

Towards a vibrant EU IoT ecosystem

Strategy White Paper
November 2021

Authors:

Dr Monique Calisti, Dr Lamprini Kolovou (*Martel Innovate*)
Brendan Rowan, Dr Robert Pomohaci, Tanya Suarez (*BluSpecs*), Prof. Dr. Rute Sofia
(*Fortiss*), Prof. Dr. John Soldatos (*INTRASOFT International*), Prof. Dr. Mirko Presser
(*Aarhus University*)

The European IoT Hub

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

n g i o t . e u

EXECUTIVE SUMMARY

Over the last decade, the Internet of Things (IoT) has undergone rapid and extensive changes becoming a key enabler of digital transformation across many sectors and driving the adoption of data-driven decision-making systems, remote management solutions and automation processes. The IoT approach evolved into a paradigm that integrates a broad set of technologies, each of which are advancing at a rapid pace. Increasingly, IoT technologies and solutions, in combination with Cloud and Edge computing, are leading profound transformation across a variety of sectors and supply chains.

In this complex and articulated context, European stakeholders are mobilising forces to ensure the foundation of a digital transformation continuum able to strengthen the European data economy and ensure the rapid restart of our society. This requires the growth of a vibrant and sustainable ecosystem structured as a community of communities for European players to join forces and align on core priorities, by overcoming their main diversities (of interests, backgrounds, and contexts) and converging around some essential core principles:

- **Boost industrial competitiveness** and sustain the economic recovery and growth.
- **Promote sustainable development** of our society in the respect of the environment.
- **Ensure European digital autonomy** and technological sovereignty.


Within this context, the EU-IoT Coordination and Support Action ambition is to act as a "hub" facilitating liaisons, collaborations, exchanges and promoting accordingly the activities and outcome of the various relevant projects and initiatives. The EU-IoT guiding principle is that to build a vibrant and impactful European IoT ecosystem, it is necessary to 1) map and engage all relevant research, innovation and policy initiatives, 2) identify the core market pull needs and technology push trends, and finally 3) coordinate and align on a common ambition and plan with all key stakeholders. The ambition is to support the development, harmonisation and consolidation of a common research, innovation, and policy roadmap for NGIoT in Europe that can guide efforts and translate into a concrete set of actions, processes and tools facilitating interaction and collaboration and grounding a vibrant and sustainable ecosystem. Such an ecosystem will grow as a community of communities and as a diverse and widely embracing movement cutting across several research and innovation areas and market segments.

This document is a revised version of deliverable *D2.1 Towards a vibrant EU IoT ecosystem* that takes into account additional information that was gathered by the consortium, including the input provided by prominent experts that have been engaged either via consultations with the EU-IoT Expert Group (EG), the EU-IoT Advisory Board (AB), as well as selected representatives of the ongoing IoT projects funded under the H2020-ICT-56 Call (gathered within the EU-IoT Coordination Board, CB). This includes:

- **An updated mapping** of various relevant efforts and initiatives.
- **A guidance framework** that has been developed to capture experts' input, together with the main outcomes of the EU-IoT EGs workshops and the AB meetings.
- A structured presentation of input gathered from ongoing EC projects, via CB dedicated sessions, that highlights major trends and priorities mapping them into the same framework used with the EG.
- A wrap-up view on how the EU-IoT plans to act as a living hub connecting the various forces and stakeholders for the growth of a vibrant and sustainable European IoT ecosystem.

Table of Contents

EXECUTIVE SUMMARY	1
THE NEXT GENERATION IoT LANDSCAPE	4
A European IoT Hub to Connect the DOTs.....	5
About this paper	7
SCOPE AND METHODOLOGY.....	8
“Towards a vibrant EU IoT ecosystem” scope	9
Methodological approach	9
THE NGIoT CONTEXT.....	12
Zooming into the EU-IoT sphere of action	13
A GUIDING FRAMEWORK TO ANALYSE R&I PRIORITIES WITHIN THE NGIoT.....	15
Human-IoT interface	18
Far Edge (device), Near Edge (gateway).....	21
Infrastructure	26
Data Spaces.....	30
MAPPING R&I ACROSS NGIoT.....	35
Technology priorities	36
Market priorities.....	37
Policy and standards priorities.....	38
Skills priorities	39
REALISING THE FUTURE OF THE NEXT GENERATION IoT.....	40
A point of convergence and collaboration – the future of the human-cloud continuum.	41
Intelligence across the board from TinyML to HPC for AI in the Cloud.....	41
Towards Interoperability: the role of Open-source and Open Standards.....	42
A value chain led transition towards edge solutions.....	43
A shifting landscape for specialists, changing roles and skills?.....	43
The impact for a green transition; the missing pieces.....	44
NGIoT ECOSYSTEM INITIATIVES.....	45
REFERENCES.....	54



THE NEXT GENERATION IoT LANDSCAPE

Over the last decade, the Internet of Things (IoT) has undergone rapid and extensive changes becoming a key enabler of digital transformation across many sectors and driving the adoption of data-driven decision-making systems, remote management solutions and automation processes. Once narrowly understood as machine-to-machine (M2M) communication, IoT has shifted to a paradigm that integrates a broad set of technologies, each of which are in themselves advancing at a rapid pace, including Cloud and Edge computing, Artificial Intelligence (AI), 5G, etc. Increasingly, IoT reaches across the traditional sensor-network-server coupling and will have far-reaching impact across the future of EU technological dominance in several vertical domains.

In this complex and articulated context, European stakeholders are mobilising forces under the lead of the European Commission (EC) and in close coordination with several national and international initiatives, to ensure the foundation of a digital transformation continuum able to strengthen the European data economy and ensure the rapid restart of our society.

As presented in the “Next-Generation Internet of Things and Edge Computing – Fireside Event Report from the Fireside Chat of 9 March 2021 [1]”, it is of utmost importance that European actors join forces to avoid silos, by exploiting existing strengths, and seizing the opportunity of rapid development of Next Generation IoT (NGIoT) and Edge computing ecosystem.

In this respect, the work done by Coordination and Support Action (CSA) projects such as EU-IoT is crucial to ensure alignment on priorities and strategies across various existing communities, as well as ongoing Horizon 2020 Research and Innovation (RIA) projects and upcoming Horizon Europe ones, at work for the development of trustworthy, sustainable, and human-centric technologies.

A European IoT Hub to Connect the Dots

The EU-IoT guiding principle is that to build a vibrant and impactful European IoT ecosystem, it is necessary to:

- 1) map and engage all relevant research, innovation, and policy initiatives,
- 2) identify the core market pull needs and technology push trends, and finally
- 3) coordinate and align on a common ambition and plan with all key stakeholders.

The ambition is to support the development, harmonisation and consolidation of a common research, innovation, and policy roadmap for NGIoT in Europe that can guide efforts and translate into a concrete set of actions, processes and tools facilitating interaction and collaboration and grounding a vibrant and sustainable ecosystem. Such an ecosystem will grow as a community of communities and as a diverse and widely embracing movement cutting across several research and innovation areas and market segments.

In this respect, EU-IoT aims to act as a ‘hub’ facilitating liaisons, collaborations, exchanges and promoting accordingly the activities and outcomes of the various relevant projects and initiatives. The challenge is to overcome the diversity and identify a set of commonly agreed upon objectives and priorities that are key to foster the development of synergies and exchange in a broader perspective with the larger community, including both academia and industry.

Acting as the hub of a network-of-networks or community-of-communities, EU-IoT brings together both primary players and the community at large of the NGIoT ecosystem, including:

IoT innovators and researchers

- Developers and providers of innovative IoT solutions from corporate R&D Labs, as well as IoT innovators, SMEs and Start-ups.
- Academic and corporate researchers and scientists in the IoT field, covering different related research domains such as Edge and Cloud computing, communication networks, AI, Big Data, Data Analytics, etc.

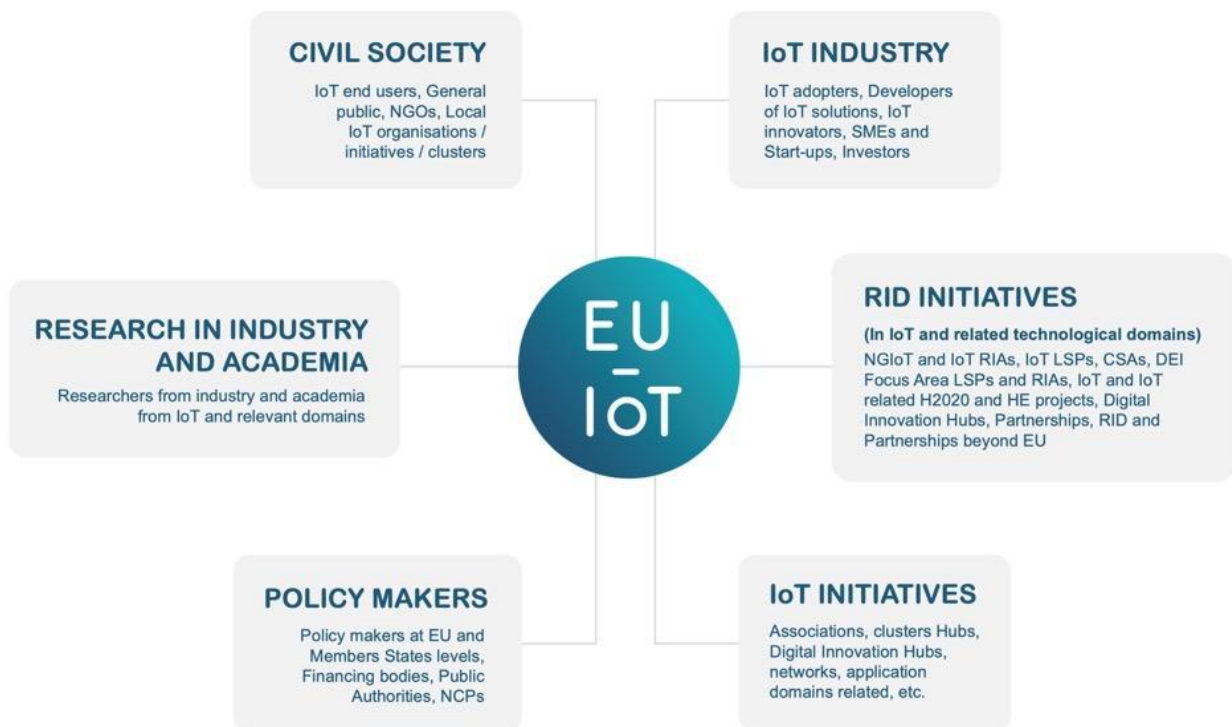


Figure 1: NGIoT ecosystem and EU-IoT positioning

NGIoT ecosystem / EC funded IoT (and related) projects

- Upcoming (under Horizon Europe) and running NGIoT projects, as well as Large Scale Pilots (DEI Focus Area), IoT LSP projects, and other H2020 ones – see section 2.

NGI ecosystem

- The projects' partners already engaged in ongoing NGI projects - as well as third party project beneficiaries, involved networks and communities including universities, research centres, SMEs/Startups and NGOs.

Market / Industrial driven initiatives

- AIOTI, ARTEMIS-IA, GAIA-X, SNS/5G PPP, DAIRO/BDVA, FIWARE, etc.
- IoT Digital Innovation Hubs.

Standardisation bodies, pre-standardisation and open-source initiatives

- Standardisation bodies and entities focused on the development of interoperable IoT solutions and services, such as but not limited to ETSI, IEEE, the OPC Foundation, the Industrial Internet Consortium, the Internet Engineering Task Force (IETF), W3C and 3GPP.
- Pre-normative bodies focused on the pursuit of novel directions that assist interoperability and productivity, as well as flexibility of services, such as the Internet Research Task Force (IRTF), specific study groups and task forces of ETSI, 5GPP, IEEE, IoT Forum, for instance.
- Open-source initiatives such as FOSDEM, IOTA, OpenStack, FIWARE, Linux Foundation, Apache, Eclipse Foundation.

Policy makers, security and privacy stakeholders

- Public national and EU organisations developing a regulatory framework for the European IoT market such as ENISA (European Union Agency for Cybersecurity), Body of European Regulators for Electronic Communications (BEREC), Organisation for Economic Co-operation and Development (OECD).
- Security and privacy stakeholders, organisations, working groups, researchers, technology providers, IoT infrastructure providers.

Enlarged community, IoT Users

- IoT industry adopters across various domains - given the cross-cutting nature of IoT, several different verticals (automotive, energy and utilities, health, agriculture, retail, industry, smart cities), are adopting IoT technology within their production processes (industry 4.0, smart agriculture) and launching 'smart products' in the market. European industry IoT adoption though is still slow. Challenges to overcome include a rather fragmented regulatory framework, lack of standards, limited adoption of IoT best practices, lack of skills, lack of resources, etc.
- Industries' associations: considering consumer IoT entities and industrial IoT entities such as the Industry 4.0 consortium, the LNI4.0 association, the OPC-UA alliance, the 5G Automotive Association, etc.
- End users / citizens: many EU individuals are already using 'IoT enabled devices' - see smart home applications and wearables devices, etc. However, often data privacy and security remain a concern, as well as possible side effects on health or impact on the environment. In this respect, engagement of end users/citizens as ultimate demand-drivers is crucial and will be fostered at the ICT-56 RIAs planned use cases/demos level. Exploratory spaces are needed where lead and alpha users can contribute and offer paths for progress in the NGIoT research, standardisation, etc.

About this paper

This document is the revised version of deliverable D2.1, which was released beginning of April 2021, with some additions and various updates considering the input from several consulted experts, via the EU-IoT Expert Groups and via the EU-IoT Advisory Board, but also from various EC representatives and ICT-56 players. This document includes:

- Definition of the scope and methodology to gather/elaborate information (section 2).
- An updated mapping of various relevant efforts and initiatives (section 3).
- A guidance framework to capture experts' input (first part section 4), together with main outcomes of the first EU-IoT Expert Groups (EG) workshop (second part section 4).
- A set of key areas of interest mapped to this guidance framework, for research and innovation within the NGIoT, as these were specified through the discussion and interaction with the members of the EG, CB and AB (section 5).
- A set of conclusions and visions provided by the EU-IoT Consortium centering on the pillars that will define the NGIoT over the coming 3-5 years (section 6).

The contents of this paper will be further enriched and elaborated leading to another iteration in early 2022 as the "NGIoT roadmap and policy recommendations".



SCOPE AND METHODOLOGY

“Towards a vibrant EU IoT ecosystem” scope

The Next Generation Internet of Things (NGIoT) initiative is a growing community of projects and related initiatives at work to maximise the power of IoT made in Europe. NGIoT works to lower the barrier for adoption and development of IoT-empowered solutions, by supporting business models, innovation and skills. In a “network of network” ecosystem, NGIoT consists of ongoing projects and upcoming funding opportunities at work for a human-centric and sustainable digital transition.

NGIoT projects are working to achieve H2020 goals while Horizon Europe will bring new opportunities to launch research and innovation projects across Europe and beyond. NGIoT works in close collaboration with related technology networks including cloud, Edge, Artificial Intelligence, 5G telecommunications networks and services, cybersecurity and blockchain.

This document is intended to be a guide to the key current trends and future direction of IoT developments, providing also a map of the most relevant actors within this ecosystem. Based on the data gathered and insights elaborated under the lead of the EU-IoT Work Package 2, recommendations to ensure that Europe is in a leading position to benefit from these emerging technologies are given. This deliverable provides indications for policy makers at regional, national and international level to better understand the IoT research, innovation, and adoption trends and challenges, and it provides the NGIoT ecosystem participants a commonly shared understanding of future work and investments directions.

Methodological approach

The EU-IoT consortium has put in place and followed an agile methodology, to allow efficient extraction, collection, synthesis and validation of valuable information from online and offline resources, but also from external stakeholders - covering a broad range of areas covered by the various NGIoT projects and related initiatives. The work was organised as depicted in the diagram of Figure 1 and it is organised in three subsequent phases as described below.

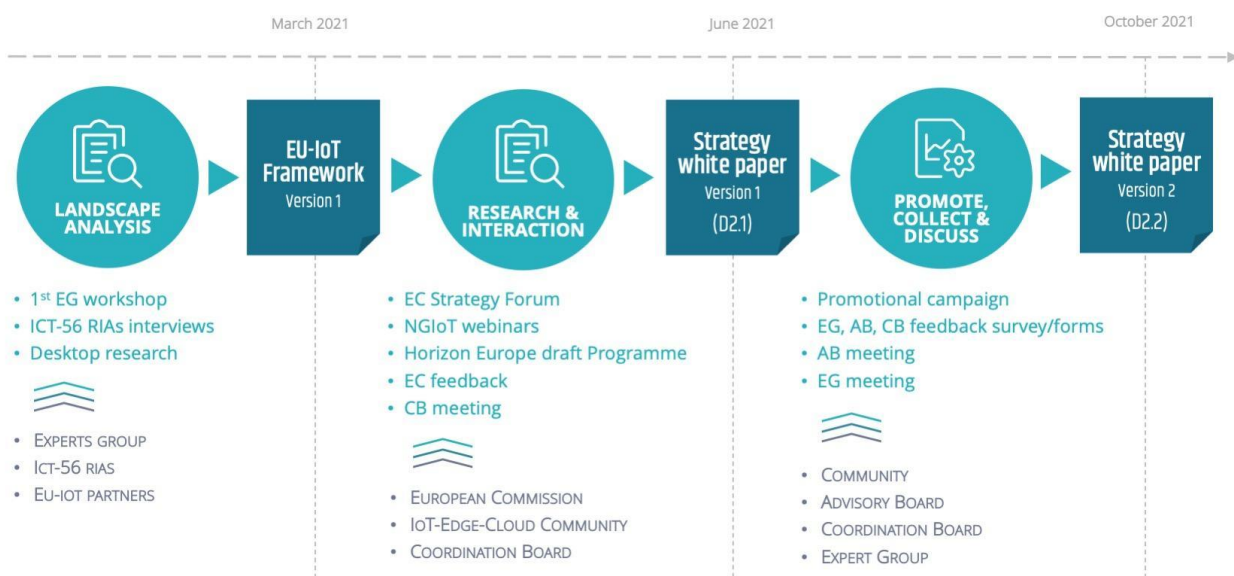


Figure 2: Strategy whitepaper methodology

Landscape analysis

Target: To understand and analyse the needs of the NGIoT growing community and create a mapping process and a framework that allows EU-IoT to properly capture the core requirements and needs, despite the diversity, while considering the specificity of different cases.

Tools & stakeholders: The EU-IoT Expert Group (EG) members provided their views, experience, know-how and opinion during the 1st EG workshop, as well as offline directly to the EU-IoT team, while a number of interviews organised with the Coordinators and representatives of the six ICT-56 NGIoT newly funded RIAs, collecting information around the aspects and areas they are dealing with in their project's planned activities. An extended desk research activity was also conducted collecting and studying information from relevant literature, online and offline studies, reports and SRIAs and related initiatives of the NGIoT community at European and international levels.

Output(s): the 1st version of EU-IoT Framework.

Research and interaction:

Target: To collect feedback on the draft EU-IoT Framework and ensure alignment on priorities and strategies across various existing communities, initiatives and ongoing Horizon 2020 Research and Innovation (RIA) and Coordination and Support Action (CSA) projects within the context of the planned EU-IoT activities and in the form of a white paper that will be promoted and discussed within the community.

Stakeholders / tools: Valuable information collected, analysed and validated through close interaction with representatives from all the types of the NGIoT community stakeholders, though the organisation of the EC Strategy Forum, the participation to the NGIoT CSA thematic webinars, the 1st Coordination Board (CB) meeting, the discussion with EC representatives and analysing the draft version of the Horizon Europe Programme published by the EC.

Output(s): the 1st version of the EU-IoT Strategy Paper¹ (deliverable 2.1) that also includes a second version of the EU-IoT Framework.

Promote, collect, and discuss:

Target: To validate and collect feedback for the published and promoted 1st version of the Strategy whitepaper through discussion and interaction with the community.

Stakeholders / tools: A dedicated promotional campaign took place for the dissemination of the 1st version of the Strategy whitepaper, a short survey implemented and feedback forms were collected with the participation of the AB, CB and EG members, dedicated sessions and discussions organised during the AB and EG workshops.

Output(s): The current 2nd version of the Strategy whitepaper (deliverable 2.2).

The contributors:

The stakeholders participating in this process through the EU-IoT bodies (AB, CB, EG) cover a wide range of IoT and IoT related domains and they are coming from all the areas of policy and strategic planning, industry, and research.

The EU-IoT AB is constituted by experts on IoT and related thematic areas representing key initiatives in the EU landscape (Open & Agile Smart Cities initiative (OASC), IDC European Government Consulting unit, BDVA, FIWARE and more) and coming from both the industry and the Academia².

The EU-IoT EG is composed of 21 members that as depicted in the diagram below are covering a wide range of key areas around IoT.

¹ <https://www.ngiot.eu/download/towards-a-vibrant-eu-iot-ecosystem/>

² <https://www.ngiot.eu/advisory-board/>

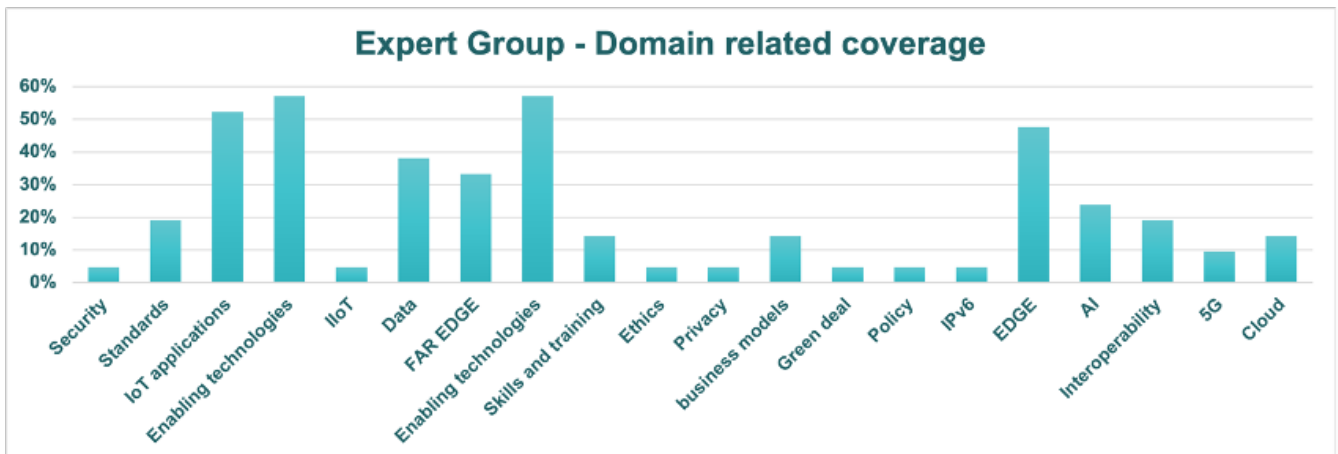


Figure 3: Expert Group- Domain related coverage

The EU-IoT CB is consisted by representatives from (a) the six ICT-56 RIAs covering areas related to IoT / M2, & 5G/MCM communications, Tactile, AR/VR, 5G MEC, SDN and virtualisation, 5G RAN, MEC e-logistics, data management and security, Hybrid cloud edge - agent system, human in the loop, Distributed AI, HW accelerators, Hybrid cloud edge - multimodal architectures, Distributed AI, HW accelerator and more, (b) the OPEN DEI and NGIoT CSAs, (c) the EC.



THE NGIOT CONTEXT

MAPPING RELEVANT INITIATIVES

The EC has planned investments in several research and innovation directions that are key drivers for the NGIoT, including Edge computing, distributed AI and analytics, augmented reality, tactile Internet, real-time applications, data-centric/secure architectures, 5G/6G networks, etc. At the core of the NGIoT vision is the ambition to enable a major shift: from digitally enabling the physical world towards automation and augmentation of the human experience with the connected world thanks to secure, resilient, safe, and trustworthy IoT. By ensuring privacy and security, while improving usability and user acceptance, EC-driven efforts push for an evolution of NGIoT infrastructure platforms so that - thanks to increasingly decentralised architectures automating processes at the edge - a variety of semi-autonomous and real-time IoT applications ensuring data privacy will be offered and new business opportunities will arise also for SMEs, Start-ups and Innovators.

The need to avoid fragmentation and foster convergence has been acknowledged by many initiatives in the last years. As a result, some other coordination efforts have been set up and could be capitalized without duplicating work. An example of this is the Transcontinuum Initiative³, which brings together input from: 5G IA, the 5G Infrastructure Association; AIOTI, the Alliance of Internet Of Things Innovation; BDVA, the Big Data Value Association; CLAIRE, the Confederation of Laboratories for Artificial Intelligence Research in Europe; ECSO, the European Cybersecurity Organisation; ETP4HPC, the European Technology Platform for High-Performance Computing; EU-Maths-In, the European Service Network of Mathematics for Industry and Innovation; and HiPEAC, the High Performance Embedded Architecture and Compilation project.

Key pillars and important milestones for this vision are rooted in several initiatives (see below), such as AIOTI, ARTEMIS, GAIA-X, Smart Networks and Services (SNS), and the Data, AI, and Robotics partnership, in which the EU-IoT partners are actively engaged and which represent the fundamental context for NGIoT-driven efforts to advance.

Zooming into the EU-IoT sphere of action

It is within this dynamic and rather articulated landscape that EU-IoT is operating to support and coordinate efforts among a variety of stakeholders and initiatives, in close collaboration with the EC, facilitating interactions and fostering synergies across the whole NGIoT ecosystem. The ambition is to effectively amplify the results and the impact of the various connected initiatives, within H2020 and beyond, acting as a coordination hub for a range of activities in the ongoing transition towards the Horizon Europe and Digital Europe Programmes.

The EU-IoT CSA started in October 2020 and will run for three years. As of today, EU-IoT is coordinating activities and providing support to the latest IoT projects, namely IntellioT, VEDLIoT, TERMINET, IoT-NGIN, INGENIOUS, and ASSIST-IoT. All these RIAs have issued or plan to issue Open Calls that will allow third-party organisations to join the NGIoT ecosystem. Support and coordination activities led by EU-IoT include:

Strategic positioning/road mapping activities

To ensure alignment on a shared vision and common goals to shape the digital future of Europe. Through the recently established EU-IoT Coordination Board (CB), which gathers coordinators of the ICT-56 projects and of the three CSAs, as well as EC representatives, experts' inputs are gathered and elaborated via consultations, interviews, workshops, webinars, and expert discussions on identified topics and priorities. This feeds into strategic guidance and policy recommendations, that are also enriched via the input of the EU-IoT Advisory Board (AB), grouping prominent experts from relevant domains⁴.

³ <https://www.etp4hpc.eu/transcontinuum-initiative.html>

⁴ <https://www.ngiot.eu/advisory-board/>

Community building

- Surveys/interviews to engage experts and gather input injecting into various planned activities and documents.
- Standardisation/pre-standardisation/open source: creating a map of relevant initiatives and facilitating input from/to various projects.
- The Next Generation IoT and Edge Strategy Forum to help shape the EC strategy and promote the results of relevant initiatives and projects.
- Organisation of two Hackathons, to engage the community and promote work and outcomes of the projects, in alignment with the EU-IoT vision and goals.
- Establishment of liaisons to other relevant bodies and initiatives - AIOTI, GAIA-X, IoT Forum, etc.
- The IoT Next Club gathers innovative SMEs and Start-ups running regular activities such as member showcases, Ask-Me-Anything events, open calls adverts, etc. to engage small to medium business players.

Recommendations about research priorities

Innovation strategies to standardisation, to facilitate activities towards standardisation and therefore, increase impact and stakeholder engagement.

Dissemination and communication

To amplify outreach and impact of ongoing projects via a dedicated Communication Task Force, the EU-IoT CTF.

Business modelling and acceleration support

For increased impact, starting from success stories and best practice use cases documentation, analysis of IoT skills needs/development leading to training and mentoring.

Impact assessment

Across the programme, identifying assets for European technological sovereignty and facilitation thereof.

The figure below gives an overview of the current NGIoT initiatives and projects.

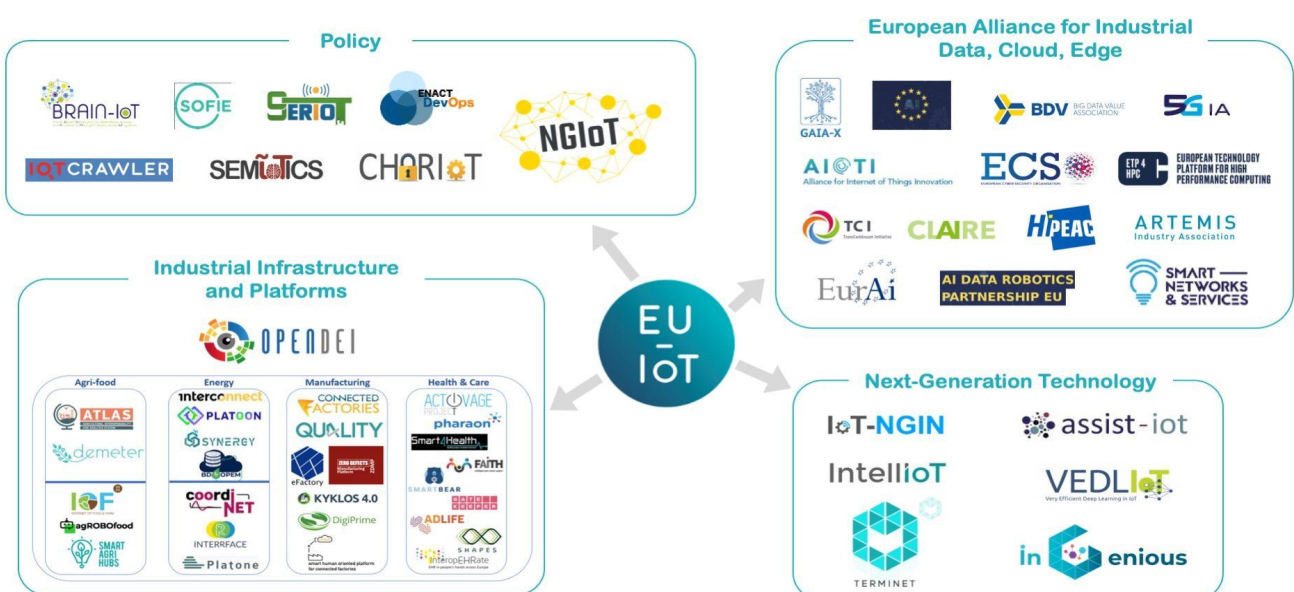


Figure 4: An overview of the current European NGIoT scenario



**A GUIDING FRAMEWORK
TO ANALYSE R&I
PRIORITIES WITHIN
THE NGIoT**

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, it is necessary to create a **mapping process and a framework** that allows EU-IoT to properly capture the core requirements and needs, despite the diversity, while considering the specificity of different cases. Staying agile and being able to capture needs in a fast-changing context is a major requirement that was accounted for within the EU-IoT project, when coming up with the framework that is proposed hereby.

The proposed EU-IoT framework operates along two axes, the first 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 identifies areas and themes of progress between and across them.

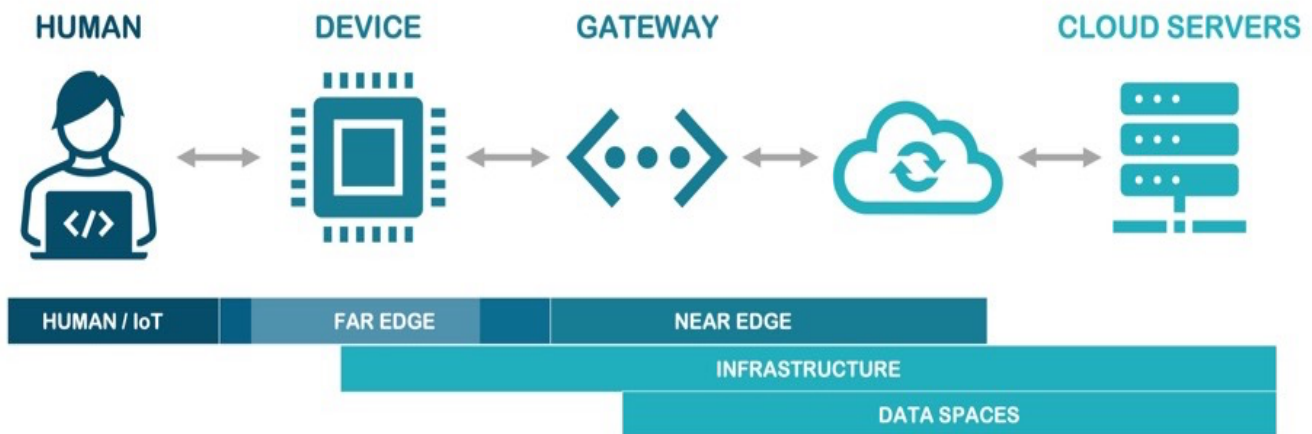


Figure 5: The IoT continuum - from human to cloud and back again with key interfaces

The second axis refers to five key research and innovation areas / technological contexts which can overlap and have a reach across the continuum that EU-IoT will focus on:

- the Human/IoT interface,
- the **Far Edge** (devices level),
- the **Near Edge** (gateway level),
- the **Infrastructure** (including networks) and
- the Data Spaces.

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 6.

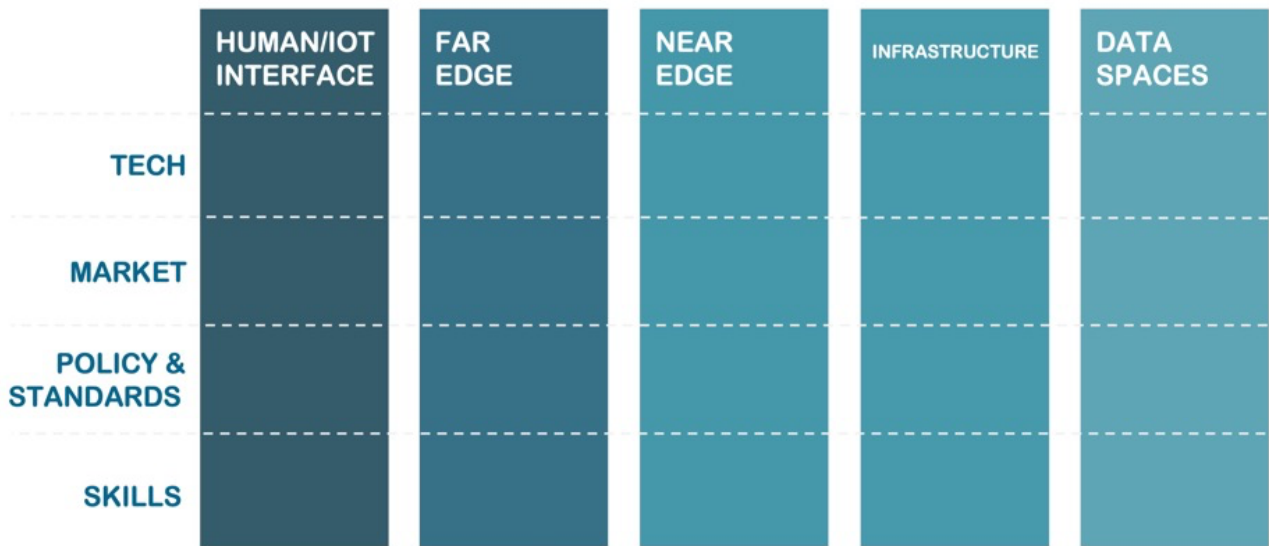


Figure 6: Guiding framework of the EU-IoT approach

These four main transversal dimensions focuses on:

- **Technology:** to identify novel and advancing enabling technologies.
- **Market:** to identify applications, services, and models enabled by the technologies (both individual and varied combinations).
- **Standards and policies:** to elaborate on common approaches, standards, and policies.
- **Skills:** to analyse the current and future demands resulting from all the above.

In the following, the focus is on each of the five key R&I areas, reporting on the main findings as gathered so far, by engaging prominent representatives via the EU-IoT Expert Groups (two workshops were held so far), via the Coordination Board meetings (two held so far), as well as the input gathered from the Advisory Board members (two dedicated meetings so far).

Area 1

Human-IoT interface

Technologies

- Mixed reality, allowing the overlaying of data into a user's field of view to complement decision-making.
- Tactile interfaces, resulting in faster and more efficient response times from operators.
- Co-bots, supporting humans in the Factories of the Future.
- Tactile Internet, consisting of codecs of the information and equipment to allow the user experience haptic feedback (data rate >1KHz).
- Biometrics and digital self-sovereign identities, which support fast and reliable user and device identification and authentication.
- Voice and speech user interface systems, allowing for direct human spoken interaction with computers, with responses enriched through AI algorithms.
- Advanced chatbots, supported by natural language processors and AI for uses such as customer services, request rerouting or information gathering among others.

Market

- Human-centred applications, interfaces designed with human needs at their core.
- Secure interfaces, to avoid unwanted information leaks from IoT devices.
- Remote support, to solve problems with devices without the physical presence of an operator.

Policy and Standards

- GDPR, the core of the European data protection regulation, aimed at ensuring that personal data is only collected and operated on where the need is clear and with consent.
- Next-Generation Internet, the EC initiative for re-engineering the Internet with European values at its core.
- IEEE SAB 1918.1, ETSI Tactile Internet group and 3GPP's 5G-NR Ultra-Reliable Low Latency Communication group.

Skills

- Operator 4.0, supporting factory workers with the skills they need to operate advanced technologies aimed at augmenting efficiency.
- Human-centred computing, considering the competences operators will need for mixed-initiative human-computer systems.

Trends and Future directions

Novel IoT interfaces are emerging, which will empower end-users to adapt this technology to their specific needs. These interfaces will bring significant cost-savings to users, and improve the general quality of life of humans, by empowering sensing for new uses and in new practical cases. These will not necessarily be completely new interfaces; **significant value is expected from the reuse of existing interfaces in a novel manner**.

In several IoT applications, **subjects will be transformed into non-users of IoT, unaware that the sensors are there, with the interface effectively disappearing unless necessary**. This will enable IoT devices to perform new functions such as personal effects protection, and collecting and valorising data seamlessly, empowering humans and improving their interaction with devices.

The environment will become the interface, with technology moving beyond legacy devices such as the mouse. The deployment of such technology on Edge devices is expected to further develop the IoT environment. Some of the key technologies enabling this evolution include:

- **Haptic sensors**, allowing devices to evolve within context, beyond phones, for the programming to better fit within their environment.
- **Micro controllers** embedded into IoT devices, powering functions such as machine learning or embedded AI, through techniques such as tinyML making the Artificial Internet of Things (AIoT) a reality.
- **Intuitive visual representation** such as Building Information Modelling (BIM) to improve the interaction of humans with data, on the collection, analytics, and display levels, making data more accessible.
- **Wearables** powered by Virtual Reality (VR), and Mixed Reality (MR).
- **Haptic-enabled/AI-empowered interfaces** to improve the man-machine complementarity.
- **Ultra-fast communication infrastructure** to meet the high availability, security, reliability and ultra-low latency of the Tactile Internet, imposed by human natural reaction times.

A key step of evolution will be the integration and standardisation of these interfaces with existing platforms, by applying familiar approaches within a given area or field. Another area of evolution for interfaces is enabling the generation as well as consolidation of trust, which is expected to solve some of the underlying privacy issues of IoT devices.

Novel human-IoT interfaces are expected to have most impact in the following sectors:

- Smart home
- Smart city
- Environmental applications
- Industrial applications in manufacturing – most value
- Health sector
- Smart mobility
- Personal data / personalisation services

Key considerations

The omnipresence of devices with novel human-device interfaces is expected to render them almost unnoticeable to the average subject [9]. This brings along new trans-humanist concerns with their own vocabulary considering the security and privacy implications of such technology [10]. Interfaces with privacy and security included by design and by default can help avoid the existing concerns and risks.

The emergence of novel interfaces also brings with it potential risks of exclusion. A digital gap will arise between those who can manage interfaces easily and those that lack the skills to do so. This risk can be mitigated through effective capacity building, by designing upskilling courses for the workforce to adapt to the use of the interfaces.

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 the ID check [11]. DIDs can keep the identity of users in private hands, bringing privacy into all the relevant layers and hardware. Combined with the concept of 5G/6G 'cold spots', where users can disconnect and no data is collected - as opposed to the hot spots of data collection - can help bring the concept of privacy in smart cities to the next level. Cold zones afford users a secluded period, resulting in an improvement of their wellbeing.

The emergence of novel interfaces raises significant concerns over human awareness, and the agency that subjects have in exercising their rights when interacting with IoT devices. Another relevant question is accountability and liability for the actions of machines, who bears responsibility for both material and immaterial results?

The key to ensuring the success of novel interface technology is the assurance of trust, by offering the end-users control over its functions. Users need support in understanding these technologies, to be able to intervene where required and defend themselves against unwanted side effects if necessary. A key to this will be to make IoT devices accountable by design and by default.

A shared methodology for the identification of human needs should be made part of the design process of novel interfaces. This should include a threat analysis. The methodology adopted by the European Digital Payments Industry Alliance (EDPIA) provides a good example. The development of novel interfaces, putting personal data protection at the core of the design process, by default, using data-driven methods will be the key to ensuring the rule of human law over machines by default. Through this legal design, secondary use of data will be done in a secure manner, anonymising personal subject details.

Support through standards that will foster the development of efficient next-generation IoT interface technology will be essential to their success.

Along with this, the interfaces need to be user-friendly, and applicable across different verticals. A key element to ensuring this is the openness of the technologies and embedding this openness into the standards.

Europe has a unique opportunity to design the NGLoT 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 upcoming AI regulation are designed to support the rights of Europeans with regards to novel technologies, assuring privacy and trust. There are however concerns that they can bring competitive disadvantages to IoT made in Europe, and raise regulatory difficulties for the European market. In designing future regulation for IoT interfaces, food, drug and medical device cases provide a good example.⁵

EU-IoT has been working to support the next generation of IoT practitioners through two and a half hours-long online training workshops, the highlights of which are summarised in the deliverable 'Report on Training Activities', released at the end of September 2022.

⁵ EU-IoT has been working to support the next generation of IoT practitioners through two and a half hours-long online training workshops, the highlights of which are summarised in the deliverable 'Report on Training Activities', released at the end of September 2022

From Europe to the world

Whilst Europe is in a good position in terms of conscientious personal data protection, and in an acceptable place in developing and regulating IoT devices and interfaces, there is room for improvement in the cloud and infrastructure areas. Also, most of the applications and the technology used with these devices come from outside Europe. Wise use of European regulation is to be made to ensure that users are protected from unwanted side effects of these applications and technologies. Europe 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^{6,7} with ephemeral identifiers providing a good example.

Area 2

Far Edge (device)

Area 3

Near Edge (gateway)

The notion of the Edge refers to computing resources located closer to the user than the cloud. This can be further split into the Far and Near Edge. The Far Edge therefore reflects computing resources located on the premises where the IoT devices are being used. The Near Edge refers to resources and services that are in the access or core regions. For more details, see the recently published EU-IoT Whitepaper 'A Vision on Smart, Decentralised Edge Computing Research Directions'⁸.

Technologies

- Fog computing, infrastructure setup where the data is processed, stored, analysed and communicated on the IoT gateway, within the local area network, decentralising operations from the cloud to the IoT Edge device.
- Edge Analytics, enabled through techniques such as Tiny ML, running intelligence on small, low-powered microcontrollers and small devices for low-latency, low power and low bandwidth model inference on Edge devices. Also includes data pre-processing, which can reduce bandwidth requirements and support edge computing. By taking advantage of these technologies, IoT devices can run ML applications on the Edge unplugged, on batteries for weeks or months.
- Micro/Nano CPUs, computer processors on a single integrated circuit, reducing the size for new applications.
- Connectivity guaranteed including multi-link aggregation (capacity of providing ubiquitous connection although the far-edge device is moving)
- Distributed architectures and applications, carrying out IoT processes through components located on different, physically unconnected platforms, connected over a communication network.
- Context-dependent IoT, devices that can be customised depending on the needs of their users or operators for efficient operations.
- Operating Systems optimised to be run on far edge and near edge IoT devices, embedding certain characteristics in a close-to-the-kernel fashion.

⁶ About Coalition, (2020) coalition.org

⁷ Secure Open Federation for Internet Everywhere project, (2020), <https://www.sofie-iot.eu/>

⁸ A Vision on Smart, Decentralised Edge Computing Research Directions, (2021), EU-IoT Consortium

- Software-defined networking that keeps pace with increasing demand for heavy traffic flows, while decreasing costs and enhancing network management at the edge.
- 5G/6G connectivity enables ultra-reliable division of computing resources to support data-rich and time-sensitive applications.
- Quantum computing, taking advantage of superposition and entanglement to improve computing.
- Open source solutions, allowing full free open collaboration in the development and deployment of IoT solutions, data interoperability, communication interfaces, cloud computing and networking. This approach reduces vendor lock-in and increases the freedom of users of technology, whilst also reducing the overall lifetime cost of applications.

Market

- Security at the Edge, over-the-air (OTA), considering the updates devices need to ensure their security and delivering them automatically.
- Contextual IoT, applications connecting inputs from the real world into ambient intelligence.
- Collaborative IoT, moving IoT operation to the Edge devices working together to reduce latency.
- Infrastructure-as-a-service (IAAS), allowing businesses to run their intensive computing on cloud servers through a pay-as-you-go model.
- Social IoT, which enhances the direct intervention of the user with the IoT infrastructure, which could be focused on far edge and near edge nodes.
- Holographic and multi-sense media, urging for offloading high processing loads to the near edge.

Policy and Standards

- Open standards, enabling developers to work together on open-source solutions, as well as creating interoperability within and between different data spaces. This will lead to the creation of dynamic value chains with processes which are supported across different platforms and data spaces. These standards can also be implemented on closed as well as open source software technologies.
- Multimodal architectures, an open infrastructure allowing for multiple modes of interaction required for cooperative IoT.
- Human as an IoT device, considering humans as a node in the IoT continuum in designing applications. This term does however raise ethical issues, particularly in terms of the mercantilisation of human rights, which need to be fully considered in policy approaches.
- Multi-access Edge trust, defining the access policies for Edge devices accessed by multiple users and operators.
- Domain-specific architecture models for IoT at the Edge such as Smart Grid Architecture Model (SGAM), Reference Architecture Model for Industry 4.0 (RAMI4.0), Multi-Access Edge Computing from ETSI, or the 3D IoT Layered Architecture from AIOTI/CREATE-IoT.

Skills

- Deep learning, supporting subjects to develop models that can learn in an unsupervised manner from unstructured data.
- Human-in-the-loop, considering the role of humans in the IoT operations.
- Applications on the Edge, teaching operators the skills they need for using NGIoT applications on Edge devices.

Trends and Future directions

Today, it is estimated that 80 percent of IoT operations are managed in the Cloud, and 20 percent on the Edge level. Within the next five years, this ratio will be turned upside down with just 20 percent on the Cloud and 80 percent on the Edge level. Novel IoT systems are therefore expected to be based on a hybrid Edge/cloud architecture. The specific delimitation, definition and architecture of the Edge varies depending on the area of application of the concept. The evolution of the NGIoT will lead to AI models being distributed from cloud to Edge, as well as active, federated and transfer learning. Placing intelligence at the Edge will fill in the high demand for speeding up decisions and assist with the validation of extracted information from data. Reliability, bandwidth, security, privacy, sustainability, and real-time reaction and decision-making of IoT devices will be improved by adding intelligence, all leading to a reduction in costs. Edge intelligence will limit data transfer, enabling low connectivity apps, saving storage, as well as optimising power consumption and traffic pattern design.

The next frontier in IoT at the Edge is the location of the data source. Clearer knowledge of the source of data will increase the functions and therefore value of IoT. Data processing capabilities are moving from the cloud to the edge. To match this, new optimisation techniques are needed, going beyond the currently used Gaussian processes. There is no obvious reason to drive data and intelligence to the cloud rather than the Edge. Intelligence at the Edge will move perception closer to where the data is generated and sensed by IoT devices, as per customer requirements, and will increase trust in the system. Machine learning and privacy preservation must however be included from the very initial design stages, to ensure that the integration of intelligence and data and user privacy are considered at all stages.

Adding intelligence on Edge devices is expected to open-up the execution of IoT functions from a centralised location to anywhere, or at least a hybrid model. This will mean that the need to write new algorithms will be greatly decreased, opening up IoT devices for further use. Future applications are expected to have an almost universal degree of abstraction, removing the complexity in various development aspects, i.e., automation, architecture, workload.

The next step in machine learning is incremental learning 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. To verify whether a data set is useful when carrying out the data transfer, differential compression is preferred to the standard of time stamping. An approach of sharing models, data and platforms will help ensure the bigger picture is taken into consideration and result in efficient ML.

The addition of AI hardware accelerators on constrained Edge devices is expected to be a major milestone in the integration of intelligence at the Edge. This will result in seamless computing across the continuum, from Edge to cloud.

Advancing intelligence on the Edge will be further supported by the integration of open source technologies (e.g. EdgeX Foundry, IoT Programming). A degree of open source standardisation at the Edge is to come as a result, with quality control and visual control of devices set to become the norm. A good example is the MIT Enigma, which aims to create a decentralised, open-source protocol where anyone can perform computations on encrypted data, ensuring privacy for smart contracts and

public blockchains. Smart contracts can therefore become secret contracts.

Security concerns over IoT accompanying the proliferation of devices are expected to lead to a decentralisation of the control over individual devices to the user. In these applications, the standard system-on-a-chip approach used previously will no longer work, as writing and optimising the programmes controlling these is time-consuming, it is therefore likely the use of simulators will proliferate.

Further information on the EU-IoT efforts in the area of standardisation and intelligence at the Edge can be found in the recently published whitepapers 'Recommendations on research priorities and innovation strategies to standardization', as well as 'A Vision on Smart, Decentralised Edge Computing Research Directions', both published at the end of September 2021. Additionally, a map of the open source ecosystem is presented in the EU-IoT deliverable 'The Internet-of-Things Open Source Ecosystem in 2021', released at the end of September 2021.

Some of the key applications which will be supported by advancing intelligence on the Edge are:

- The Internet of Autonomous Things - embodied intelligence in functionally rich machines (e.g. robots, vehicles) able to perceive and interpret the environment and to act and collaborate autonomously "like humans" in an industrial IoT context.
- Cobots.
- Swarm computing.
- Real-time control loops that can be activated for emergency situations.
- Adaptive sampling techniques that allow different sampling frequencies and data analytics requirements under different contextual situations.
- Devices benefitting from collaborative intelligence and lower computing power.

Bringing intelligence to the Edge is expected to have most impact in the following verticals:

- Manufacturing
- Industrial IoT
- Smart cities
- Smart living
- Smart mobility / transport
- Smart agriculture
- Smart logistics
- Mobility, autonomous vehicles
- Applications in remote or disconnected locations
- Smart buildings, smart critical infrastructure, water management, energy, smart grids
- Healthcare / pharmaceuticals.

Key considerations

Several conditions need to be fulfilled to successfully add intelligence on edge devices:

- More advances in Edge AI learning. When considering federated learning, the types of models need to be considered, not just the analysis of the data itself. A suggested solution to the challenges of implementing AI practically in building solutions is developing no or low-code

models, and making the ML selection and data normalisation process more automatic and visual. This is a key step in order to move away from pilot purgatory and scale-up existing models for intelligence on the Edge.

- A flexible, open and simplified foundation for distributed intelligence at the Edge. The landscape of Edge computing is highly complex, with many available technologies and legacy investments and varying levels of skills required. Choosing a distribution to be used for adding intelligence on the Edge is an evolving and ongoing process. The EVE-OS project of the LF Edge foundation offers a good example⁹.
- The emergence of a marketplace to distribute AI models or use them in as-a-service fashion. This is to be complemented by an evolution of viable IoT business models aimed at commercialisation activities to accommodate the evolution of intelligence on Edge IoT devices, such as the need for an open market to enable innovation by Start-ups and SMEs, filling customer demands, and de-personalising the needs of users.
- Supporting the processing power needed for intelligence on the Edge on the hardware side through ultra-low power computing platforms.
- Synchronising data as required for the next-generation machine learning models and across sectors. This is contingent on efficient communication between devices. Semantic validation will be required to make data analysis efficient and reduce uncertainty, while contributing to automating future engineering processes.
- More efficient, ultra-fast and resilient communication through stronger networking power, by deploying infrastructure such as 5G/6G.
- Ensuring privacy by adding a certain level of encryption will be necessary when applying intelligence on the edge. A privacy-friendly solution to data aggregation and analysis is homomorphic encryption of data, a method of securing data where computing can be done automatically without the access to the secret key. Also, stricter requirements for device authentication and authorization techniques, considering quantum resilience, will ensure higher protection against the -expected high-volume- data breaches.
- Ensuring security against malicious attacks in IoT systems will be critical, as ever-more sophisticated attackers are arising. AI-based IDS systems and anomaly detection techniques will be needed to predict or early-identify potential attacks and minimize their impact on IoT networks
- Data integrity and asset sharing will be critical in supporting payment exchanges in the IoT systems. Immutable persistence of transactions across distributed ledgers, possibly combined with self-sovereign identities to support privacy-preserving identification format for things will be needed to ensure the security of transactions across IoT platforms.
- A specific regulatory framework for autonomously active machines, addressing both technical and economic aspects.
- In terms of the use cases, there is a need for research and development aimed at practical, real-world applications of intelligence at the Edge to develop the use cases of technology.

The success of intelligence at the Edge requires multi-disciplinarity, specifically more targeted collaboration between IoT devices, machine learning developers, hardware, systems, networking solutions as well as social networks.

⁹ EVE project, LF Edge (2020), <https://www.lfedge.org/projects/eve/>

From Europe to the world

The combination of AI with “physical things” (machines) for aims beyond analysing personal data, particularly those deployed as Edge devices is a strength for Europe as “thing makers”.

Europe is in an advanced position in the roll-out and adoption of intelligence at the Edge, but there is still work to be done to improve computer science research in this area. We are behind other locations in the area of Edge AI technologies and their application in real world verticals, as well as on the development and deployment of Edge computing platforms.

Europe presents a united view on several themes on IoT such as privacy or infrastructure deployment. A social behaviour change to come will impact the IoT landscape overall, by bringing the data source closer to humans. Considering this, Europe may be a good place to deploy and experiment with new IoT intelligence-at-the-Edge solutions. The EU has shown industrial leadership in areas such as manufacturing, Industry 4.0 and 5.0.

Area 4

Infrastructure

Technologies

- 5G/6G, and the new applications that will be made possible with the low latency these new networks will bring.
- Massive machine-type-communications (MMTC), allowing many devices that intermittently transmit small amounts of traffic.
- Low-Earth Orbit (LEO) picosats, miniaturising satellites to reduce cost to launch, can be used to create constellations for low data rate communications, using formations to gather data from multiple points.
- Network Functions Virtualisation (NFV), running network services such as router, firewalls and load balancers virtually, without specific hardware; multiple functions can be run on a single server, saving space, power, cost.
- Time Sensitive Networking (TSN), as a wired, secure, reliable, IoT-oriented specification opening many possibilities in the Industrial IoT scenario.
- Software-Defined Networking (SDN), enabling simpler and cost-efficient management of network resources.
- Scalable deployment and management technologies for secure automated management and deployment of IoT applications.
- Network Slicing – allowing to provide separated networks for different customers and applications on the same physical infrastructure.

Market

- Autonomous AI, allowing the operations of unsupervised intelligence on the network for efficient decision-making.
- Industrial IoT, deploying IoT infrastructures to realise the vision of the Factory of the Future.
- IoT in infrastructure domains like Smart Grid, Smart City
- Distributed manufacturing, decentralising production to several locations, coordinated with next-generation networks.
- Digitalized supply chains, logistics, networked ecosystems.

Policy and Standards

- Open standards, allowing for the collaborative and efficient development of architectures for the Next Generation Internet.
- Security, ensuring the infrastructure and communication endpoints are safe and therefore trustworthy.
- Energy efficiency, reducing the level of power use for sustainability.

Skills

- Next generation protocols, making users and operators familiar with the mode of operation of novel devices.
- Secure chains, embedding trust at all nodes of the network through informed operators.

Trends and Future directions

The infrastructure for the NGIoT is expected to evolve with the deployment of privacy-preserving architectures, decentralised storage, cloud environments and Edge computing. New infrastructures are expected to bring more trust in data usage, with one enabling technology being private Edges. IPv6 link-local addresses are an interesting application in developing private Edges, by using scrambled MAC addresses.

Novel communication technology such as 5G including private 5G networks will be key to support the infrastructure of the NGIoT. This needs to be approached from a user or subject perspective, rather than the operator side as has been the case. The automation of M2M communication, as well as P2P is to optimise the NGIoT communication infrastructure.

Wireless communication infrastructures are expected to be deployed in control loops, resulting in privacy-aware infrastructures with a more efficient energy use.

These infrastructures are to be supported by network architectures that enable data democratisation, to solve specific problems in IoT. These new architectures will adapt and integrate several aspects of existing networks such as information-centric networking, security, naming and in-network caching. These improvements will lead to further reduction in latency across all layers.

In terms of optimising energy use of IoT devices, 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) devices. The integration of these new devices 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.

These next-generation infrastructures will bring along the possibility to explore new business models and applications derived from cooperative sensing.

The sectors where novel infrastructures for IoT will have most impact are:

- Industrial IoT
- Safety-critical IoT, public safety control
- Autonomous vehicles (cars, trucks, UAVs)
- Consumer IoT devices
- Personal data usage and processing
- Manufacturing

- Healthcare
- Smart cities
- Agriculture

Home automation is seen as a lesser priority sector.

Key considerations

It will be essential to reduce the complexity of operations and maintenance of the network architecture for the NGLoT initiative to succeed. Future applications should be then developed on top of this architecture with the help of easy-to-use platforms. Applications should be integrated into the infrastructure, by focusing on the networking architecture and semantics.

- Connected to this, applications need to be built on top of decentralised architectures, fostering interoperability. A range of innovative platforms that developers can build applications on top of and experiment with are suggested, including: IPFS¹⁰, FileCoin¹¹ and Ethereum¹². Considering the volatility of cryptocurrencies, it is recommended that a more protective framework should be developed, integrated into the infrastructure within which it will be eventually deployed.
- Currently, the strong presence of large tech conglomerates is in some respects hindering evolution and progress for NGLoT infrastructure. There is a need for decentralisation, in order to support key management needs and ensure end-to-end security on both the Edge and cloud levels.
- The user interaction aspect needs to be also developed, with attractive UIs for a good experience. An important piece of the puzzle is creating applications that are searchable by their content, through Information Centric Networking (ICN), rather than location, as the web is currently built. Without larger-scale support, ICN will not reach a large-scale success.

Access technologies are important but not key to IoT. Technologies to assist interoperability such as 5G will be essential.

When considering the evolution of low-energy devices, there is a robustness/latency trade-off to be considered. Solutions with robust latency and low energy use will be required in order to improve infrastructures.

Programmable networks are an interesting area of development, but more feedback is needed in order to successfully integrate computation and networking to a desired level.

This will require IoT developers to think creatively in terms of IoT use, considering solutions to address extensive and potentially costly privacy and security concerns. Novel infrastructures will need to address the concerns of users by bringing confidentiality to data. One approach is to hide IoT devices from the wider Internet, deploying them in private networks. Open IoT solutions that whole communities can use, ensuring sovereignty and not just in terms of data spaces.

An improvement in standards, considering the whole ecosystem is a prerequisite for interoperability and should therefore be actively driven.

A key area of focus of IoT projects should be the development of business models for the solutions developed. Currently, there is a significant focus on use case implementation during projects, which

¹⁰ <https://ipfs.io/>

¹¹ <https://filecoin.io/>

¹² <https://ethereum.org/en/>

is not followed through after the project end, leading to a lack of sustainable results.

A culture change is required, taking more risks and allowing for failure in order to learn, as well as more focus on engineering the new IoT applications rather than marketing them.

From Europe to the world

Europe is in a good position on decentralised technologies, although more efforts in this direction are needed, in Edge computing, as well as in active use and improvement of privacy-enabling technology and decentralised storage.

Fundamental research is a key strength in Europe. However, a better connection between entrepreneurship and research should be developed, where projects are valued and supported to develop commercially successful products – more accelerators and incubators are needed.

All large European players should be involved in the NGIoT, and SMEs should also be supported. GAIA-X is a good example of collaboration between different actors within the cloud regulation space, and the NGIoT should align with GAIA-X on their activities and learn from their experience. The TransContinuum Initiative offers another model of successful collaboration between European players and can provide a similar level of coordination within the IoT space. Whilst Europe has an edge in IoT applications in areas such as automotive, manufacturing, privacy and sustainability, there is more work to be done to improve future competitiveness. This could be done by supporting collective projects involving industry in areas such as aeronautics or space, but they need to be results and application-focused. This will lead to the development of specific European IoT infrastructure products, which is an area that China is currently leading.

Europe should increase its involvement in open-source efforts and standardisation, taking advantage of community networks across countries such as The Things Network¹³ (TTN). FIWARE provides a good example of creating an Open Source ecosystem, and they are also working to drive the creation of standards in multiple domains:

- ETSI Standard NGSi-LD.
- CEF Building Block Context Broker.
- Standard GitHub Data models¹⁴.

¹³ <https://www.thethingsnetwork.org/>

¹⁴ <https://github.com/smart-data-models>

Area 5

Data Spaces

Technologies

- Relevant technical building blocks for data interoperability (data models and formats, data exchange APIs and data provenance and traceability), data sovereignty and trust (identity management, access and usage control policies, trusted exchange), data value creation (metadata and discovery protocol, data usage accounting and publication and marketplace services)
- High-performance computing (HPC), aggregating computers into larger units to allow for more powerful processing.
- Distributed ledgers and inter-ledger solutions, consensually shared and synchronised databases across multiple sites and locations.
- Federation, understood as the technological capacity of widespread devices to work together towards a specific aim.
- Self-sovereign identities, proving unique identifier of an entity along with several claims or attributes
- Decentralised identity management, affording data subjects sovereignty over their personal information, through the use of digital wallets (see ID Union¹⁵ for a good example)
- Knowledge Graphs to represent and understand hyperdata in a unified, searchable graph within a data space through methods such as Linked Data.

Market

- Federated services, collecting services together into a centrally managed larger service domain.
- Cloud/data market, creating a marketplace for the data and making the most of this.
- Other business building blocks for data spaces: operational service level agreements, data accounting schemes, billing and charging schemes and smart contracts.
- Decentralising renewable energy production, managed through a smart grid system, based on interoperable data.

Policy and Standards

- An architecture for data spaces which can enable data sharing empowerment, trustworthiness, publication, economy and interoperability, as well as supporting the data space community and engineering flexibility.
- Data portability interoperability and allowing users control, as well as the ability to delete the data that operators hold on them, through domain data standards.
- Operational data space building blocks for trust: unique identifiers, authorisation registries and setting up trusted parties.

¹⁵ <https://idunion.org/?lang=en>

- Data space administration, organisation and guidance building blocks: data space boards, overarching cooperation agreements, continuity models and specific regulations for each data space.
- Strategic autonomy, ensuring that NGLoT is designed with European principles. Particularly, assuring data sovereignty for Europe, ensuring data stays in the location where it is generated, or that the generator has full control over it.
- Accountability, ensuring the data operators are answerable for their processing activities to subjects.
- Citizen Science is a key tool for Community Building, and will likely gain more importance during the coming years in the context of open research and development of platforms for the NGLoT with the view to bringing new actors to the table.
- Relevant regulations for the design and development of data spaces include GDPR, eIDAS, PSD2, Context Broker and EBSI.
- Standardised Ontologies, based on a unified set of principles governing data spaces.

Skills

- Federated data management, connecting databases for multiple storage into a composite virtual database.
- Industrial data spaces, combining data across value chains and the industry sector to create a shared ecosystem.

Trends and Future directions

Currently, large amounts of data are generated by IoT devices in a decentralised fashion, without any central control, which makes the enforcement of standards difficult. There is a clear need for IoT devices to provide a benefit for the end-users, be they policy makers or companies, by first organising this into data spaces, and then generating insights from the data collected in order to bring clear benefits.

The concept of 'data spaces' is the central focus of the European Data strategy, and refers to data integration based on distributed data stores, interconnected on a need basis. Effectively, a data space is a federated data ecosystem within a given application domain, based on specific policies and rules. Users can share data here within a secure, transparent, trusted, easy and unified manner. The Commission defines nine initial domains for data spaces: manufacturing, Green Deal, mobility, health, financial, energy, agriculture, public administration and skills.

Data spaces are designed along four principles:

- Data sovereignty – giving data subjects exclusive self-determination rights in relation to economic data goods.
- Data level playing field – removing barriers to entry for new players in a data space and empowering users to move frictionlessly between data providers.
- Decentralised soft infrastructure – organising data spaces as a collection of interoperable implementation agreements supported by functional, technical, operational, legal and economic agreements.
- Public – private governance – including and engaging all relevant players in the ecosystem: users, providers, technology partners and professionals.

For more details on the principles of data space and how to bring them into reality in practice, see the recently published position paper from Open DEI¹⁶.

The evolution of data spaces will be supported by the development of data pre-learning and preparation methods, to improve the functionality of AI through data. This could lead to semi or fully automated data enrichment and integration, and a higher degree of interoperability.

The next frontier for the adoption of IoT is in research infrastructures, for remote distributed sensing, particularly for environmental work. Over 20 pan-European infrastructures are already active in this domain. IoT has significant potential to increase the time productivity of research communities in Europe and bring further benefits by then making research data and information available to policy makers. There is also a good opportunity for data spaces to improve the mobility model of citizen commuting patterns. This will support the preservation and sustaining of key infrastructure.

The areas where new modes for data will have the highest impact are:

- Agriculture
- Energy
- Finance
- Geoinformation
- Health
- Industry 4.0 and SMEs
- Mobility
- Public sector
- Smart cities and region
- Smart living

The emergence of personal data spaces in these verticals and beyond will certainly bring significant societal benefits through informed decision making.

Key considerations

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, the development and integration of more automation is required. It will be key to automatically integrate data sets from individual sensors, for full cloud-based data analytics, as well as for in-situ processing.

Semantical compatibility of data sets from different devices is a key prerequisite in order to allow for processing in private clouds. 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. Analytics should be deployed on top of this, to support the organisation, curation and integration of data sets.

With this, a careful balance between data protection needs and the practicability of data sharing and integration will be necessary. Specifically, different types of data will require different standards to handle, to increase interoperability. Currently, it is not clear who holds the responsibility for data set maintenance after a project ends, who hosts and keeps the data sets up to date. Perhaps this

¹⁶ *Design principles for data spaces, (2021), Open DEI*

responsibility should fall with the research community that generated it but currently it is not clearly defined.

EU projects often lack usable standards (good open source) for coordination with Standard Development Organisations. It is recommended to connect projects with SDOs.

Data sovereignty is a key European principle, essential for achieving our goal of strategic autonomy. In order to achieve this, standards for the management of both personal (GDPR) and non-personal data are paramount. The International Data Spaces Association standards provide a good approach of regulation protecting privacy especially when sharing data. These standards will need to be implemented for data storage and analytics in IoT and Edge devices. Concomitantly, citizens should be made more aware of the need of sharing and using data, as well as of existing privacy rules.

More focus is needed on developing open source results which can generate tangible outcomes. Strong IoT applications are needed, like generating specific insights for significant benefits. EU projects often have toy use cases, where too much time is spent on agreeing on data standards and/or models to be used.

Projects and research need more investment in the technical developments, and in ensuring that the research results become market-ready. A key part of this will be more partnering between research and industry.

Connected to this is the development of data-driven business models, combining the ownership of data with the right business knowledge for success. An upcoming relevant trend is the proliferation of models focused on data monetisation¹⁷. As the market matures, organisations are starting to leverage IoT data to support new digital business models or products. The COVID-19 pandemic has been a major impetus of this change, with organisations looking to build resiliency through their digital initiatives. IoT platforms are the core of the strategy, sitting at the heart of the ability to collect, analyse and eventually monetise data. Leveraging IoT data can help business models move from a product to a service-oriented business.

The need for better business models around data is particularly pressing for research infrastructure, in order to boost the innovation and adoption of solutions developed there. More use case partners are needed to test these business models. These will turn data spaces into a structured business, combining all the data available for market use. For example, Amazon is taking advantage of Landsat satellite data with the support of Sinergise, a Slovenian SME, for the organisation of the data into an easily analysable model.

Further information on novel business models in IoT is collected from practitioners in the EU-IoT deliverable 'Report on best practices for use cases Version 1', released at the end of September 2021.

The European Open Science Cloud (EOSC) is a centralised European large infrastructure that is working to support and develop open science and open innovation in Europe and beyond. It provides a virtual environment where European researchers can store, manage, analyse and re-use data for research, innovation and educational purposes. Whilst currently in its incipient phases and exploring the initial roadmap, efforts are already underway to set up business models and bring its results to market.

Regulations ensuring project exploitation and sustainability are also needed. Recent analysis showed that of the 12 funded projects in the German framework programme 'Smart Service World', eight had a work package dedicated to creating a data platform for the services developed¹⁸. All projects had the ambition to develop a sustainable platform, and all failed in this attempt. A better strategy would be to reuse existing data platforms and technologies and to focus more on the development of the

¹⁷ Top 5 Trends for IoT Platform and Analytics in 2021, Stacy Crook, IDC

¹⁸ Smart Data Economy: New study presents data sharing platforms for organizations, https://www.digitale-technologien.de/DT/Redaktion/EN/Downloads/Publikation/smartdata_%20Datasharing.html

services on top of the platform. It is recommended that calls for projects reflect these findings.

There is also a need to invest in people and their skills, particularly in the IoT space within research communities.

From Europe to the world

The current attitude and rules around data protection in Europe are strong, having defined a clear data ownership model. Several relevant regulations have been recently released, including but not limited to GDPR, the regulation on the free flow of non-personal data (enabling free movement of non personal data between different EU countries and IT systems in Europe), Regulation of online platforms, the Data Governance Act, or the Data Protection Law Enforcement Directive.

The stringent European regulatory climate 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. Still, ensuring that regulation is IoT-friendly and application-specific is a must for the future.

GAIA-X is paving the way for developing the next generation of federated and secure data infrastructure, based on European principles, to create an open, transparent and secure digital ecosystem. Through this initiative, Europe pioneers in data sharing across six verticals (industry 4.0, health, energy, mobility, finance and insurance and space), leveraging on data sovereignty and trust, as well as on cloud/edge cloud infrastructures.

The International Data Spaces Association (IDSA) is carrying out key work to bring the European Commission's vision of international data spaces grounded in the values of trust and self-determination of data usage by data providers, leading to data sovereignty. IDSA have specifically defined a framework for a reference architecture model, IDS-RAMI, used as a key element to integrate the data spaces concept in the overall EU data strategy.

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.

However, we are behind with deployment, Asia is leading in this space as the regulation is more permissive there. In Europe, the focus has been on protection and avoiding data misuse, but it is now necessary to look at how to merge and exchange data in meaningful ways.

In order to succeed in deploying effective data spaces, the Open DEI position paper³⁹ calls for a public-private partnership, starting with a convergence phase, where all the existing European initiatives (IDSA, BDVA/DAIRO, FIWARE, GAIA-X, etc.) bring together their efforts into creating the soft infrastructure required. This step is expected to take two to three years, and will consist of the co-creation of a set of agreements for the soft infrastructure, the establishment of a governance structure and creating awareness of this infrastructure in the ecosystem. This is to be followed by deployment, ensuring the governance of the daily data space operations and processes, maintaining and also innovating with each data space, offering implementation support to speed up adoption and continuing to raise the awareness and educate the participants on how to make the most of the data spaces. In parallel with the convergence and deployment, three other continuous activities will be carried out: standardisation, experimentation and awareness.



MAPPING R&I ACROSS NGIoT

The following section outlines some of the key areas of interest for research and innovation within the NGLoT. The mapping demonstrates the active fields within the five main contexts from the technologies being explored and developed to the market applications and the standards being progressed.

Technology priorities



Figure 7: Technology priorities in the NGLoT landscape

Key areas of focus in the technology aspect of the NGLoT include:

- Interfaces mixing the virtual and digital world (AR, VR, MR) to improve sensing, for example offering safety managers a full, continuous view over their assets.
- Automated co-bots assisting humans for routine tasks such as industrial robotic arms in Factory of the Future settings.
- Devices to power intelligence on the far edge, such as accelerators, allowing for in-situ processing for example to assist sustainability in autonomous driving and automated monitoring of assets in the field.
- Novel secure-by-default hardware and software architectures for devices and their system software that are more resilient against attacks.
- End-to-end identifiability and integrity reporting between edge devices and cloud using Remote Attestation anchored in integrated Root-of-Trust.
- Digital twins on the near edge, empowered through federated architectures, allowing for efficient and active smart grid monitoring, upfront testing and simulations and more.
- Time-sensitive networks, assisted by the required latency through 5G communications, allowing for optimal resource allocation and network orchestration. This can allow for intermodal asset tracking in sea transportation, by empowering low-power, wide-area networks and satellites.

- Distributed ledgers improve traceability and trust, for example in custom manufacturing to record all the steps in production accurately.
- Augmented humanity - the convergence of technology and humanity, bringing together technologies such as augmented/virtual reality (AR/VR), wearables, and brain-computer interfaces (BCI) — to transform human senses, capabilities, perceptions and insights.

Market priorities

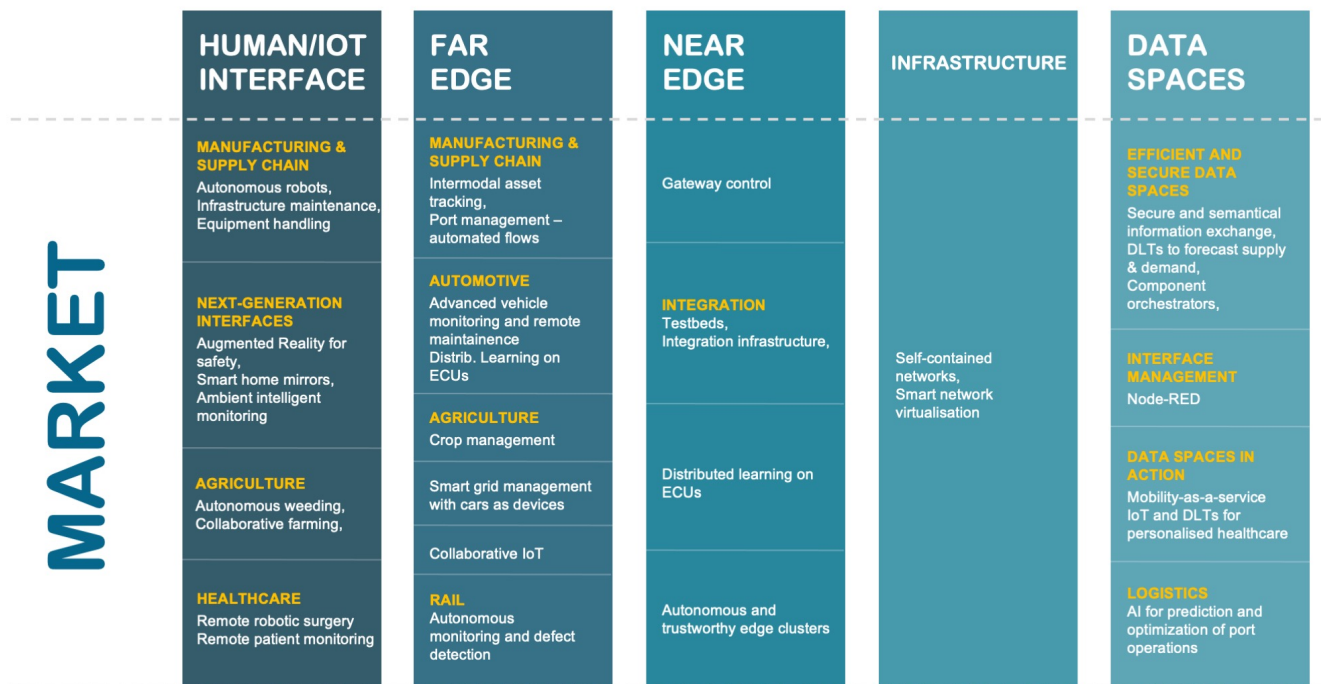


Figure 8: Market applications priorities in the NGIoT initiative

In the following, we refer to methods to identify applications, services, and models enabled by the technologies (both individual and varied combinations of technologies). Some of the highlights of the market applications within the NGIoT include:

- Automating the supply chain at every step, from VR interfaces for managers to visualise shipping container handling, factory maintenance with low-power deep learning enabled devices to actively monitor the condition of installations such as power switches or integrating the whole chain into a smart ecosystem using distributed ledgers to ensure secure and semantical exchange of data.
- Supporting smart agriculture by allowing farmers a real-time view of their assets for grazing or crop management with Edge devices and AR-assisted visualisation, autonomous e-tractors supported by collaborative intelligence and drones, and AI models for crop disease prediction.
- Supporting surgery via AR interfaces, remote patient monitoring or intelligent robot arms, as well as data spaces deployed to coordinate hospital infrastructure and patient personal data.
- Next-generation mobility, supporting co-commuting, traffic flow prediction, crowd management as well as driver-friendly dispatchable EV charging, with the aim of supporting proactive grid management via AI.
- Cohesive vehicle monitoring and diagnosis for sustainability and efficiency using intelligent, open (Linux-based) electronic control units (ECUs).

- Ultra low-power sensors with local anomaly detection and defect reporting for monitoring safety-critical parts of vehicles to lower maintenance costs by widening fixed inspection intervals.

All of this is complemented by new business models which are leveraging data flows from IoT in the cloud-edge mixed context.

Policy and standards priorities



Figure 9: Key policy and standard considerations for NGIoT applications

The advent of the NGIoT brings along several policy considerations, standards must support:

- Human-in-the-loop policies – when is control handed back to human operators when using autonomous devices for instance? This is particularly relevant for all safety applications.
- Connected to this, where does the liability lie in the unfortunate case of accidents – the device manufacturer, the operator, the model developer?
- The need to embed privacy, trust and security by design into IoT devices. This will likely require an adaptation of the architecture to a vertically agnostic standard, with approaches building from previous work such as the CREATE-IoT 3D architecture which evolved into a DevSecOps methodology. Combined with this, novel encryption methods such as Software Guard Extension for remote attestation are showing promise.
- The use of common, open-source solutions (p4, Python) to enable interfaces, ECUs of cars and AR enablers based on open OS platforms, Management and Orchestration (MANO) frameworks for network function virtualisation (NFV).
- Using meta-AI models to monitor models from a central location, to avoid model pollution, be it by a malicious actor or by operator mistake, with a sentinel and honey pot approach, as well as intra-DLTs to communicate between blockchain at different nodes in a federation of models to record if data is being tampered with.

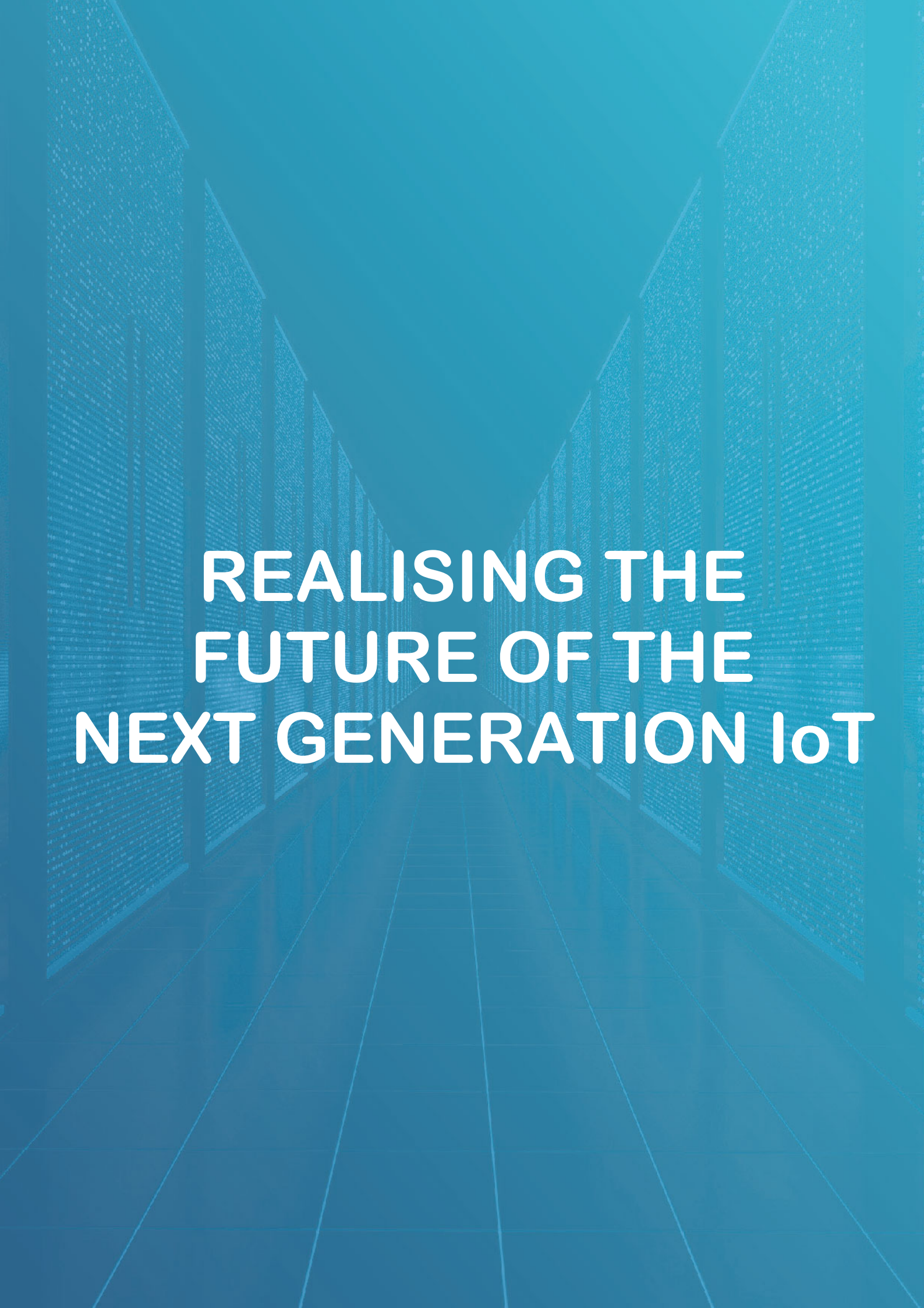
- Network policies taking advantage of the low latency of 5/6G for real-time decision making through automated M2M communications to share uplink spectrum where underutilised.
- Enhanced cellular IoT communication technologies, driven by 3GPP standardization body, to provide efficient, reliable and secure solutions for ubiquitous connectivity of IoT devices while enabling new emerging IoT use cases and applications by fully addressing their highly demanding requirements.

Skills priorities

The emergence of this new stack of technologies, as well as the accompanying applications and policies, requires all actors to upskill to successfully operate them. Several approaches are suggested for the development of skills, included but not limited to:

- Training courses and modules for PhD candidates.
- Workshops for upskilling/reskilling of workers in factories and across the supply chain.
- Hackathons to support solution developers.
- Advisory services to adopting the technology developed as part of projects.
- Events centered around knowledge sharing and lessons learned between the ICT-56 projects, as well as with other European initiatives.
- Certifying training indicating their relevance to the NGLoT ecosystem.

For many of the experts and actors within the NGLoT ecosystem, while they recognise the importance and the challenge that the new skills demands and their combinations will pose for adoption and ultimate value generation, they struggle to articulate or refine what the NGLoT professionals and profiles of the future will be. EU-IoT will be addressing this shortcoming over the coming months through its EU-IoT COACH activities which will seek to create skills profiles and learning pathways to support the upskilling that will be required because of the tech development.



REALISING THE FUTURE OF THE NEXT GENERATION IoT

The previous sections of this document have provided knowledge, data and opinions from a variety of voices and activities within the NGLoT ecosystem; each of these provides a vector for the direction of the future of IoT as it transforms based on the current momentum. Taking a viewpoint on the pillars that will define the NGLoT over the coming 3-5 years, we present a set of conclusions and visions from the EU-IoT Consortium below.

A point of convergence and collaboration – the future of the human-cloud continuum.

As with evolving IoT architectures, for the NGLoT the integration is no longer just vertical but horizontal and the solutions to be developed on these novel technologies will span the human-cloud continuum. The combination and cross-over between the previously clearly defined and in some cases delineated technological domains is shaping the ecosystem of players surrounding these areas. The interplay is already being observed as tech developers strike out from their disciplines to form collaborative teams and nuclei around a specific application. This is also being reflected at a higher-level with the evolution of key European ecosystems, the growth and relevance of GAIA-X which is bridging the gaps being created by current and new operational modes, the broadening of BDVA's mandate beyond big data into DAIR0, and the formation of partnerships such as the TransContinuum Initiative, the Smart Networks and Services Joint Undertaking and the formation of the European Alliance for Industrial Data, Edge and Cloud.

The future of the NGLoT is going to require a massive shift in approach, reintegrating the hardware and semiconductor community away from a commodity provider and back into a development partner together with cloud/edge providers and AI developers. The NGLoT initiative will help connect these heterogeneous communities, providing the foundation of the future collaborative and integrated ecosystem (a network of networks) stretching from the cloud to the device and end users.

Intelligence across the board from TinyML to HPC for AI in the Cloud

The on-going shift in terms of data processing from the cloud to the edge will unlock the innovation potential of a host of cloud/edge intelligent technologies. Data driven intelligence based on the increasing deployment of AI techniques (machine learning, swarm intelligence, etc.) will not necessarily reside in the cloud. It will be shifted towards the edge of the network, leading to several benefits, in terms of energy efficiency, low-latency and privacy preservation. In this direction, a host of edge artificial intelligence models are emerging, such as:

- **Federated Machine Learning approaches**, which train machine learning models on local datasets, build local models and then combine them into more accurate cloud models. Such approaches are much more power efficient than executing AI in the cloud.
- **Embedded Machine Learning approaches**, which execute machine learning models within embedded IoT devices. This reduces data transfers and I/O operations and leads to minimal CO2 emissions. It also enables low-latency, real-time operations, as required for various industrial use cases. The benefits of embedded machine learning can be pushed to their extreme, based on the TinyML paradigm that deployed machine learning (including deep learning) applications on microcontrollers.
- **Approaches for “learning with small data” such as Transfer Learning** i.e. paradigms that can be trained on smaller datasets, which leads to less CO2 emissions and reduces training times.

The above listed paradigms are already deployed and validated in some ICT-56 projects that are at work to demonstrate and gauge the sustainability and performance benefits of decentralised intelligence paradigms in a variety of cloud/edge computing settings. In the convergence to such a

continuum computing, the challenge is to identify what is the best technological combination/solution in relation to the specific business needs. In several cases, IoT analytics must be executed on the cloud to benefit from the collection, management and availability of large numbers of data points (i.e., Big Data), but also from access to HPC (High Performance Computing) resources (including the emerging Quantum Computers). With so many different options at hand, application developers, application integrators and infrastructure providers (i.e., cloud service providers, telecom providers) must manage resources and services in a very heterogeneous landscape. Tools and techniques that select the optimal deployment paradigms in this diverse continuum are therefore required.

Towards Interoperability: the role of Open-source and Open Standards

The IoT European landscape is being built on multiple open-source platforms [13] and also being supported by a large number of IoT consortia and fora [14]. These efforts, albeit fragmented, are essential to provide IoT with the much needed interoperability and scalability. Successful examples of IoT platforms have given rise to new IoT services, as corroborated by FIWARE in the Smart Cities domain, or by solutions based on Eclipse IoT.

With the further expansion of AIoT across different domains, open-source solutions are becoming increasingly relevant as they are the basis for the development of both Far Edge services, and the basis for the service decentralisation that is today one of the cornerstones of the Cloud-Edge continuum. Open-source is also highly relevant to assist the much required upgrading of IoT skills, in particular having in mind the development of Edge-based services in traditional European competitiveness domains, e.g., manufacturing, agriculture. Open-source brings multiple benefits to the IoT ecosystem, e.g., improved interoperability from the far Edge to data spaces; commercialization benefits due to the varied and flexible open-source licenses; sustainability, due to the possibility of renewal (reinvention). However, it also requires an investment in terms of skills training and a solid methodological approach to support a fast cycle of development and an adequate time-to-market.

Moreover, both open-source and open standards are highly relevant aspects to ensure a smooth development of an IoT/Edge ecosystem. Specific actions towards openness are already being realized by different SDOs, e.g., IEEE, IETF and also by different consortia and associations, e.g., BDVA. Moreover, industry is driving multiple efforts [14] in regards to the development of open platforms that can boost a solid and end-to-end IoT development. Still, in addition to the technical challenges and to the need to reduce fragmentation and assist in the development of skills as well as in increasing awareness to the high number of relevant IoT open-source platforms [13], an aspect that needs further addressing is the development of guidelines that can support openness from an end-to-end perspective, addressing both software and hardware aspects, ranging from interfaces to infrastructure and considering data spaces as well. This can be facilitated by working together with SDOs, having in mind the development of different models of open standards. For instance, open standards may address open specifications to allow for interconnection and interoperability while at the same time providing a value-add to develop proprietary business models; open standards may also be offered with a Minimal Viable Product (MVP) approach, to increase the interoperability across proprietary solutions.

Global initiatives to assist in developing further interoperability having in mind next generation IoT and people-centric services (Far Edge services) are much needed. While there are already some initiatives in this context being driven by SDOs (e.g., IEEE P2413, working together with IIC, etc.), service decentralisation and the further miniaturization of AI on the far Edge introduce additional problems which need to be addressed by considering an interdisciplinary methodology involving relevant consortia and fora as well as SDOs across different domains, and considering, in addition to a cross-layer technical approach, aspects such as specific domain legislation (which may undermine technical approaches in different domains); ethics and trustworthiness aspects (related with the further support of decentralisation and self-organising behaviour across Edge-Cloud).

While there are multiple efforts towards openness in IoT, the cooperation efforts in Europe are still quite fragmented. There is the need to invest in the development of an open IoT ecosystem covering an end-to-end perspective; addressing ways for IoT products to work independently of a specific platform, allowing consumers direct and secure access to IoT across different domains. This requires interoperable and open standards covering the full IoT end-to-end spectrum, from the Far Edge towards data spaces, considering hardware, software, Edge-Cloud applications and: accessible, open data sets (which requires an automated support to convert and validate proprietary data sets into open formats).

A value chain led transition towards edge solutions

The main trend for IoT is still heavy centralisation and use of cloud computing solutions¹⁹ with the aim of controlling and managing data efficiently and effectively. However, the edge computing market size is expected to grow from USD 36.5 billion in 2021 to USD 87.3 billion by 2026, at a Compound Annual Growth Rate (CAGR) of 19.0% during 2021-2026²⁰.

Using centralised solutions, benefits are clearer and transferable to other digital technologies, specifically IoT and other data intensive systems.

The questions that are unanswered with respect to moving further towards the edge and far edge reverberate around the ability to replicate business requirements such as security or data analytics capabilities with the same fidelity.

Still, we can see success cases emerging that present edge computing benefits. There are two reasonable scenarios emerging as alternatives to cloud-based solutions. (1) presently cloud based systems are scaled to edge nodes to offer hybrid solutions that span the cloud continuum. (2) A truly edge-based solution emerges to challenge centralisation.

For Edge-based solutions to emerge from a value chain analysis perspective, clearer benefits need to be demonstrated by industry from such solutions. Presently the cloud market is driving the adoption of solutions, hindering edge-based adoption and rollout. There also needs to be a clearer presentation of benefits beyond cloud benefits being replicated at similar fidelities in edge architectures such as for example privacy and green computing.

The edge computing ecosystem is still emerging, and the edge is not homogenous. We see that a value chain led transition is complicated by the many players from different ecosystems coming together in edge solutions, and the often specific requirements that different use cases may have. New capabilities will be required for a value chain led transition towards edge solutions, for example orchestrating workloads across different clouds, optimising networks for this distributed architecture and developing applications that benefit from edge computing.

A shifting landscape for specialists, changing roles and skills?

Most research reports on the IoT markets²¹, including reports from the NGIoT community acknowledge the IoT skills shortage. This proclaimed talent gap in IoT skills is already challenging IoT

¹⁹ *Ioud Computing Trends: 2021 State of the Cloud Report*; <https://www.flexera.com/blog/cloud/cloud-computing-trends-2021-state-of-the-cloud-report/>

²⁰ *Edge Computing Market*; <https://www.marketsandmarkets.com/Market-Reports/edge-computing-market-133384090.html>

²¹ <https://www.iotworldtoday.com/2020/11/19/skill-gaps-persist-in-iot-disciplines/>

adopters and developers. However, the situation is expected to become even more challenging as a result of:

- **The on-going technology acceleration**, which expands the spectrum of IoT technical skills in novel areas like TinyML, cyber-security for IoT applications and distributed ledger technologies.
- **The dynamics of the future of work**, which introduces changes in job profiles and positions, including changes in workers' skills. For instance, a recent World Manufacturing Forum (WMF) report illustrates that the future shopfloor will require new positions and workers with new skills²².
- **The need for interdisciplinary and cross-disciplinary positions in the IoT systems landscape**, such as positions combining IoT technical skills with expertise in legal, ethical, business, and management issues, as well as social sciences and humanities (SSH) expertise.

In this context, there is a need for IoT upskilling and reskilling processes in the above-listed directions. The latter directions must be reflected in novel skills development programmes, training courses, skills profiles and learning paths that lead to the key skills that these profiles require. EU-IoT is working on providing representative examples of such skills profiles and learning paths, as well as of related training programs.

The impact for a green transition; the missing pieces

As underlined by the EU Digital Decade ambition, it is not possible to decouple digital transformation from the sustainable development of our society and economy. ICT needs to become greener and has an essential role in helping to green the environment and protecting our planet. At pan-European level, an increasing number of initiatives and stakeholders, both from the public and private sectors, are investing on developing technologies and approaches to meet the 2030 Environmental Goals, in line with the European Green Deal objectives, and as recently reiterated in several ways at the recent COP26 in Glasgow, this requires to join forces at different levels - political, societal, economic, legislative, fiscal, etc.

Within this context, increasingly, intelligent Edge/IoT-based solutions and applications are being developed and used to manage processes and resources more effectively (in buildings, in factories, in cities, etc.), to monitor the environment, to optimise resource consumption, and to minimise data transmission, which overall lead to minimise carbon emissions. As a matter of fact, while more and more data centers are powered by greener sources of energy, by shifting computation to the edge, while avoiding central computation and storage, there is a dramatic cut in data traffic and thereby in energy consumption and CO2 emissions.

EU-IoT plans to further investigate how ongoing ICT-56 projects and upcoming 3rd party projects funded via cascade funding will contribute to a green digital transition, by stimulating discussion at various levels on advanced green and "greening" intelligent Edge/IoT solutions.

²² <https://worldmanufacturing.org/wp-content/uploads/WorldManufacturingFoundation2019-Report.pdf>



NGIoT ECOSYSTEM INITIATIVES

The Alliance for Internet of Things Innovation (AIOTI)

It was established in 2015 with support from the EC to foster the creation of an innovative and industry driven European IoT ecosystem. AIOTI gathers 12 working groups focusing on several transversal and vertically focused research and innovation areas and has recently contributed to the Smart Networks and Services partnership proposal for Horizon Europe, in close collaboration with the 5G IA and Networld2020 group, recently renamed NetWorldEurope – European Technology Platform.

- AIOTI representatives have been directly consulted and engaged in various EU-IoT activities since the very beginning of the project - notice Tanya Suarez CEO of BluSpecs is member of the AIOTI Board. As background to the work presented in this deliverable is also the *Strategic Foresight Through Digital Leadership IoT and Edge Computing Convergence paper published in October 2020* [3].

Website: <https://aioti.eu>

ARTEMIS Industry Association

It is the association for actors in Embedded Intelligent Systems within Europe gathering industry, SMEs, universities, and research institutes, within the broader ECSEL Joint Undertaking context. One of its main goals is to promote the research and innovation interests of its members to the EC and the Public Authorities of the participating Member States and contributing on one coordinated, pan-European strategy towards the success of the Embedded Intelligent Systems sector in Europe, promoting EU competitiveness, innovation, global impact, and improving day-to-day life. Of direct relevance to the EU-IoT work, two recent ARTEMIS publications:

- **Strategic research and innovation agenda (SRIA) 2021** – Electronic Components and Systems [4]. The SRIA describes the major challenges, and the necessary R&D&I efforts to tackle them, in micro and nanoelectronics for smart systems integration all the way up to embedded systems and System of Systems (SoS). Among others, this document stresses the importance of ensuring European sustainability in AI, edge computing and advanced control.
- **From Internet of Things to System of Systems** - Market analysis, achievements, positioning and future vision of the ECS community on IoT and SoS [5] that highlights how embedded intelligence represents the last evolutionary step of IoT allowing organizations to transform collected data into insightful knowledge, deriving a real commercial benefit. Five major challenges have been identified:
 - Fill the lack of trust in IoT technologies with end-to-end human-centric solutions, which only partly depends on technologies and largely on policies.
 - Ensure an adequate level of interoperability. The right trade-off between confidentiality and openness, which also requires coordinated standardisation efforts.
 - Develop open IoT/SoS platforms capable to take advantage of the technology evolution in terms of ubiquity, pervasiveness, autonomy, sustainability, interoperability, etc.
 - Provide engineering support for the entire lifecycle of the IoT solutions. Engineering support allows the research results to be exploited and transformed into real products. But it also ensures the continuous engineering.
 - Define a pan European strategy to bundle forces and develop a solid IoT/SoS ecosystem, able to support the IoT value networks with EU policies, common strategies, roadmaps and joint public-private funding.

Website: <https://artemis-ia.eu>

GAIA-X

GAIA-X is a project initiated by Europe for Europe and beyond that aims to develop common requirements for a European data infrastructure. GAIA-X envisages a networked data infrastructure connecting existing decentralised data infrastructures into a homogenous data ecosystem. Its core, the so-called Federation Services, are to be created open source. So, what emerges is not a cloud, but a networked system that links many cloud services providers to ensure openness, transparency, and trust.

- As recently presented at the **NGIoT Edge and IoT Computing Strategy Forum**²³, several members of GAIA-X are working on enabling Intelligent collaboration, self-organisation, self-management, and self-healing across many and heterogeneous resources present in all kinds of IoT Edge devices, micro edge data centres, edge resources, near/far edge, private enterprise clouds, and large public Clouds.

Website: <https://www.data-infrastructure.eu/GAIA-X/Navigation/EN/Home/home.html>

Smart Networks and Services Partnership

The EC has adopted its legislative proposal for a strategic European partnership on Smart Networks and Services (SNS) as a Joint Undertaking (JU), with a public R&I investment over the new long-term budget period 2021-2027. SNS will coordinate research activities on 6G technology under Horizon Europe as well as 5G deployment initiatives under the Connecting Europe Facility (CEF) and Digital Europe programmes.

- The research and development foundation of the SNS vision and main objectives are documented in the *Strategic Research and Innovation Agenda 2021-27 - European Technology Platform NetWorld2020* [6]. Two essential aspects are:
 - Deep Edge, Terminal and IoT device integration are essential aspects for the development of system architectures able to span all types of resources, regardless of their nature (compute, networking), realization (virtual/physical) and position (remote/local), dynamically adding and removing resources as they come and go (churn). SNS architectures should cope with terminals and IoT domains, which are to be considered full-fledged resources, allowing to deploy services at the deepest possible “edge” and in the direct user vicinity.
 - Open distributed edge computing architectures and implementations for IoT and integrated IoT distributed architectures for IT/OT integration, heterogeneous wireless communication and networking in edge computing for IoT, and orchestration techniques for providing compute resources in separate islands, are key to enable efficient distributed services delivery.

Website: <https://5g-ia.eu/sns-horizon-europe>

BDVA/DAIRO The Big Data Value Association

BDVA, (from 2021, DAIRO - Data, AI and Robotics aisbl), is an industry-driven international not-for-profit organisation with more than 230 members all over Europe and a well-balanced composition of large, small, and medium-sized industries as well as research and user organisations. BDVA/DAIRO focuses on enabling the digital transformation of the economy and society through Data and Artificial Intelligence by advancing in areas such as big data and AI technologies and services, data platforms and data spaces, Industrial AI, data-driven value creation, standardisation, and skills.

²³ <https://app.swapcard.com/event/next-generation-iot-and-edge-computing-strategy-forum/>

DSBA

The Data Spaces Alliance is the first initiative of its kind, bringing together the necessary industry players to realise a data-driven future in which organisations and individuals can unlock the full value of their data. The alliance is created to drive the adoption of data spaces across Europe, bringing together data providers, users and intermediaries. Together, the Alliance's founding organisations represent 1,000+ leading key industry players, associations, research organisations, innovators, and policy-makers worldwide.

TM Forum

It is an alliance of global companies, including 10 of the world's top network and communications providers, which aims to break down technological and cultural barriers between digital service providers, technology suppliers, consultancies and systems integrators. Their membership consists of 850 companies, generating US\$2 trillion in revenue and serving five billion customers across 180 countries. They have developed an IoT reference architecture and component suites and have a library of Open APIs which are used extensively by FIWARE, Synchronicity and others in the ecosystem. These enable scalability and reuse up the architectural stack. They are also working with the ITU-T regarding making these formal standards, recommended by ITU-T.

Website: <https://www.tmforum.org/about-tm-forum>

IDS

The International Data Spaces Association is a coalition of more than 130 member companies that share a vision of a world where all companies self-determine usage rules and realize the full value of their data in secure, trusted, equal partnerships; and we are making that vision a reality. The members represent dozens of industry sectors based in 22 countries across the European Union and around the world.

Website: <https://internationaldataspaces.org>

FIWARE

Fiware is a market-ready open-source software, combining components that enable the connection to IoT with Context Information Management and Big Data services in the Cloud. Their network consists of more than 150 cities, 21 iHubs, a FIWARE Accelerator Programme, and strategic partnerships with GSMA, TM Forum, CEF, and ETSI, amongst others.

Website: <https://fiware.org>

IoT-LAB

The IoT-Lab provides a facility suitable for testing networking with small wireless sensor devices and heterogeneous communicating objects. The product has over 5,000 users globally, spread across more than 40 countries. IoT-LAB is a part of the FIT (Future Internet of the Things) platform. FIT is a set of complementary components that enable experimentation on innovative services for academic and industrial users.

Website: <https://www.iot-lab.info>

CPS4EU

The Cyber-Physical Systems for Europe aims to arm Europe with extensive value chain across key sectors by strengthening CPS Technology providers, mainly European SMEs, to increase their market share and their competitiveness to become world leaders. To achieve these goals CPS4EU will develop 4 key enabling technologies, such as computing, connectivity, sensing, and cooperative systems.

Website: <https://cps4eu.eu>

TCI

The TransContinuum Initiative is a horizontal collaboration between 8 European associations and projects involved in IT technology, application and services provisioning for the Digital Continuum: 5G IA, AIOTI, BDVA, CLAIRE, ECSO, ETP4HPC, EU-Maths-In and the HiPEAC project. The ambition of TCI is also to become a meeting place of experts representing various disciplines in both science and industry – an asset that Europe can apply in the resolution of its other challenges such as healthcare, climate change or smart cities.

Website: <https://www.etp4hpc.eu/transcontinuum-initiative.html>

The 5G IA

The 5G Industrial Association is committed to the advancement of 5G in Europe and to building global consensus on 5G. To this aim, the Association brings together a global industry community of telecoms & digital actors, such as operators, manufacturers, research institutes, universities, verticals, SMEs and ICT associations. The 5G IA carries out a wide range of activities in strategic areas including standardization, frequency spectrum, R&D projects, technology skills, collaboration with key vertical industry sectors, notably for the development of trials, and international cooperation.

Website: <https://claire-ai.org/vision>

CLAIRE

The Confederation of Laboratories for Artificial Intelligence Research in Europe CLAIRE seeks to strengthen European excellence in AI research and innovation. The network forms a pan-European Confederation of Laboratories for Artificial Intelligence Research in Europe. Its member groups and organisations are committed to working together towards realising the vision of CLAIRE: European excellence across all of AI, for all of Europe, with a human-centred focus.

Website: <https://5g-ia.eu/about>

ECSO

the European Cybersecurity Organisation federates the European Cybersecurity public and private stakeholders, including large companies, SMEs and start-ups, research centres, universities, end-users and operators of essential services, clusters and association, as well as the local, regional and national public administrations across the European Union (EU) Members States, the European Free Trade Association (EFTA) and H2020 Programme associated countries. The main goal of ECSO is to coordinate the development of the European Cybersecurity Ecosystem support the protection of European Digital Single Market, ultimately to contribute to the advancement of European digital sovereignty and strategic autonomy.

Website: <https://www.ecs-org.eu/about>

ETP4HPC

The European Technology Platform for High-Performance Computing is a private, industry-led and non-profit association. Their main mission is to promote European HPC research and innovation in order to maximise the economic and societal benefit of HPC for European science, industry and citizens. Their members have diverse profiles, from HPC technology players active in Europe to HPC users: vendors - both large industrial companies and small SMEs, academic HPC research organisations and industrial HPC users.

Website: <https://www.ecs-org.eu/about>

EU-MATHS-IN

The European Service Network of Mathematics for Industry and Innovation aims to leverage the impact of mathematics on innovations in key technologies by enhanced communication and information exchange between and among the involved stakeholders on a European level. It is a dedicated one-stop shop to coordinate and facilitate the required exchanges in the field of application-driven mathematical research and its exploitation for innovations in industry, science and society. It acts as facilitator, translator, educator and link between and among the various players and their communities in Europe.

Website: <https://www.etp4hpc.eu/who-we-are.html>

HiPEAC project

The High Performance Embedded Architecture and Compilation is a European network of almost 2,000 world-class computing systems researchers, industry representatives and students, providing a platform for cross-disciplinary research collaboration, promotes the transformation of research results into products and services, and is an incubator for the next generation of world-class computer scientists.

Website: <https://www.hipeac.net>

DAIRO

The AI, Data and Robotics Partnership partnership focuses on delivering the greatest benefit to Europe from AI, Data and Robotics, this Partnership will drive innovation, acceptance and uptake of these technologies and will boost new markets, applications and attract investment, to create technical, economic and societal value for business, citizens and the environment. BDVA, CLAIRE, ELLIS, EurAI and euRobotics are joining forces integrating a wide range of stakeholders into the activities of the Partnership so the raised ambition can be realised.

- As discussed in more details in the *Strategic Research, Innovation and Deployment Agenda AI, Data and Robotics Partnership* [7] - IoT supported by ubiquitous networks of AI-based sensors is key to leverage the full potential of a completely digitised European Industry. The seamless integration of IoT technology (such as sensor integration, field data collection, Cloud, edge and fog computing) with AI, Data and Robotics technology, is essential to enable the growth of IoT-enabled Data Marketplaces, across various vertical market sectors.

Website: <https://ai-data-robotics-partnership.eu>

AI for good

It has a main objective to drive forward technological solutions that measure and advance the UN's Sustainable Development Goals. It creates impact by bringing together a broad network of interdisciplinary researchers, non-profits, governments, and corporate actors to identify, prototype and scale solutions that engender positive change. Founded in 2015 by a team of Machine Learning and Social Science Researchers in the US and Europe, AI for Good is headquartered in Berkeley, California with an international network of core team members, partners and volunteers supporting our work.

Website: <https://ai4good.org>

AI commons

AI Commons is a non-profit organization supported by the ecosystem of AI practitioners, entrepreneurs, academia, NGOs, AI industry players and organizations/individuals focused on the common good. AI Commons was born in 2016 from the collective discussion and efforts of a group of individuals and organizations working towards promoting AI for Good and bringing the benefits of AI to everyone and using the technology towards social and economic improvement. The reflections, dialogs, and gatherings resulted in the identification and formulation of an open and collaborative efforts to maximize the dissemination of our common knowledge of AI.

Website: <https://ai-commons.org>

IoT-EPI

The European IoT Platform initiative was launched in 2016 to develop and validate innovative platform technologies and foster technology adoption through community and business-building activities around seven major Horizon 2020 RIAs (INTER-IoT, BIG IoT, AGILE, symbIoT, TagItSmart!, VICINITY and bloTope) with a total funding of €50 million. Although these projects finished, their network of consortia and third-party organisations represent an important part of the NGIoT community.

Website: <https://iot-epi.eu>

IoT-LSP

With an EU financial contribution of €100 million, The IoT European Large-Scale Pilots initiative started in January 2017, and funded five RIAs (ACTIVAGE, IoF2020, MONICA, SYNCHRONICITY, AUTOPILOT) and two CSAs (Create-IoT and U4IoT). More recent pilots active in the energy, agriculture, and health sectors include INTERCONNECT, SMART AGRIHUB, ATLAS, DEMETER, SHAPES, CARESSES, SMART-BEAR and PHAREON. By supporting the testing and experimentation of new IoT-related technologies, these pilots are expected to accelerate standards-setting across different business sectors.

Website: <https://european-iot-pilots.eu>

IoT-ESP

The IoT European Security and Privacy projects cluster launched in 2018 includes eight IoT security and privacy research projects (IoT-Crawler, CHARIOT, ENACTDevOps, SERIOT, BRAIN-IoTZ, SecureIoT, SOFIE) with an EU budget of €37 million to explore how to enhance overall security and deploy new approaches for data privacy such as Distributed Ledger Technology/Blockchains.

Website: <https://www.ngiot.eu/community/iot-esp-projects/>

ICT-56 Research and Innovation Action (RIA)

The most recent research and innovation efforts within the NGIoT initiatives, besides the EU-IoT CSA, are channelled through six ICT-56 Research and Innovation Action (RIA) projects, which started late 2020. The aim of these projects is to develop and demonstrate novel IoT concepts and solutions in line with the Next Generation Internet vision, proved through specific use cases, with the goal of better serving end-users. The six projects are:

- **ASSIST-IoT** - Architecture for Scalable, Self-, human-centric, Intelligent, Secure, and Tactile next generation IoT
- **iNGENIOUS** - Next-Generation IoT Solutions for the Universal Supply Chain
- **IntellIoT** - Intelligent, Distributed, Human-centered and Trustworthy IoT Environments
- **IoT-NGIN** - Next Generation IoT as part of Next Generation Internet
- **TERMINET** - Next Generation Smart Interconnected IoT
- **VEDLIoT** - Very Efficient Deep Learning in IoT

These projects are addressing key issues at the heart of new and advanced technologies such as decentralised architecture, low-power devices and hardware accelerators, federated and distributed intelligence, autonomous intelligence, human-in-the-loop intelligence, distributed ledger technology-enabled data management, active and proactive cybersecurity, 5G in action (smart networking, network function virtualisation, orchestrators), tactile IoT and mixed realities, explainable and trustworthy AI, Edge AI, cognitive IoT, AR and mixed realities. These technologies are deployed in several use cases, across diverse domains such as agri-food, healthcare, smart homes, energy, mobility, smart cities, industrial manufacturing (including automotive) and supply chains (ports, transportation).

The OPEN DEI CSA

Running until spring 2022, is supporting an ecosystem of 19 projects (18 are Innovation Actions, (IAs)) in the domains of Digital Platforms and Pilots. Some of them are in the IoT technological domain, others in Big Data, some in AI, and others in domain-specific communities such as the Digital Manufacturing Platform cluster. An extended ecosystem of an additional 16+ projects is reached thanks to domain-specific Working Groups (Manufacturing, Agri-food, Energy, Health and Care) and cross-domain Task Forces (Data Spaces, Platforms and Pilots, Impact and Benchmarking, Ecosystem).

Website: <https://www.opendei.eu>

The Next Generation Internet of Things (NGIoT) CSA

Finished in October 2021, has been actively involved in the engagement of the IoT-LSP projects, supporting them with community building, communication, as well as coordination of road mapping efforts. This has led to the publication of a roadmap [2] and a precedent scoping paper [3]. By focusing on the challenges and recommendations for the future Horizon Europe Programme (HEP), these documents aim to support the EC in setting priorities for the future Programme, the framework programme for research and innovation, and the Digital Europe Programme (DEP) for the implementation and deployment of digital technologies.

Website: <https://www.ngiot.eu>

IPCEI

The Important Projects of Common European Interest may represent a very important contribution to economic growth, jobs and competitiveness for the Union industry and economy. IPCEIs make it possible to bring together knowledge, expertise, financial resources and economic actors throughout the Union. The IPCEI-CIS (IPCEI on Next Generation Cloud Infrastructure and Services) will directly contribute to the implementation of the EU Data Strategy in particular to the set-up of the High Impact Project “to develop data processing infrastructures, data sharing tools, architectures and governance mechanisms for thriving data sharing and to federate energy-efficient and trustworthy cloud infrastructures and related services”.

Website: https://ec.europa.eu/competition-policy/state-aid/legislation/modernisation/ipcei_en

Digital Europe

As the leading trade association representing digitally transforming industries in Europe that stands for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. It represents over 35,000 businesses who operate and invest in Europe. It includes 91 corporations which are global leaders in their field of activity, as well as 39 national trade associations from across Europe.

Website: <https://www.digitaleurope.org>

National Digital Transformation Strategies

National Digital Transformation Strategies of Member States

SDOs

Standardisation bodies as presented in the [ngiot.eu](https://www.ngiot.eu) platform .

Website: <https://www.ngiot.eu/archive-standardisation-bodies>

REFERENCES

- [1] <https://digital-strategy.ec.europa.eu/en/library/next-generation-internet-things-and-edge-computing>
- [2] Preliminary version of Roadmap for IoT Research, Innovation and Deployment in Europe, https://www.ngiot.eu/download/ngiot-draft-roadmap-for-iot_research-innovation-deployment-in-europe/?wpdmdl=688&masterkey=5e5fdc5573311
- [3] Strategic Foresight Through Digital Leadership IoT and Edge Computing Convergence, AIOTI - IoT Research Working Group, October 2020 - <https://aioti.eu/wp-content/uploads/2020/10/IoT-and-Edge-Computing-Published.pdf>
- [4] Strategic research and innovation agenda 2021 – Electronic Components and Systems – January 2021.
- [5] From Internet of Things to System of Systems – Market analysis, positioning and future vision of the ECS community on IoT and SoS – ARTEMIS – IA <https://www.eurotech.com/en/white-papers/from-internet-of-things-to-system-of-systems>
- [6] Strategic Research and Innovation Agenda 2021-27 - European Technology Platform NetWorld2020 - <https://5g-ia.eu/sns-horizon-europe/>
- [7] Strategic Research, Innovation and Deployment Agenda AI, Data and Robotics Partnership - Third release September 2020 - <https://www.bdva.eu/DAIRO>
- [8] Building a roadmap for the Next Generation Internet. Research, innovation and implementation 2021 – 2027 <https://www.ngiot.eu/download/building-a-roadmap-for-the-next-generation-internet-research-innovation-and-implementation-2021-2027/?wpdmdl=777&masterkey=5ecd0411a3e50>
- [9] The Computer for the 21st century, Weisser, M., 1991 Scientific American, <https://www.lri.fr/~mbl/Stanford/CS477/papers/Weiser-SciAm.pdf>
- [10] Security, privacy and health, Pankati et al, 2003, IEEE Pervasive Computing - <https://ieeexplore.ieee.org/document/1186730>
- [11] 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
- [12] Vodafone IoT Barometer 2019, accessible at <https://www.vodafone.com/business/news-and-insights/white-paper/vodafone-iot-barometer-2019>
- [13] J. Soldatos, R. C. Sofia, D. Rublova. The IoT open-source ecosystem in 2021. EU-IoT White paper, October 2021.
- [14] R. C. Sofia, J. Soldatos. A vision on Smart, Decentralised Edge Computing Research Directions. EU-IoT White paper, October 2021.



The European IoT Hub

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

FOLLOW US



WWW.NGIOT.EU



The EU-IoT work is partly supported by the European Union's Horizon 2020 Research and Innovation Programme (Grant Agreement no 956671).
Special thanks to all partners from the EU-IoT consortium and to the EU-IoT Expert Group for valuable contributions.