and economic potential (blue) of NGIoT enabling technologies across the human-cloud continuum.

In the EU-IoT framework, and within literature, often a difference is being made between Near and Far Edge[2]. This separation splits the application of IoT technologies onto a **device within the field** (Far Edge) or onto a **central cluster** (Near Edge).

There is a question of the division point of the '**fuzzy edge**' – where is the line to be drawn between the near and far edge? In practice, a series of these technologies such as deep learning, explainable AI or Digital Twins can be applied across both the Far and Near Edge. Where the difference appears is in the **maturity** of applying these technologies, and their **future economic potential**.

According to the rating of the experts (see Figure 3), technologies on the Near Edge are more mature, but also of less future economic potential compared to applying it on the Far Edge, confirming the potential of the **Far Edge Intelligence as the next frontier in the NGIoT**.

To 5G and beyond

The use of 5G brings along not just faster connection speed but will also allow novel sensing technologies such as **instant haptic feedback** or **AR visualisation** of devices to come into

---

[1] https://www.nvidia.com/en-us/autonomous-machines/embedded-systems/

[2] A Vision on Smart, Decentralised Edge Computing Research Directions, EU-IoT Consortium, 2021

fruition. By applying techniques such as **orchestration** or **network slicing**, applications such as private edges, as well as the **federation** of resources will be made possible, transforming the NGIoT with new modes of processing data. **Cloud-to-far-edge service network meshes** can enable the distribution of intelligence and decision making from the cloud to the edge.

The two areas expected to see most evolution are both the very **high end** (mm-wave/THz) and the very **low end** (backscatter networking for battery-free communication) **communications** in terms of energy use. However, their integration into 5G/6G networks will not be straightforward. Infrastructures will evolve to allow for **joint communication and sensing**, increasing robustness through automation, and reducing latency across the whole protocol stack. However, there is a robustness/latency trade-off to be considered. Solving this will enable novel NGIoT applications beyond mobile communications such as ubiquitous instant communications.

Ultra-low power wireless networks enabled through backscatter are expected to reduce the energy costs of communications. **Energy harvesting** from the ambient environment in wireless sensor networks is expected to further reduce the energy use. **Quantum networks** using qubits between quantum processors is another area of future development. New networks powered by peer-to-peer connections, as well as **decentralised storage and delivery networks** (such as IPFS or Filecoin) are expected to result in novel communication manners.

Visible light modulation can also improve connectivity, through the technique of visual light communication (VLC), rather than the standard of radio waves for high-speed internet connectivity.

New modes for data

The NGIoT also brings along novel data processing models that will enable the effective implementation of the concept of data spaces. These include **decentralised cloud**, or **function as a service**, or scalable and energy-efficient **consensus algorithms for DLT** and **smart contract platforms**. In general, this will enable a shift from vertical infrastructures to a more distributed, peer-to-peer model.

The use of decentralised storage and delivery networks will allow for privacy-preserving data storage and delivery. The development of **context-aware Machine Learning Operations** (MLOps), and the integration of these methods and practices within a function-as-a-service model will also be a key enabler of data spaces.

Once data spaces are implemented, managing them through technologies such as **distributed ledgers** for provenance, contracts or transactions within a data space will be key to their success. **Making the data self-aware is a key approach to ensuring its security**. Successful applications of these technologies will result in creating a personal data market that is efficient and privacy-preserving.

A privacy-friendly solution to data aggregation and analysis is **homomorphic encryption of data**[3], a method of securing data where computing can be done automatically without the access to the secret key.

[3] Mark A. Will, Ryan K.L. Ko, Chapter 5 - A guide to homomorphic encryption, The Cloud Security Ecosystem, Syngress, 2015, Pages 101-127, https://doi.org/10.1016/B978-0-12-801595-7.00005-7.

3.1.2 Potential barriers and obstacles

Hardware

The **closed nature** of existing IoT solutions, controlled by specific vendors, leaving developers locked into select manufacturers often hinders progress in the NGIoT. The perceived solution to this is wide adoption of open-source solutions which provide interoperability and cross-domain support.

NGIoT solutions also have significant computational and therefore **power requirements**. A reduction in the energy use of computing platforms and infrastructure is necessary, along with a transition to robust latency solutions. Other key ingredients include enabling the required networking power through the deployment of infrastructure such as 5G/6G.

Software

The **Edge AI models are not advanced enough** to bring the full potential of IoT to the Far Edge, specific advances in edge AI models are needed. This could be supported through the development of a marketplace to distribute AI models.

Software architectures are normally not secure-by-default, leading to security risks. There is also a lack of unification in the architectures, leading to issues of interoperability.

Often the software is **vendor specific,** rather than open-source, making interoperability and collaboration across verticals and applications difficult.

Policy

Trust from the end-users is a significant barrier to wider adoption. Users need to feel in control of IoT device functions. Novel technologies will require a good level of **usability**, as well as the **applicability** across different areas. Attractive user interfaces are often lacking from NGIoT technologies. Applications that are searchable by their content, through Information Centric Networking (ICN), rather than location, as the web is currently built to provide a good approach, but they require larger-scale support.

Many **legacy technologies** are available for edge intelligence, requiring varying levels of skills and investments.

Different types of data require different **standards**, and it is not always clear where the **responsibility** lies for data maintenance in the long run. When deploying automated methods, specific provisions for data integration and interoperability will be essential to success in this area. With this comes the need for a careful balance between data protection needs and the practicability of data sharing and integration.

The conditions for success of intelligence at the edge are multi-disciplinary, specifically more **targeted collaboration** between IoT devices, ML developers, hardware, systems, networking solutions as well as social networks are required. What is missing is a **unified approach** bringing together the achieved progress, supported by a specific regulatory framework addressing both technical and economic aspects. Collaboration as presented by the GAIA-X model will be essential to ensure that the NGIoT fits the needs of all relevant actors.

3.1.3 Opportunities for Europe

Europe is in a good position in terms of regulation of IoT interfaces and devices, and personal data protection, having defined a **clear ownership model**. Most of the applications and the technology used with these devices comes from outside Europe, with regulation being more permissive in Asia. Europe also has little or no agency in regulating IoT device interfaces as there are **no European services or apps developed** for these. Early attempts to fix this are in progress [4],[5], with ephemeral identifiers providing a good example. The key competitors are Asia and USA.

AI applied to machines, rather than to analyse personal data is a particular strength for Europeans as **'thing makers'**. Bringing the data source closer to the user, to the **Far Edge**, will bring social behaviour change in the IoT landscape overall, and Europe is in a good place to deploy and experiment with intelligence at the Edge. The combination of AI with "physical things" (machines), particularly those deployed as Edge devices could be a sweet spot for EU as "thing makers".

Europe is in a good position on **decentralised technologies**, although more projects actively building on those technologies and improving privacy-enabling technology are needed.

3.2 Applications

3.2.1 Future directions

The four key domain areas and use cases for NGIoT

There are four sectors identified as high priority for the NGIoT, with the following existing and nascent applications:

- **Agriculture**
  - **Collaborative farming**, supporting agricultural operations with drones assisting vehicles and also Edge processing on the vehicle.
  - **Autonomous weeding**, integrating autonomous vehicles to weed larger crops such as orchards within large fields, with guidance from drones. The processing is done on the vehicle, and a model of models is deployed, learning from human decisions when overriding the controls.
  - **Crop management**, precision farming enabled by deploying Edge nodes in the field, with fertilisation or harvesting equipment run autonomously, and the data centralised for the farmer for decision-making.
  - **Animal welfare conditions management**, using NGIoT sensors to help farmers monitor the condition of animal pens automatically and adapt them as needed to improve welfare
  - **Intelligent precision agriculture**, enabled by federated machine learning and autonomous farming, assisted by IoT sensors and actuators, with the data centralised in a client platform, leading to remote and therefore more efficient and

[4] About Coelition, (2020) coelition.org

[5] Secure Open Federation for Internet Everywhere project, (2020), https://www.sofie-iot.eu/

cheaper resource management, as well as optimal crop cultivation.

 - Measuring the dimensions and conditions of the field (to support management and regulations), with **image-based remote monitoring** using a networked computer board to capture the image data. This can be analysed by AI/ML remotely to communicate to the farmers who control the crop, offering them real-time information. A wide range deployment of LoRaWAN can be used to scale up monitoring capability in small edge nodes.

- **Manufacturing**
  - **Autonomous robots** carrying out maintenance operations in factories, supporting critical infrastructure and handling equipment in industrial settings.
  - **Intelligent production**, improving operations through the leverage of data from production processes of acoustic panels, by the implementation of wireless PLC sensors in a plug and play format. This will enable the collection and merging of data across machines, production environment and manual configurations. The machine operations are based on data rather than operator subjective decisions, resulting in better insights on the case and effects of issues in production performance, identifying opportunities to optimise production and increase performance through data-driven decision making and quality management.
  - **Valve monitor and automation**, an end-to-end IoT solution to make assets smart, automate processes and deliver actionable insights into industrial operations. The IoT valve monitor is a plug-and-play low power device combining a variety of sensors facilitating the automated monitoring and control of valves, reducing the need for manual operations such as valve checking and emergency monitoring.
- **Mobility**
  - **Intermodal asset tracking** deployed within ports, monitoring the location and condition of containers in transit. Decisions can be then made automatically on what can be done to ensure safe transit.
  - **Port management**, supporting automated flow by transforming the cranes into devices, with an AR interface for managers to gain an overview of the system.
  - **Automated driving**, a system enabling sustainable and safe mobility within an urban connected environment, based on a standardised and easily deployable architecture (driver assistance and shared control systems), enabled by perception sensors, cameras and real time trajectory generation of data. This improves driver experience in regards of safety, inclusion, time, efficiency or environmental sustainability, with obstacle and danger detection features.
  - **Reactive bicycle lights**, using IoT sensor technology to monitor the environment and cyclist behaviour at a high rate (800 times per second) to protect cyclists and improve smart city infrastructure. This brings in automated visibility in dangerous encounters with brighter and faster flashing lights at roundabouts, through haptic feedback, meaning the cyclists do not need to check their phone for directions. The IoT device would also be passively collecting information about the city infrastructure for planners and engineers to support their decision making.
  - **Intelligent e-charging stations**, modules integrated with a dedicated application, collecting remotely readable flows of real-time information. This fosters intelligent sustainable infrastructure by balancing energy output with input from renewable energy sources, resulting in better customer service in terms of payments, geolocalisation and consumption overview, as well as allowing station owners to remotely monitor, control and actuate the stations.

    - Improvement of the mobility model through **analysing citizen commuting patterns**. This will support the preservation and sustaining of key urban infrastructure.

- **Energy**
    - **Water infrastructure** on the Edge, integrating a plug-and-play IoT solution with the accompanying software element to enable monitoring and management of water networks, and a micro-hydro system converting the water flow into a stable power supply. The solution offers increased control over water networks, reducing leaks and improving cost and performance through predictive maintenance. Collaboration between sensors will allow the precise detection of a leak, and autonomous deployment of resources to fix this.
    - **Smart water metering**, using IoT sensors supported by a software platform for remote and automated water usage and waste readings, increasing efficiency and reducing costs. Also offers customers automated billing and real-time water consumption overview.
    - **Smart grid metering**, the implementation of IoT energy measuring devices to measure the amount of electricity consumed by users, offering near-real time data and algorithms or forecasting and awareness of the status of the grid. The solution brings in decision support systems with abnormality detection based on ML algorithms and AI functionalities.
    - **Building management systems**, control systems for all the consumer devices in the house and defining a power demand/supply plan, bringing together the power storage, solar power sources and electric car(s) within a home (e.g. where to charge electric power to the car at home/work/somewhere in between, community pool, backup traditional power supply etc.). Every device can become an edge node, and they can be organised in layers of edge node. The management system would then spur applications ranging from power monitoring, where to supply, community sharing etc. Given the complexity of this task, AI/ML will be key to help to control the system as well as individual edge nodes. This is where 5G networks of higher capability can come in, as most buildings already have management systems deployed, but integrating intelligence onto them will result in an overload to servers.
    - **Grid balancing** using electric cars, with charging stations connected to the grid, supporting intelligent energy allocation as needed to balance the grid by storing the energy into cars that are charging.

In addition, the experts and the project identified the following domains of interest:

- **Smart Homes**
- **Digital Health and Pharmaceuticals**
- **Personal Data Management**
- **Public Safety Control**
- **Resource Management**, including condition management of shared infrastructure, such as temperature.
- **Environmental Sciences**, particularly in disaster mitigation and sustainable land use.

In addition, a case applicable to all verticals was discussed: **management of shared infrastructure** such as cars or tractors with the support of the Edge, with local computation done on the device, to monitor the condition of the infrastructure such as temperature.

A full list of IoT success stories as analysed by the consortium is available in the recently published EU-IoT deliverable 4.1 'Report on best practices for use cases'.

Opportunities for the application of NGIoT technology in new domains

With intelligence applied on Edge nodes, value comes from eventually **sharing the data** with the wider ecosystem in the federation of independent Edge nodes. This model removes the reliance on contracts over the parameters of the data sharing, as is currently practiced in contracts with hyperscalers. Many IoT startups have been attracted by the nature of contracts with cloud providers such as AWS, where the scaling up is made very easy, but at a certain point in demand the costs become unsustainable and can lead to the collapse of the growing company.

Edge nodes can also take advantage of **physical locality**, with devices close together being able to communicate directly and not via cloud, reducing latency and energy use.

The Edge does not necessarily bring openness, certain providers might prefer maintaining the systems closed model in order to increase their profits. The only way out is through the development of a platform that is compatible with multiple systems which is open by a disruptor. The move towards the edge will, however, **facilitate greater data agency with those companies who generate it**, enabling coopetition and permissioned use of federated data models within smaller companies; reducing the risk that their own data may be used against them in the market.

Cooperative sensing through next-generation infrastructures and applying intelligence to sensors leading to context awareness and therefore direct responses to environmental changes will bring along the possibility to explore new business models and applications within the NGIoT. **Distributed sensing**, particularly developed in a research context, presents a new frontier here. This will need to be combined with data-driven business models, combining the ownership of data with the right business knowledge for success. For example, Amazon is taking advantage of Landsat data with the support of Sinergise, a Slovenian SME, for the organisation of the data into an easily analysable model.

3.2.2 Potential barriers and obstacles

New applications can only arise through a thorough and out-of-the-box **analysis of the infrastructure** of the future through the application of intelligence of Edge nodes, assessing how this is different to what is currently on offer, and how novel parts of the system will need to be managed and addressed. IoT business models are not ready for the integration of intelligence at the edge, which is hindering commercialisation activities. Additionally, more use case partners for the IoT community are needed.

Results from projects and research need more investment in the technical developments, as well as **support with exploitation** to ensure results are market-ready. EU projects often have "toy use cases" where data is collected and the partners work on agreeing on standards and models, rather than its exploitation. Collaboration between research and industry and SDOs is required to overcome this challenge and lead to results for tangible outcomes.

The **inertia** of transitioning from cloud systems is a major obstacle to the proliferation of intelligence at the edge. Currently, **hyperscaler cloud currently offers an easier to use interface, simpler management of process and more perceived efficiency**. However, in the long run, after full implementation, Edge Computing can overcome these obstacles through wide adoption. It requires an **equally attractive interface and engagement with developers as users**.

The market for IoT applications is **not currently open**, leading to barriers to entry for startups and SMEs.

A lack of specific **hard, soft, and business skills** on the part of the users of IoT devices is another significant obstacle.

Data sets need to be **semantically compatible** in order to allow for processing in private clouds. Analytics should support the organisation, curation and integration of data sets.

3.2.3 Opportunities for Europe

Europe has shown **industrial leadership** in areas such as manufacturing, Industry 4.0/5.0. We also still have an edge in areas such as automotive, manufacturing, privacy and sustainability, but unless more work is done the future of European competitiveness is at risk. Significant relevant research and standardisation is being carried out in Europe, but we are missing the development of specific products, which China is leading on.

We are however behind other global players in **applying and deploying edge AI technologies** and platforms in real world verticals.

3.3 Standardisation

3.3.1 Future directions

Trust, security and privacy for NGIoT technologies

The **omnipresence of IoT devices** is expected to render them almost unnoticeable to the average subject[6]. This raises significant concerns over human awareness, around the agency that subjects have in exercising their rights when interacting with IoT devices[7]. There are unsolved issues around the **accountability and liability for actions of machines**, for both material and immaterial results. Novel interfaces combined with the right standards enable the generation as well as consolidation of **trust**, ensuring the **privacy** of IoT devices, bringing **confidentiality** to the data.

Decentralised Identifiers (DIDs) [8], combined with **5G/6G 'cold spots'**, can help bring the concept of privacy in smart cities to the next level. These are areas of disconnect within a smart city where no data is collected, affording users a secluded period and therefore improving their wellbeing.

Architectures supporting the NGIoT

Novel IoT systems will be based on a **hybrid edge/cloud architecture**, supported by the integration of open-source technologies. The specific delimitation, definition and architecture of the Edge varies depending on the area of application of the concept. The evolution of the NGIoT

[6] The Computer for the 21st century, Weisser, M., 1991 Scientific American

[7] Security, privacy and health, Pankati et al, 2003, IEEE Pervasive Computing

[8] van Kranenburg R. et al. (2020) Future Urban Smartness: Connectivity Zones with Disposable Identities. In: Augusto J.C. (eds) Handbook of Smart Cities. Springer, Cham. https://doi.org/10.1007/978-3-030-15145-4_56-1

will lead to AI models distributed from cloud to edge, as well as federation of learning. A degree of **open-source standardisation** at the edge is to come as a result of adding intelligence to the edge, with quality control and visual control of devices set to become the norm.

The infrastructure for the NGIoT is expected to evolve with the deployment of **privacy-preserving architectures**, decentralised storage, cloud environments and edge computing. Particularly, decentralisation will be essential for success both at the edge and cloud level.

Network architectures that enable **data democratisation** are expected to emerge, integrating several aspects of existing networks such as information-centric networking, security, naming and in-network caching, to further reduce latency across all layers.

Large amounts of data are generated in a **decentralised** fashion, without any central control, which makes the enforcement of standards difficult. New modes for data ownership, storage, handling and access are expected to be developed in the near future. To manage this large scale of connected objects, a significant degree of automation is required.

A birds-eye view of the standardisation landscape of the NGIoT

The EU-IoT consortium has carried out an extensive mapping work, defined in the deliverable 3.7 ‘Recommendations on research priorities and innovation strategies to standardization’. This has identified more than **80 relevant bodies**, including Standards Defining Organisations (SDOs), Pre-normative bodies and Consortiums & Alliances (C&A).

Presented with the map of bodies according to the EU-IoT framework (see Annex 1), the Experts suggested that **a fine-grained view on C&As particularly is necessary**. Specifically, most of the work on Edge and IoT is currently supported by entities that fall in the category of C&A. This is, for instance the case of the Eclipse foundation, which supports the development of Edge computing[9], or of the Linux Foundation with LFEdge[10]. In the same category, entities such as LoRa define standards. Therefore, the experts recommended to provide a finer-grained perspective of C&A based on their type of contribution:

- C&A that generate standards, such as ZigBee, LoRa.
- C&A that apply standards, e.g., via the creation of implementation references, such as Eclipse.
- C&A that provide recommendations for standardisation, such as AIOTI.

Specific standards making groups rather than global entities are to be accessed (e.g., Eclipse Edge instead of Eclipse). More entities that address **specific domains** should also be addressed, such as Automotive alliances.

Larger bodies such as ISO and ITU-T play a significant role in **personal data protection standards**. They transfer fundamental rights of data protection into technical measures, providing suggestions to integrate these into the design of IoT applications by default. Data protection authorities, particularly in Europe, have been rejecting international standards that are not fully consistent with privacy guidelines, and the trend will likely continue with the adoption of AI regulation as well as with the ongoing decentralisation of services led by Edge computing.

The experts selected the bodies they believed are most relevant for the future of the NGIoT, see Table 1 below for full details.

[9] https://www.eclipse.org/community/eclipse_newsletter/2019/october/discover.php
[10] https://www.lfedge.org/

Table 1 Standards bodies' ranking for the future of the NGIoT

Rank	Standards body	Role in the NGIoT and comments
1	• IETF • ISO	• Key SDO for interoperability in Internet and related services, highly relevant across different NGIoT scope areas • Key SDO in supporting data protection and privacy, working towards fundamental aspects to IoT/Edge computing. ISO does not today provide the required level of support for the near/far Edge context.
2	• ETSI	• Active across several NGIoT areas, more relevant on the legal side of implementing regulations, rather than developing specific IoT standards. They drive the Mobile Edge Cloud (MEC) model as developed by Nokia, and carry out proof of concept work to drive research into standards. ETSI also drives a SAREF effort supporting ontologies which are relevant to IoT.
3	• 3GPPP • GAIA-X • ITU-T	• Acting across multiple domains, many relevant to the NGIoT • A new frontier, unexplored territory of international cooperation on the development of regulation and standards by and for Europe. A wide area of possibility remains to be seen if the necessary consensus for success can be achieved. They have done significant work on establishing European sovereignty principles, but they have yet to deliver specific standards supporting interoperability aspects. It remains to be seen whether they will develop their own standards, or provide a European take on international standards.
4	• IEEE • IRTF	• Acting across multiple domains, many relevant to the NGIoT
5	• AIOTI • Linux Foundation • Zigbee Alliance	• Relevant for particular applications within the NGIoT
6	• BDVA • W3C/WOT • GSMA • LORA • ORAN • FIWARE, ONEM2M • RISC V • EEC IIC • OPC • CENELEC	• Relevant for specific domains such as OPC in Manufacturing, or active across two domains one or two domains, e.g., agriculture, manufacturing, for LoRA and now expanding to other verticals such as energy. Some are active across other verticals outside of the 4 key NGIoT directions, such as GS1, Zigbee or AIOTI.

A suggested approach has been the organisation of **common events** between the NGIoT initiative and SDOs specifically focused on addressing barriers due to regulatory frameworks of the different domains.

3.3.2 Potential barriers and obstacles

Open and decentralised solutions and standards

Many of the existing standards are **closed**, which limits the applicability of NGIoT across different domains. Open standards are the key to opening up the NGIoT to wide applications.

Open IoT solutions that whole communities can use, ensuring **sovereignty** and not just in terms of data spaces are needed to allow for innovation. A range of innovative platforms that developers can build applications on top of and experiment with are suggested, including: IPFS, Filecoin and Ethereum.

Security, privacy and trust

A certain level of **encryption** will be necessary for the application of intelligence at the Edge in order to preserve privacy.

One approach to ensuring security and privacy is to **hide IoT devices** from the wider Internet, deploying them in private networks. Ipv6 link-local addresses are an interesting application in developing private edges, by using scrambled MAC addresses.

End-users often lack the **skills** required to operate these novel interfaces, as well as to understand the potential impact NGIoT technology could have in their day to day lives, both positive and negative. Standards should specify that IoT devices should be made **accountable by design and by default**, allowing people to defend themselves against unwanted side effects. To ensure this, a shared methodology for the identification of human needs should be made part of the design process of novel interfaces, including a threat analysis. A key element of this is personal data protection, which will need to be at the core of the design process, by default, using data-driven methods to ensure the rule of human law over machines by default. The methodology adopted by the European Digital Payments Industry Alliance (EDPIA) provides a good example.

New architectures and new approaches

As the monopolies of big tech conglomerates are hindering evolution and progress, there is a need for **decentralisation**, in order to support management and ensure end to end security. It will be essential to reduce the complexity of operations and maintenance of the network architecture in order for the NGIoT initiative to succeed. Future applications should be then developed on top of this decentralised architecture with the help of easy-to-use platforms, fostering interoperability. **Semantic interoperability** will be required in order to aggregate the data sets to take advantage of the new modes. The data should **converge at the network layer**. The process should be **automated** where possible, allowing for manual data copying and gateway operations

A **culture change** is required, taking more risks and allowing for failure in order to learn, as well as more focused on engineering the new IoT applications rather than marketing them. NGIoT standards need to also support the whole ecosystem and the deployment of novel and improved business models. A better connection between entrepreneurship and research should be developed, where projects are valued and supported to develop commercially successful products. Digital Catapults in the UK provide a good example of this.

3.3.3 Opportunities for Europe

The current **attitude and rules around data protection** in Europe are strong, which may be seen as a disadvantage initially but could be turned into an advantage. Products developed should take these restrictions into account and manage them by design.

Europe has a unique opportunity to design the NGIoT environment around and according to human needs and rights, using the principles outlined in the EU Charter of Fundamental Rights as a checklist to ensure all bases are covered. The **GDPR** and **AI regulation** are well designed for this and likely to make the difference with the rest of the world in terms of ensuring privacy and trust. In designing future regulation for IoT interfaces, food, drug and medical device cases provide a good example.

An update to GDPR allowing for **appropriate data storage and analytics in IoT and edge devices** will be required, whilst preserving privacy, ensuring data protection during sharing. Concomitantly, citizens need to be made more aware of the need of sharing and using data, as well as of existing privacy rules.

A key approach will be an increase in European involvement in **open source efforts** and standardisation, taking advantage of community networks across countries such as The Things Network (TTN).

Europe has good experience in sharing data and infrastructures for computing across borders and organisations. For example, Google has archived EU Copernicus open space data in their cloud, which researchers can use to do their analytics.

4 THE EU-IOT EXPERT GROUP STRUCTURE AND ACTIVITIES

The EU-IoT Experts Groups were established in 2021 as a community of specialists tasked with providing guidance to EU-IoT project in concrete areas in order to guide its principal actions The Expert Group brings together leading members of the European and International IoT community to provide inputs on specific aspects of relevance to the Next-Generation IoT community. This group focuses on set topics of interest as defined by the EU-IoT consortium together with the NGIoT Coordination Board, EU-IoT Advisory Board and the European Commission. They lend their experience, expertise and opinion to provide strategic guidance in their areas of expertise to ensure that the work undertaken by the project has a full understanding of the ongoing challenges, trends and initiatives.

Expert Group Members are regularly requested to provide impartial views and inputs to EU-IoT work through discussions and documents, both during Expert Group Workshops, as well as informal discussions through the mailing list. Participants commit to providing such input in a timely manner to enable proper consideration and integration of these inputs. For a full list of the 20 Expert Group Members, see Annex 2.

4.1 Membership criteria

Members of the Group are high-level experts who demonstrate clear experience and knowledge of the IoT landscape in Europe with strong international networks. They are leaders in industry, and have extensive expertise in the specific IoT areas of interest.

Membership of the Group is on an individual basis and Members do not represent any organisation or group while in position. The Experts Group strives to achieve balance, both in terms of gender and geographical representation.

All members commit to a mandate of three years for the duration of the EU-IoT project and adhere to the stringent Code of Conduct.

The following criteria are applicable to members of the Expert Group:

- A minimum set of required language skills.
- Strong expertise and thought leadership to demonstrate direct relevance to at least one of the key areas of IoT as approached by the EU-IoT project.
- A visible and active role within relevant European and International networks.
- Possibility of providing access to new knowledge and expertise in the area of interest.
- Availability for active participation in the Expert Group meetings.

Examples of profiles of Expert Group members include:

- Representatives of leaders within digital and non-digital companies with a presence in Europe (e.g. directors and leaders in corporates and multinationals, directors and representatives from traditional and non-traditional SMEs, and scale-ups working cross-border with advanced technologies).
- IoT advocates and leaders (e.g. directors and leaders with a responsibility for IoT adoption at social partners, such as trade unions, associations, and NGOs).
- Representatives of the IoT technology providers or adopters in Europe (e.g. corporations or start-ups developing IoT solutions or working to integrate or promote them).

4.2 Expert Group engagement structure

The Expert Group meets in sessions once every six months, for a concentrated two-hour session, with future full-day sessions planned in person when possible. The sessions providing the forum to debate, discuss and define key topics and challenges identified within the next-generation IoT technologies. The result of the sessions is captured in brief outcome papers by the EU-IoT consortium, which form the foundation of the strategic road mapping of the European Next-Generation IoT research and innovation agenda.

The sessions are facilitated by the EU-IoT consortium, with a focus on the structured gathering of inputs, identification of priority and emerging themes and creation of recommendations.

Expert Group members commit to:

- Participate actively in the biannual online Expert Group sessions and constituent workshops.
- Provide inputs and opinions on a set of predefined topics.
- Review discussion outputs to help guide the EU-IoT strategy and activities.
- Share information about relevant advances or items of interest in their respective areas of activity.

4.3 Expert Group workshop

Due to ongoing travel restrictions, the first two sessions were organised remotely, via Zoom, and reduced to a time of two hours to ensure focused insight collection.

The goal of the first of the EU-IoT Expert Group Session was to introduce the Expert Group, the NGIoT initiative and perform a validation of the key assumptions behind the constituent themes and topics along the edge-to-cloud continuum. The session ultimately addressed the key concepts driving the Next-Generation IoT ecosystem.

Experts approached together the concept of the future of the IoT, through discussion in parallel sessions, guided by the EU-IoT team who provided the structure for inputs. Experts expressed their opinion and brainstormed on a series of key questions with the assistance of a Miro board, in the four topic areas of the EU-IoT framework:

- PS1: Human-IoT interfaces
- PS2: Advancing intelligence on the edge
- PS3: Infrastructure for the next generation IoT
- PS4: New modes of data

The second session also took place remotely, via Zoom. The aim was to build up on the insights gained in the first Workshop, as well as across the EU-IoT activities, in order to enrich the existing knowledge base on key NGIoT technologies, applications and standards needs.

The Experts were invited to share opinions and experiences in one of the following transversal areas of the EU-IoT framework, through a series of guided exercises:

- Tech: understanding and prioritising the key enabling technologies for the next generation IoT.
- Applications: defining and mapping the key use cases for AIoT and Edge Computing.
- Standards: mapping existing standards and SDOs by relevance within key application sectors.

The nine Experts that attended the session were divided into small teams, providing contributions to one of the three groups. After the session, they were also able make contributions directly to the boards of other groups, or directly to the EU-IoT team.

4.4 The Expert Group for 2022

Analysing the current Expert Group composition, there is strong expertise in the area of enabling NGIoT technologies, IoT applications and data processing architectures. There is also good coverage in terms of standards. More expertise on IoT Skills and Training, Business models and technology implementation is required.

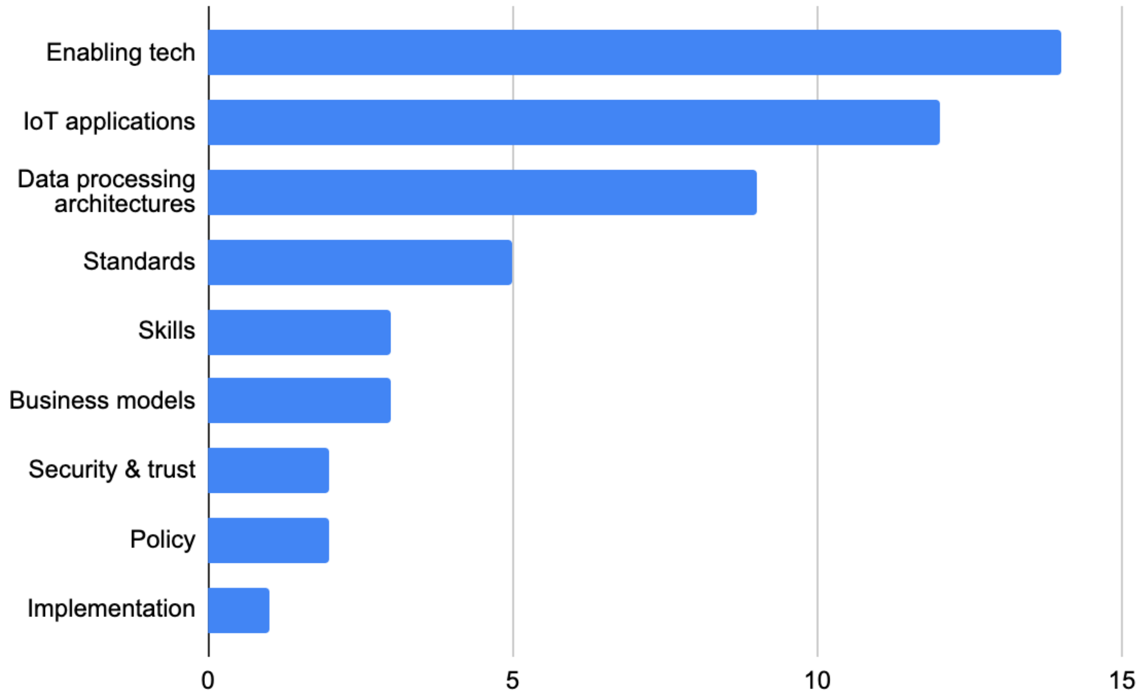

Figure 4: Expert group areas of knowledge

In terms of the sectors where the Experts hail from, half are from a research background. There is scope for expanding industry, as well as non-profit and association representation.

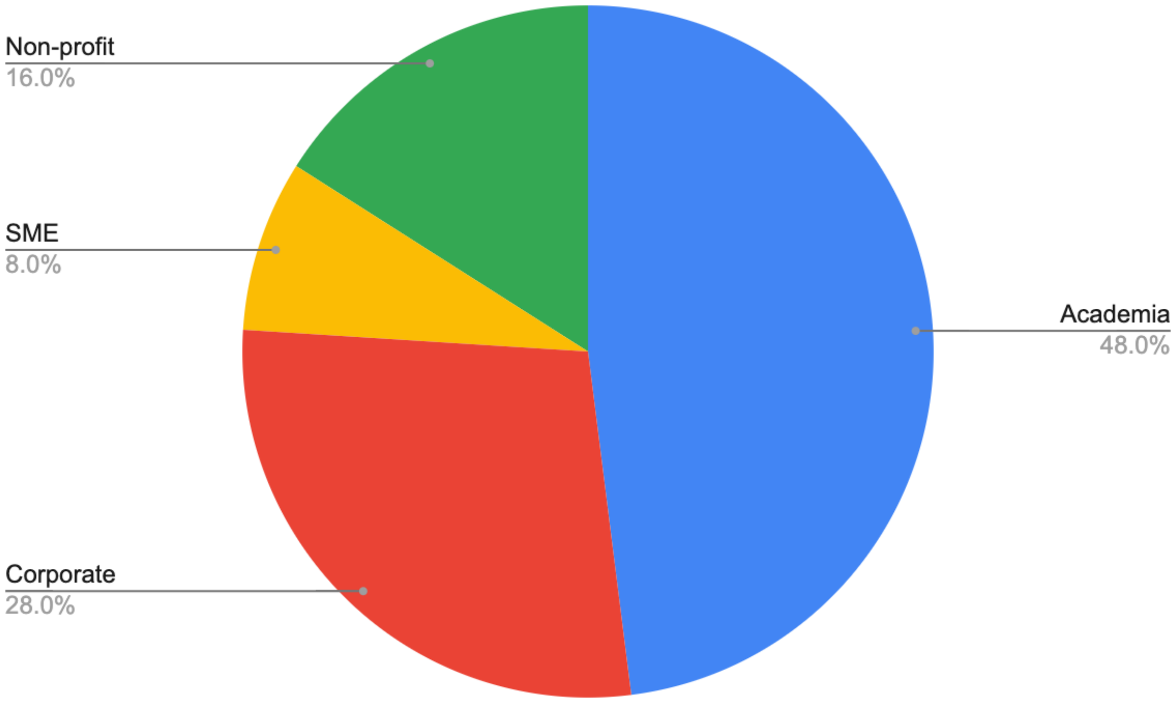

Figure 5: Expert Group affiliations

Related to their geographical location, all Experts are originally from Europe. More representation from outside Europe is needed, particularly from the USA and Asia.

5 CONCLUSIONS

The EU-IoT consultations with experts provide a key overview of the current and emerging landscape of NGIoT in Europe and beyond. We structure the conclusions reached around four key areas.

5.1 Where will the NGIoT evolve in the next 10 years?

At the human-device interface, the NGIoT is enabling novel applications through new dashboards, powered by AR, VR or MR, combined with digital sensing such as haptic feedback and automation speech recognition and interaction. This will only become possible through advanced networks such as 5G.

AI techniques and ML models are now being placed onto IoT devices, in a shift to Edge Intelligence. This is powered by technology such as microcontrollers and advanced optimisation, and enabled by orchestration or network slicing through 5G networks. The application of intelligence on the Far Edge, rather than in a central cluster on the Near Edge is seen as both of higher economic potential, as well as of currently lower technological maturity. Far Edge nodes can also take advantage of physical locality for easier data transfer.

Reducing computational and energy use is another frontier for the NGIoT, through techniques such as THz communications or backscatter networking. Energy harvesting from the ambient environment can also help alleviate this problem.

Distributed ledgers will enable new modes for data, such as decentralised cloud, and techniques such as homomorphic encryption of data will ensure privacy and security.

GAIA-X offers a new frontier in European collaboration, and now is the time for its principles to be translated into regulation and standards. Collaboration between developers and standards organisations, particularly the specific task forces involved in NGIoT applications will be key to the success of the initiative.

5.2 What elements are needed to ensure the success of the NGIoT?

The key to success will be opening up both software and hardware to allow for contributions from all sectors of the ecosystem. Placing values such as usability and applicability at the core of technology development will be key to wide adoption. Collaboration in development, implementation and standards is necessary.

Incentives to move the solution developers, particularly start-ups, from resorting to cloud hyperscale providers located outside Europe are needed.

A focus on commercial exploitation of NGIoT results, particularly for research projects, by defining and fostering IoT business models will be key to wide adoption.

Open, hybrid edge-cloud architectures, enabling semantic compatibility between data sets, privacy and trust, and integrating these concepts by default into the architecture of the NGIoT is another crucial element for success.

5.3 Which domains will NGIoT technology have most impact on?

The four priority sectors for the NGIoT application are Agriculture, Energy, Manufacturing and Mobility, with further use cases developed across the domains of Health, Smart Homes, Personal Data Management, Safety, Infrastructure Management and Environmental Sciences.

5.4 Where is Europe's position relative to the world?

The key competitors for Europe in the NGIoT come from China and USA.

Europe has defined a clear ownership model for IoT device data, but most of the device makers are located outside of Europe, making enforcement difficult. AI applied to machines, particularly on the Far Edge, is a key sector where Europe can advance.

Europe has industrial leadership in automotive, manufacturing, privacy and sustainability, but the development of specific products is now needed, which is an area that China is leading on. We are also behind other global players in applying and deploying edge AI technologies and platforms in real world verticals.

5.5 Next steps for WP2 EU-IoT GUIDE

During the first year of the EU-IoT project, WP2 has established all the planned bodies (EG, CB, AB) to ensure coordination across the NGIoT initiative, and with the wider IoT ecosystem. By collecting insights from the IoT community, this work package provided and validated a full map of the European IoT ecosystem, which through reports such as this deliverable, as well as the white-paper 'Towards a Vibrant European IoT Ecosystem' (D2.1 and D2.2) will guide European IoT policy for the next 10 years.

For the following year, WP2 will be dedicated to consolidating the collected inputs and validating the policy roadmap through 2 more EG sessions, in March and September 2022, as well as through regular CB and AB meetings. These will crystalise into a deliverable outlining the NGIoT roadmap including relevant policy recommendations, with an interim version released in March 2022, and the final version in September 2023.

ANNEX 1: EXPERT GROUP SESSION ACTIVITIES

In the figures below, we present the full outcomes collected from Experts as part of the consultation workshops, both in the first session in March, as well as the second in September 2021.

First Expert Group Workshop

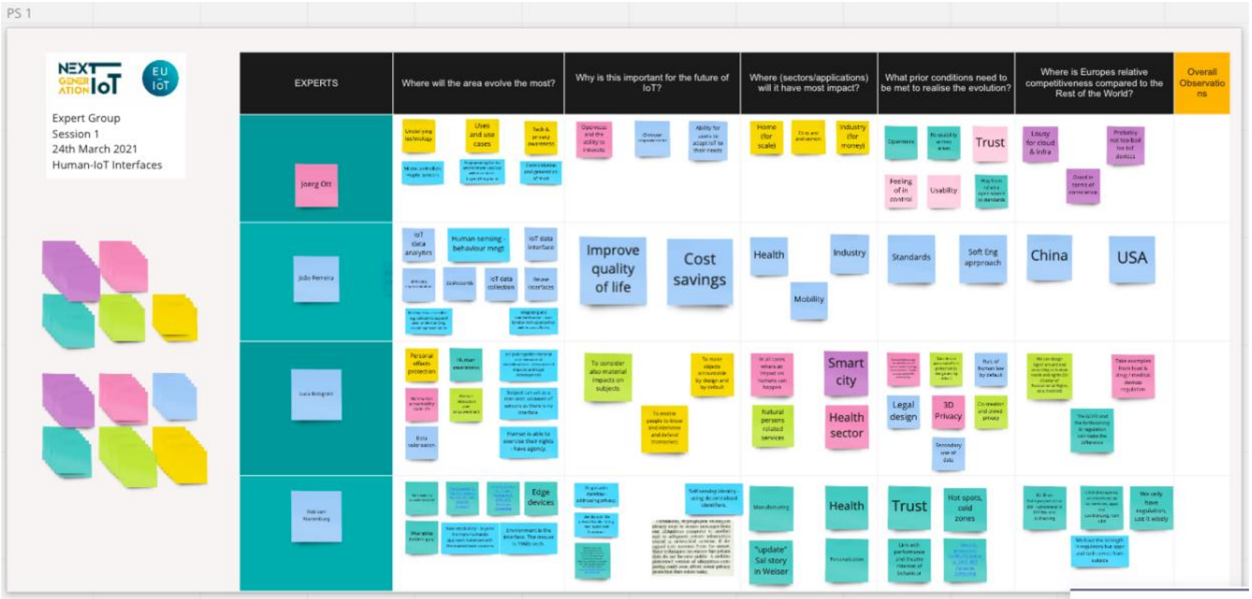

Figure 6: Miro board for Group 1

Figure 7: Miro board for Group 2

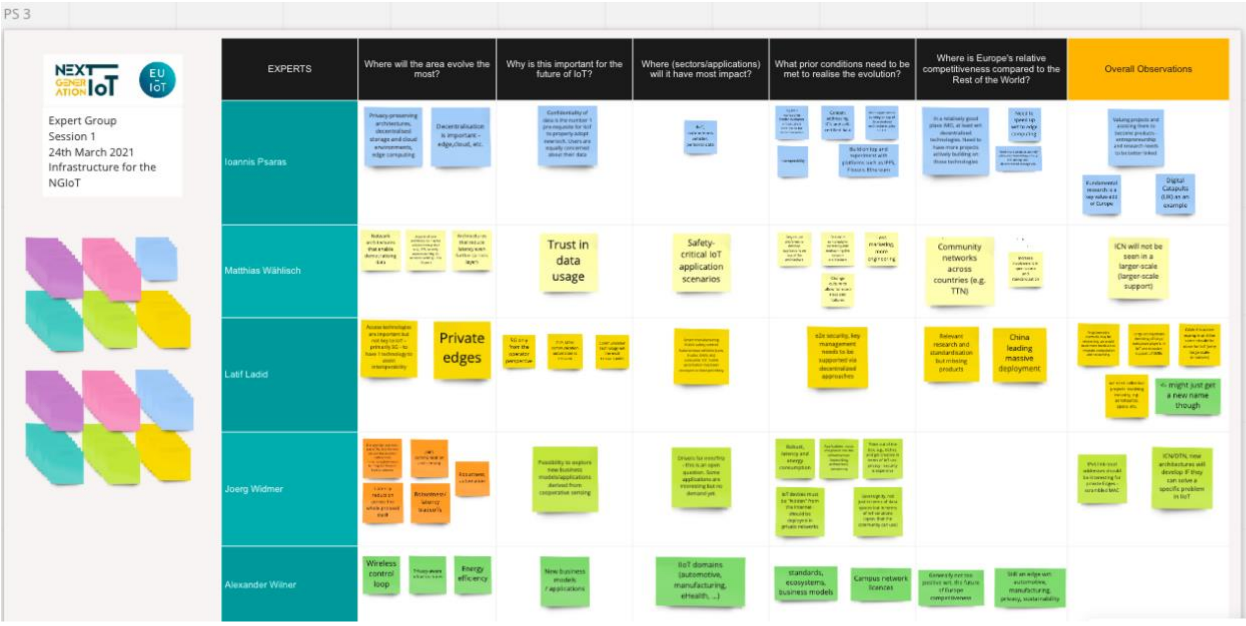

Figure 8: Miro board for Group 3

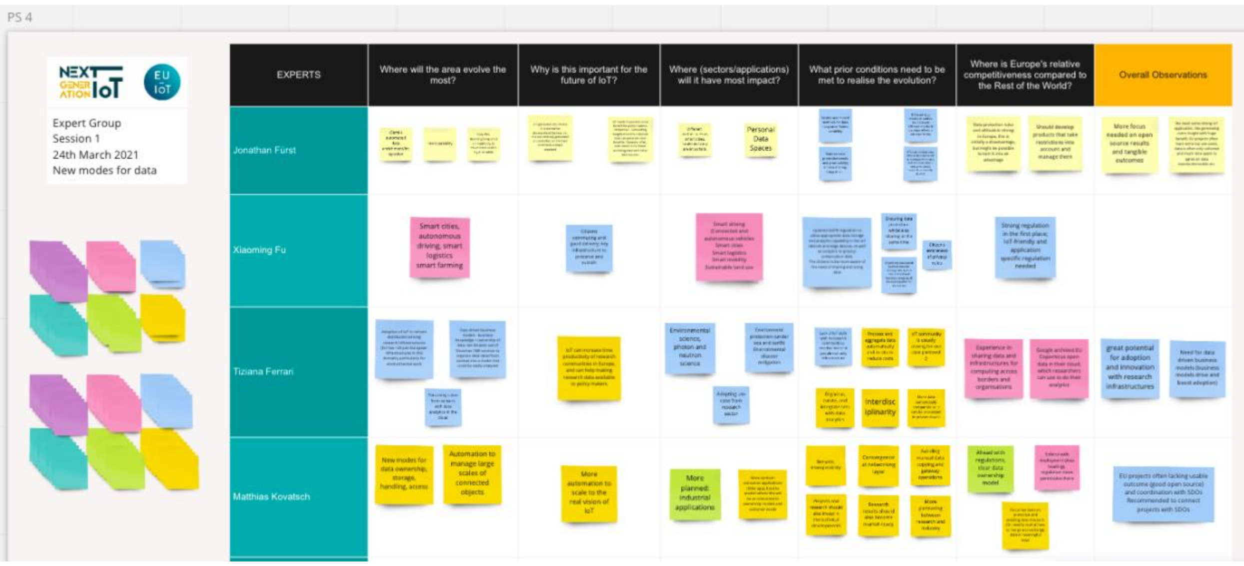

Figure 9: Miro board for Group 4

Second Expert Group Workshop

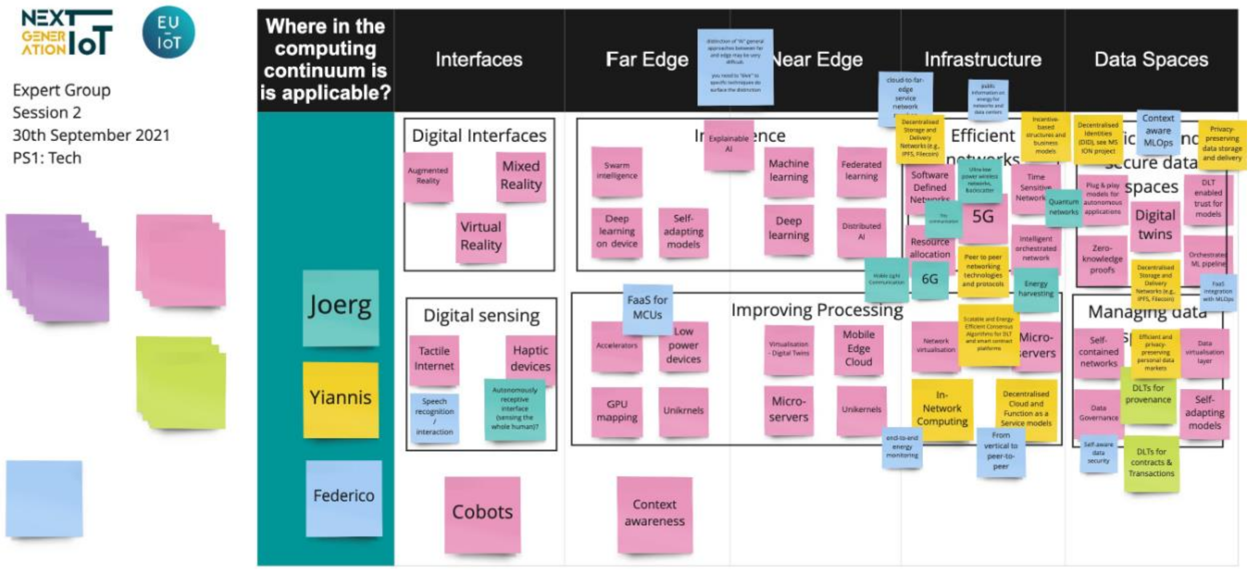

Figure 10: First Miro Board for Group 1

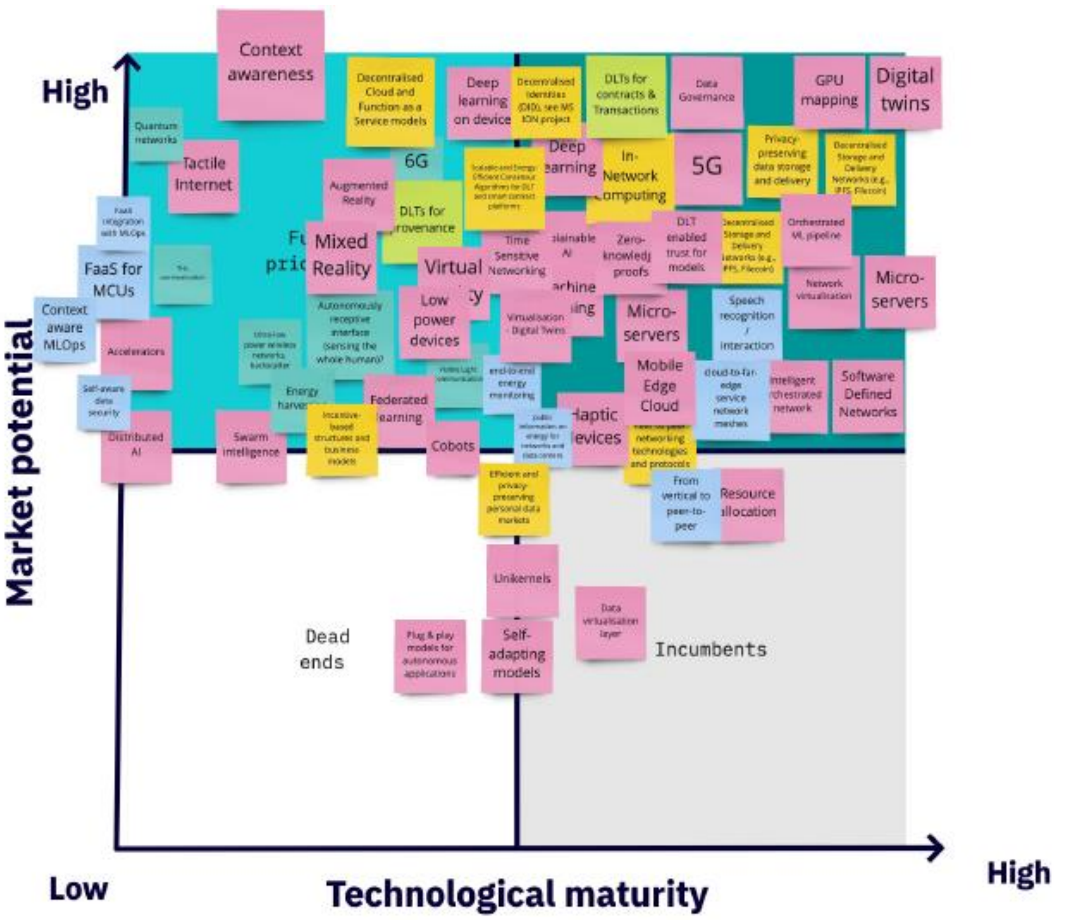

Figure 11: Second Miro Board for Group 1

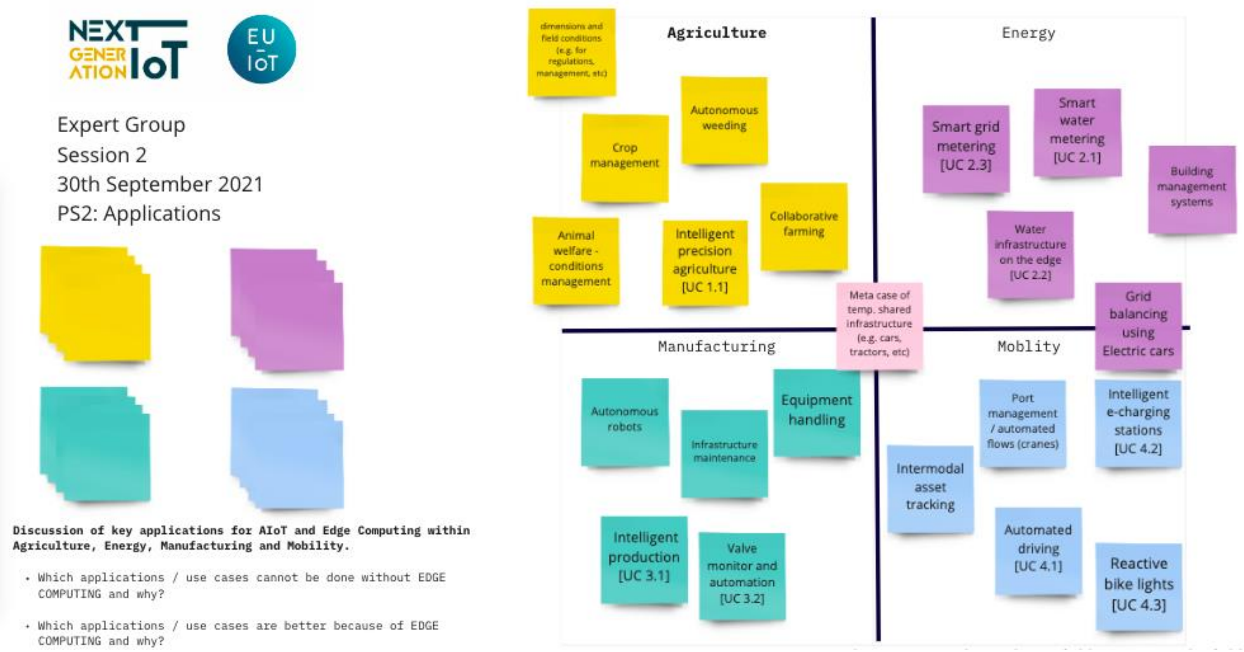

Figure 121: Miro Board for Group 2

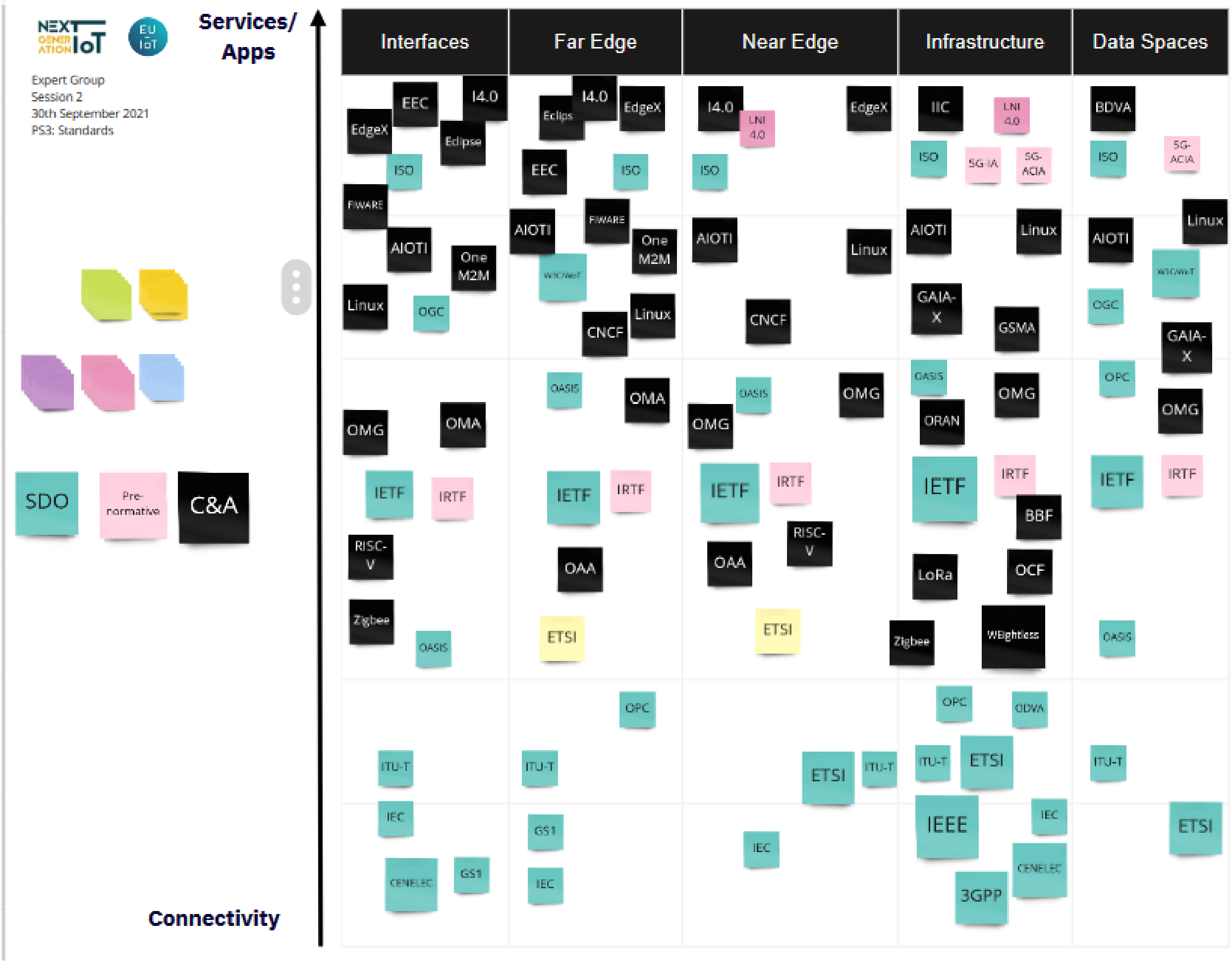

Figure 132: First Miro Board for Group 3

Figure 14: Second Miro Board for Group 3

ANNEX 2 - CURRENT EXPERT GROUP MEMBERS

As of October 2021, the EU-IoT Expert Group is composed of the following members:

Table 2 Expert Group membership October 2021

Name	Affiliation	Role	Area(s) of expertise	Sector
Joao Ferreira	Instituto Universitario de Lisboa	Assistant Professor with Aggregation; head of IoT Lab	Security and trust; Standards and interoperability; IoT applications; Enabling technologies; Skills and training	Academia
Rui A. Costa	Ubiwhere	CEO	IoT applications; Green deal	Corporate
Eiko Yoneki	University of Cambridge	Head of Data Centric Systems Group	Data processing architectures; Enabling technologies	Academia
Rob Van Kranenburg	IoT Council	Director	IoT applications	Non-profit
Matthias Wählisch	Freie Universität Berlin	Head of Internet Technologies Research Group	IoT applications; Enabling technologies; Standards and interoperability; Implementation	Academia
Latif Ladid	IPv6 Forum	Founder & President	Standards and interoperability; IPv6	Academia/ Non-profit
Jörg Ott	Technische Universität München	Chair of Connected Mobility	IoT applications; Enabling technologies; Data processing architectures; Skills and training	Academia
Joerg Widmer	IMDEA Networks Institute	Research Professor and Research Director	Enabling technologies; Implementation	Academia
Jonathan	NEC	Research	IoT applications;	Academia

Fürst	Laboratories Europe GmbH	Scientist	Data processing architectures	
Alexander Wilner	CISS TDI GmbH	Managing Director	Standards and interoperability	Corporate / SME
Matthias	Huawei Technologies Duesseldorf GmbH	Principal Researcher	IoT applications; Enabling technologies; Standards and interoperability	Corporate
Xiaoming Fu	Georg-August-Universität	Professor and Head of Computer Networks Group	IoT applications; Data processing architectures; Enabling technologies; Skills and training	Academia
Georgios Karamanolis	Hellenic Blockchain Hub	Chairman of Hellenic Blockchain Hub	Enabling technologies; IoT applications	Corporate/SME
Ioannis Psaras	University College London	University Lecturer and EPSRC Fellow	Data processing architectures; Enabling technologies	Academia
Luca Bolognini	Istituto Italiano per la Privacy	President	Policy; Security & trust	Academia/ Non-profit
Wael Elrifai	Hitachi Vantara	Global VP of Solution	Enabling technologies; IoT applications; Business models	Corporate
Christian Winkler	Siemens AG	Senior Principal Expert IoT, Corporate Technology	IoT applications; Enabling technologies; Data processing architectures; Business models	Corporate
Tiziana Ferrari	EGI Foundation	Director	Enabling technologies; Data processing architectures	Academia/ Non-profit
Michael Boniface	University of Southampton	Professorial Fellow of Information	Data processing architectures;	Academia

		Systems, Head of the IT Innovation Centre	Enabling technologies; Policy	
Charles Sheridan	Google	EMEA Technical Director for Industrial IoT, Google Cloud	Data processing architectures; IoT applications; Enabling Technologies; Business models	Corporate