Grant Agreement N°: 956671

Topic: ICT-56-2020

The European IoT Hub

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

D2.1: Towards a vibrant EU IoT ecosystem

Strategy White Paper

Revision: v.1.0

Work package	WP 2
Task	Task 2.1
Due date	31/03/2021
Submission date	04/05/2021
Deliverable lead	Martel
Authors	Dr Monique Calisti, Dr Lamprini Kolovou (Martel Innovate), Brendan Browan, Robert Covaci (Bluspecs)
Version	1.0
Dissemination level	PUBLIC

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 in themselves 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 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 ecosystem will grow as a community of communities and as a diverse and large embracing movement cutting across several research and innovation areas and market segments.

This document is one of the first EU-IoT outcomes and represents a preliminary step to build and ensure the growth of a vibrant European IoT ecosystem, and it includes:

- A critical mapping of various relevant efforts and initiatives.
- A guidance framework to capture experts' input, together with main outcomes of the first EU-IoT Expert Groups (EG) workshop.
- A structured presentation of input gathered from ongoing EC projects 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.

The contents of this paper will be further enriched and elaborated leading to a more consolidated version that is planned to be delivered at the end of 2021.

TABLE OF CONTENTS

LIST OF FIGURES

ABBREVIATIONS

AI	Artificial Intelligence
BMI	Building Information Modelling
DID	Decentralised IDentifier
CB	Coordination Board
CSA	Coordination and Support Action
CTF	Communication Task Force
DEI	Digitasing European Industry
DEP	Digital Europe
HEP	Horizon Europe
IA	Innovation Actions
IoT	Internet of Things
JU	Joint Undertaking
M2M	Machine to Machine
NGI	Next Generation Internet
NGIOT	Next Generation Internet of Things
RIA	Research and Innovation Actions
R&I	Research and Innovation
SNS	Smart Networks and Services
SoS	System of Systems
SRIA	Strategic Research and Innovation Agenda
VR	Virtual Reality

1 THE NEXT GENERATION IOT LANDSCAPE

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 recently 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 at work for the development of trustworthy, sustainable, and human-centric technologies.

1.1 About the EU-IoT approach

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 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 ecosystem will grow as a community of communities and as a diverse and large embracing movement cutting across several research and innovation areas and market segments.

In this respect, the success of the EU-IoT work, but ultimately the capability of European players to join forces and align on core priorities, builds upon the ability to overcome the main diversities (of interests, backgrounds, and contexts) and define a commonly agreed upon strategic agenda.

This document is one of the first EU-IoT outcomes and represents a preliminary step to build and ensure the growth of a vibrant European IoT ecosystem, and it includes:

- A critical mapping of various relevant efforts and initiatives (section 2).
- A guidance framework to capture experts' input (first part section 3), together with main outcomes of the first EU-IoT Expert Groups (EG) workshop (second part section 3).
- A structured presentation of input gathered from ongoing EC projects that highlights major trends and priorities mapping them into the same framework used with the EG (section 4).
- 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.

The contents of this paper will be further enriched and elaborated leading to a more consolidated version that is planned to be delivered at the end of 2021.

2 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 will be offered and new business opportunities will arise also for SMEs, Start-ups and Innovators.

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

- **The Alliance for Internet of Things Innovation[1] (AIOTI)** 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].
- **ARTEMIS Industry Association[2]** 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

[1] AIOTI, https://aioti.eu/
[2] https://artemis-ia.eu/

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 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.

- **GAIA-X**[3] 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**[4], 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.
- **Smart Networks and Services partnership**[5]**.** 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,

[3] https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html
[4] https://app.swapcard.com/event/next-generation-iot-and-edge-computing-strategy-forum/
[5] https://5g-ia.eu/sns-horizon-europe/

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.

- **Data, AI and Robotics Partnership**[6] (DAIRO) 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.
- **The European IoT Platform initiative** (IoT-EPI, https://iot-epi.eu/) 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, symbIoTe, TagItSmart!, VICINITY and bIoTope) 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.
- **The IoT European Large-Scale Pilots initiative** (IoT-LSP, https://european-iot-pilots.eu/), with an EU financial contribution of €100 million, 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.
- **The IoT European Security and Privacy** (IoT-ESP, https://www.ngiot.eu/community/iot-esp-projects/) projects cluster launched in 2018 includes eight IoT security and privacy research projects (IoTCrawler, 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.
- 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

[6] https://ai-data-robotics-partnership.eu/

- **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).
- **The Next Generation Internet of Things (NGIoT) CSA,** finishing 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 [8]. 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.

2.1 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 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 will be gathered and elaborated via consultations, interviews, workshops, webinars, expert discussions on identified topics and priorities. This will feed 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 domains[7].

[7] https://www.ngiot.eu/advisory-board/

- **Community building** which includes:
  - 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 proposed 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 Startups 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 and 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.

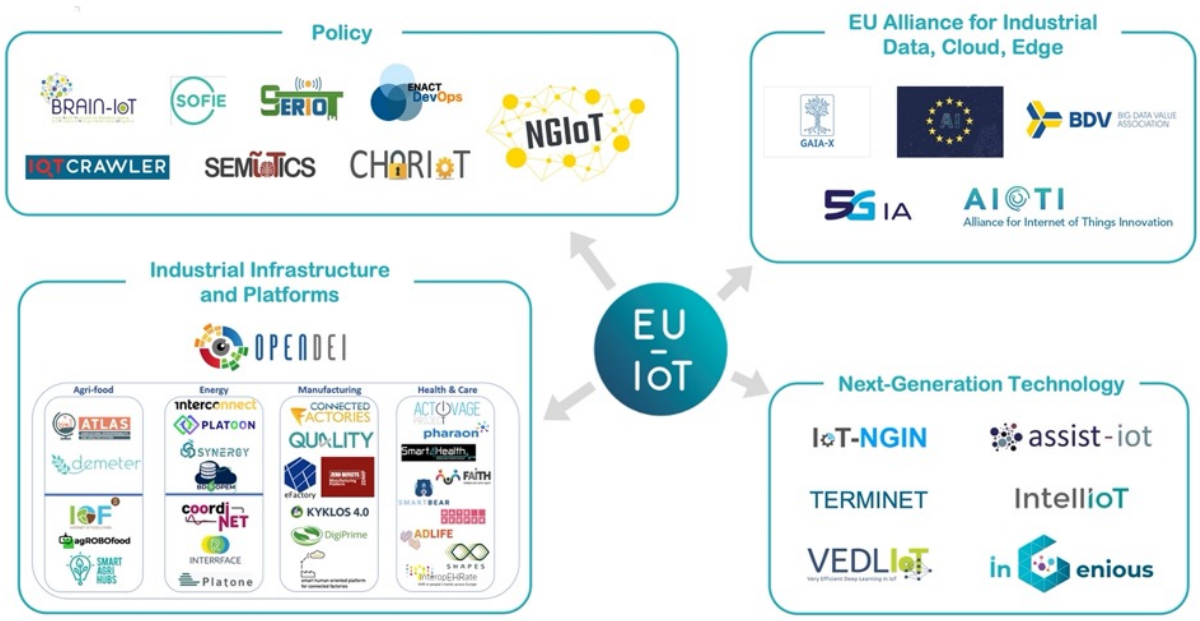

Figure 1: An overview of the current European NGIoT scenario.

3 A GUIDING FRAMEWORK FOR THE NGIOT INITIATIVE

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 searches for areas and themes of progress between and across them.

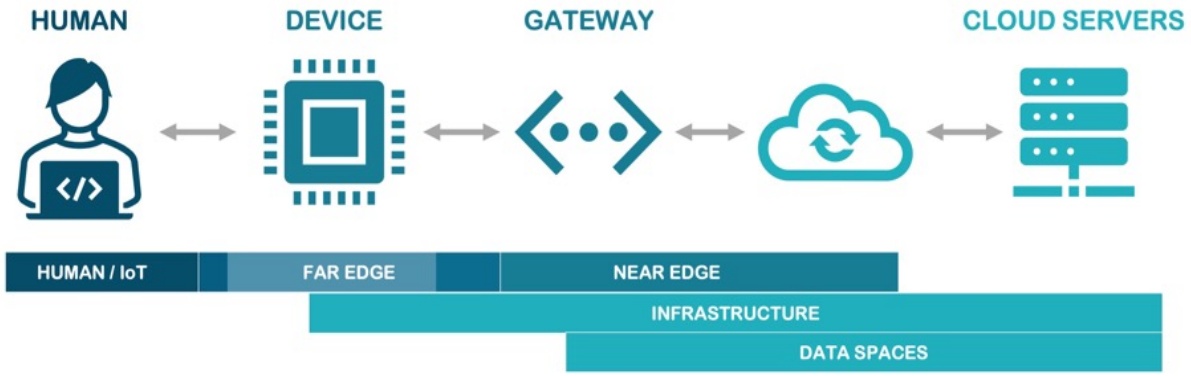

Figure 2: The IoT continuum - from human to cloud and back again with key interfaces

The key research and innovation areas / technological contexts which can overlap and have a reach across the continuum that EU-IoT will focus on are five: 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 3.

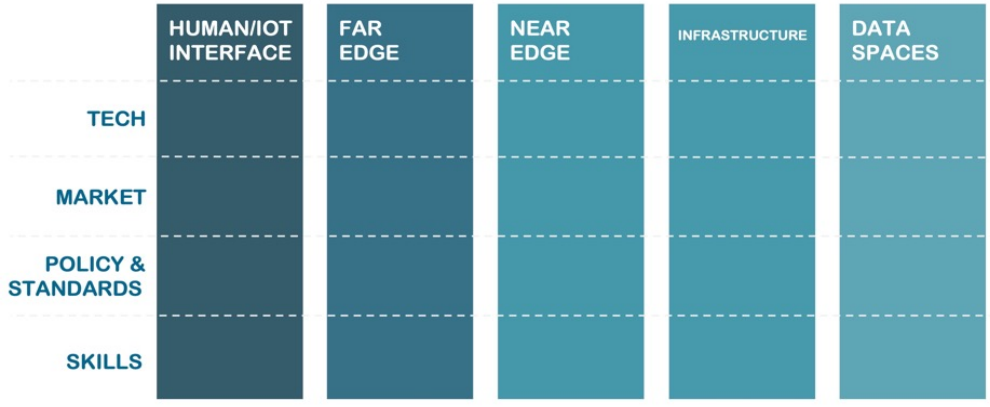

Figure 3: Draft guiding framework of the EU-IoT approach

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.

3.1.1 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.
- **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.
  - Next-Generation Internet, the EC initiative for re-engineering the Internet with European values at its core.
- **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.

3.1.1.1 Human-IoT interfaces – 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, not even aware 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 the functions.
- **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).
- **Haptic-enabled/**AI-empowered interfaces to improve the man-machine complementarity.

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 interface 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.

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

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[8], [9], with ephemeral identifiers providing a good example.

3.1.2 Area 2: Far Edge (device) and Area 3: Near Edge (gateway)

- **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.
  - Tiny ML, run intelligence on small, low-powered microcontrollers and small devices for low-latency, low power and low bandwidth model inference on Edge 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.
  - Distributed architectures, carrying out IoT processes through components located on different, physically unconnected platforms, connected over a communication network.
  - Context dependant IoT, devices that can be customised depending on the needs of their users or operators for efficient operations.
- **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.
  - Cooperational 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.

[8] About Coelition, (2020) coelition.org
[9] Secure Open Federation for Internet Everywhere project, (2020), https://www.sofie-iot.eu/

- **Policy and Standards**
  - Open source and standards, allowing full free open collaboration in the development and deployment of IoT solutions.
  - 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.
  - Multi-access Edge trust, defining the access policies for Edge devices accessed by multiple users and operators.
- **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.

3.1.2.1 Far and Near Edge – Trends and Future directions

Novel IoT systems are 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 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 Edge to the cloud. 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 must however be included from the very initial design stages, to ensure that the integration of intelligence is 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 project, 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 coming with 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 with proliferate.

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 with a physical body, with robots acting as humans in an industrial IoT context.
- Cobots.
- Swarm computing.
- Real-time control loops that can be activated for emergency 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
- Mobility, autonomous vehicles
- Applications in remote or disconnected locations
- 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 example[10].
- The emergence of a marketplace to distribute AI models. This is to be complemented by

[10] EVE project, LF Edge (2020), https://www.lfedge.org/projects/eve/

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. This is contingent on efficient communication between devices. Semantic validation will be required to make data analysis efficient and reduce uncertainty.
- More efficient 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.
- A specific regulatory framework for autonomously active machines, addressing both technical and economic aspects.
- In terms of the use cases, we need 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.

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.

3.1.3 Area 4: Infrastructure

- **Technologies**
  - 5G/6G, and the new applications that will be made possible with the low latency these new networks will bring.
  - 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.
  - 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.

- **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.
  - Distributed manufacturing, decentralising production to several locations, coordinated with next-generation networks.
- **Policy and Standards**
  - Open standards, allowing for the collaborative and efficient development of architectures for the Next Generation Internet.
  - Encryption, ensuring the infrastructure is 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.

3.1.3.1 Infrastructure – 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 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

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 NGIoT 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: IPFS, FileCoin and Ethereum.
- Currently, the strong presence of large tech conglomerates is in some respects hindering evolution and progress for NGIoT 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 expensive 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 and how the business models can be improved should be considered.

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 and IoT would benefit from a similarly large-scale initiative. 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 on.

Europe should increase involvement in open-source efforts and standardisation, taking advantage of community networks across countries such as The Things Network (TTN).

3.1.4 Area 5: Data Spaces

- **Technologies**
  - High-performance computing (HPC), aggregating computers into larger units to allow for more powerful processing.
  - Distributed ledgers, consensually shared and synchronised databases across multiple sites and locations.
  - Quantum computing, taking advantage of superposition and entanglement to improve computing.
- **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.
- **Policy and Standards**
  - Data portability, allowing users control and the ability to delete the data that operators hold of them.
  - Data sovereignty, ensuring data stays in the location where it is generated, or that the generator has full control over it.
  - Accountability, ensuring the data operators respond for their processing activities to subjects.
- **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.

3.1.4.1 Data Spaces – 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 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 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:

- Smart cities
- Healthcare
- Industry 4.0 and beyond
- Consumer apps – unplanned applications
- Smart mobility and driving (connected and autonomous vehicles)
- Smart logistics
- Smart farming, sustainable land use
- Environmental science
- Photon and neutron science

The emergence of personal data spaces in these verticals and beyond will certainly bring significant benefits.

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.

Data sets from different devices need to be semantically compatible 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 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.

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

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. This need 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.

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. This 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.

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 we now need to look at how to merge and exchange data in meaningful ways.

4 MAPPING NGIOT RESEARCH AND INNOVATION PRIORITIES

As anticipated in Section 1, the NGIoT Initiative brings together a set of RIAs which are pushing the boundary of the current vision of the future of IoT. The six ICT-56-2020 projects EU-IOT is more directly interacting with represent a combined EC investment of 48 million Euro, advancing the combined application and generation of technologies along the human-to-cloud continuum. Projects are exploring novel human-IoT interfaces, distributed intelligence on device, models of models approach to autonomous deployments, interoperable Distributed Ledger Technologies (DLTs) for data management and trust, advancing the relevance and applications of 5G and new networks with piloting in diverse areas such as autonomous agriculture systems, port and logistics management, novel automotive systems, and robotic manufacturing.

In the remaining of this section, the focus is on mapping the NGIOT research and innovation priorities and efforts in the areas of technology, market and use cases, policy and standards and skills, at the different points along the human-to-cloud continuum. This mapping has been elaborated by combining input from the Expert Group and closely interacting with the EU-IoT Coordination Board (CB), which gathers representatives from all ICT-56-2020 projects.

4.1 Technology priorities

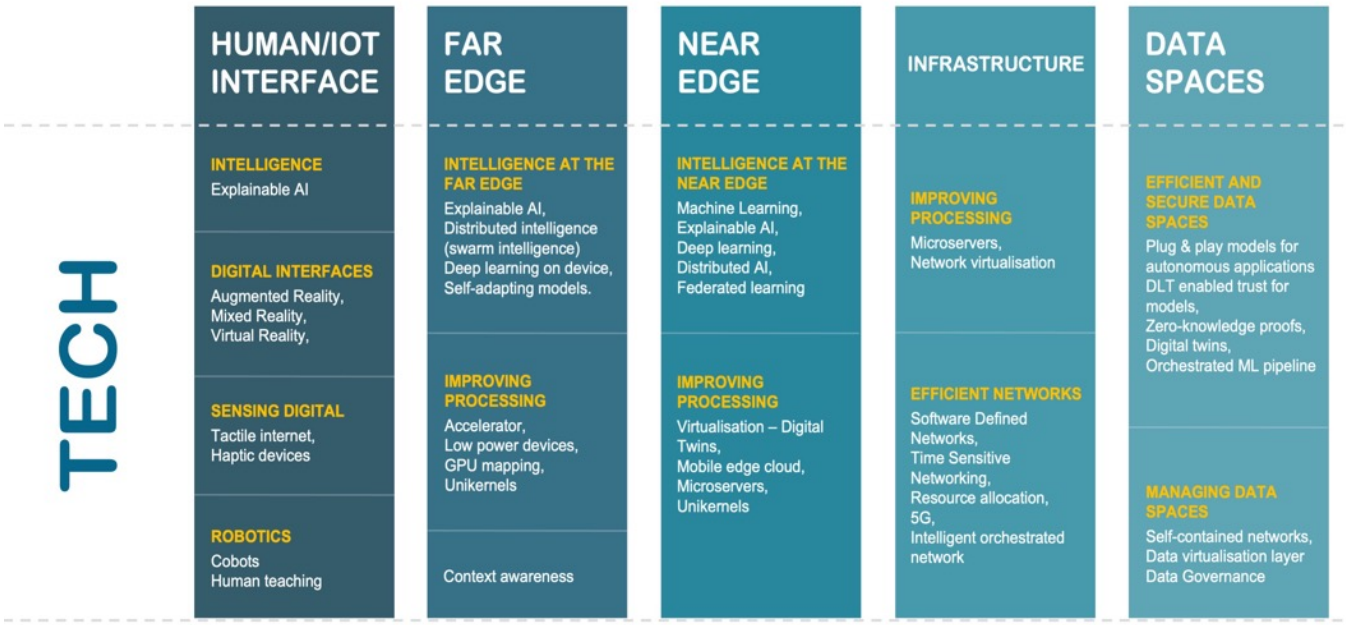

Figure 4: Technology priorities in the NGIoT landscape

Key areas of focus in the technology aspect of the NGIoT 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.
- Digital twins on the near edge, empowered through federated architectures, allowing for efficient and active smart grid monitoring.
- 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 improving traceability and trust, for example in custom manufacturing to record all the steps in production accurately.

4.2 Market priorities

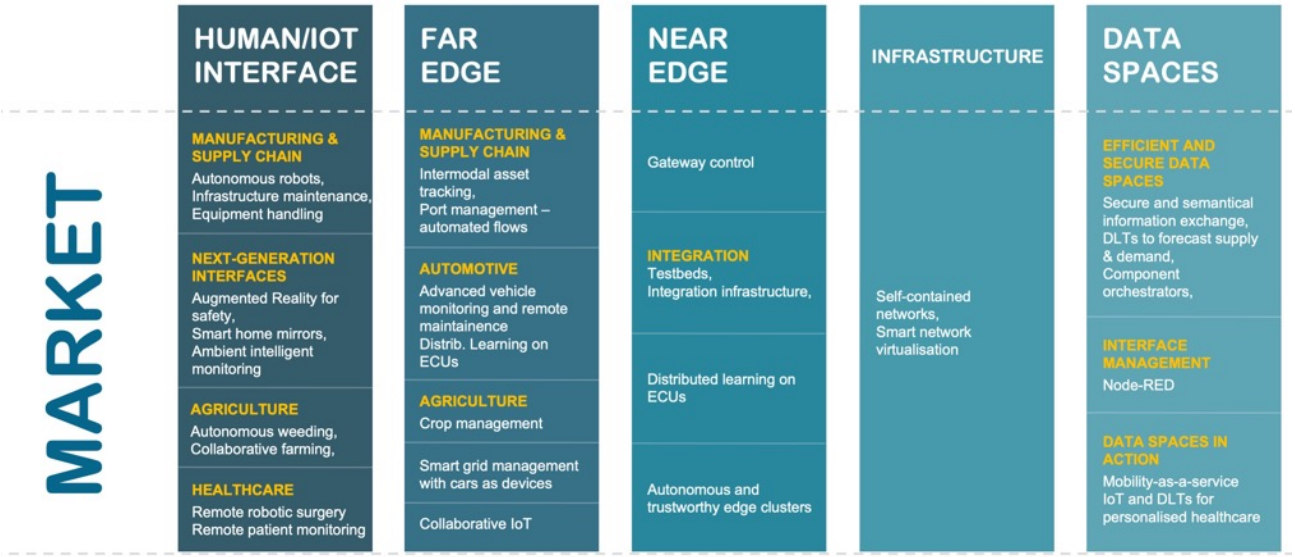

Figure 5: Market applications priorities in the NGIoT initiative

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).

4.3 Policy and standards priorities

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.

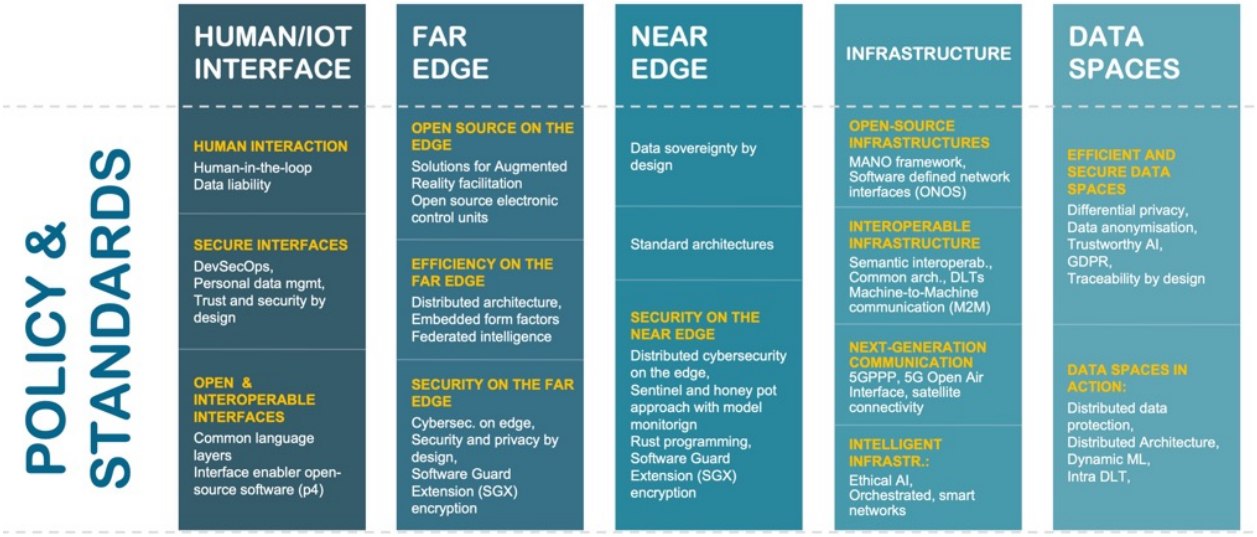

Figure 6: Key policy and standard considerations for NGIoT applications

4.4 Skills priorities

The emergence of this new stack of technologies, as well as the applications and policies that go along, 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 NGIoT ecosystem.

5 A EUROPEAN IOT HUB TO CONNECT THE DOTS

One of the core pillars of the EU-IoT vision and approach, as a driving force to grow and consolidate the NGIoT initiative, is to establish a competitive advantage for Europe, by overcoming the current fragmentation of efforts thanks to a strong and connected research and innovation community.

In this respect, EU-IoT aims to act as a "hub" facilitating liaisons, collaborations, exchanges and promoting accordingly the activities and outcome 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.

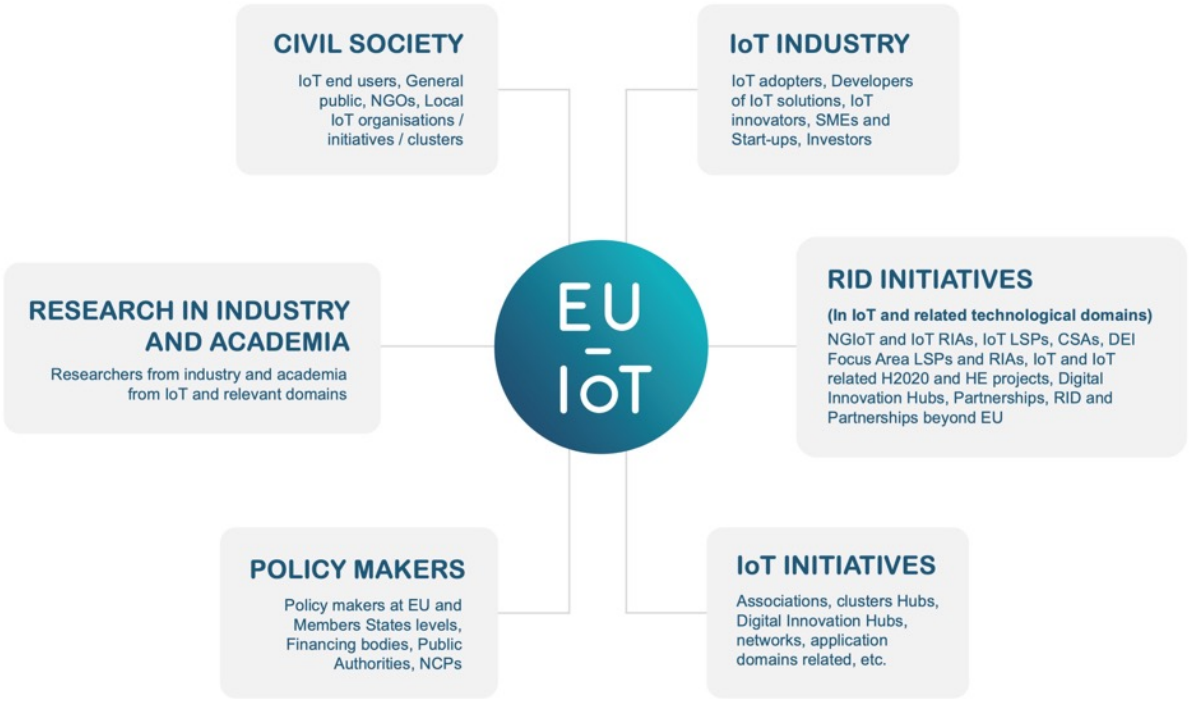

Figure 7: NGIoT ecosystem and EU-IoT positioning

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 leading SMEs and Start-ups growth.
- 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.

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 centers, 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, 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 taskforces of ETSI, 5GPP, IEEE, for instance.
- Open-source initiatives such as FOSDEM, IOTA, OpenStack, FIWARE, Linux 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.

5.1 WRAP-UP AND NEXT STEPS

To effectively connect the dots across such a large and diverse community of communities, is a major challenge as it requires to pull together entities and players with diverse backgrounds, interests, and priorities. On the other hand, for Europe to succeed and European players to overcome the ongoing major crisis at several levels, what is needed is to overcome diversities and act along commonly agreed upon objectives. The EU-IoT work and planned next steps (consultations, surveys, events, strategic road mapping, skills development/training, business analysis and acceleration, standards/open-source mapping, etc.) have the ambition to help converging and joining forces 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.

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