Grant Agreement N°: 956671
Topic: ICT-56-2020

A Federated Future

Mapping of the future directions towards the Cloud Edge IoT from IoT and Edge community

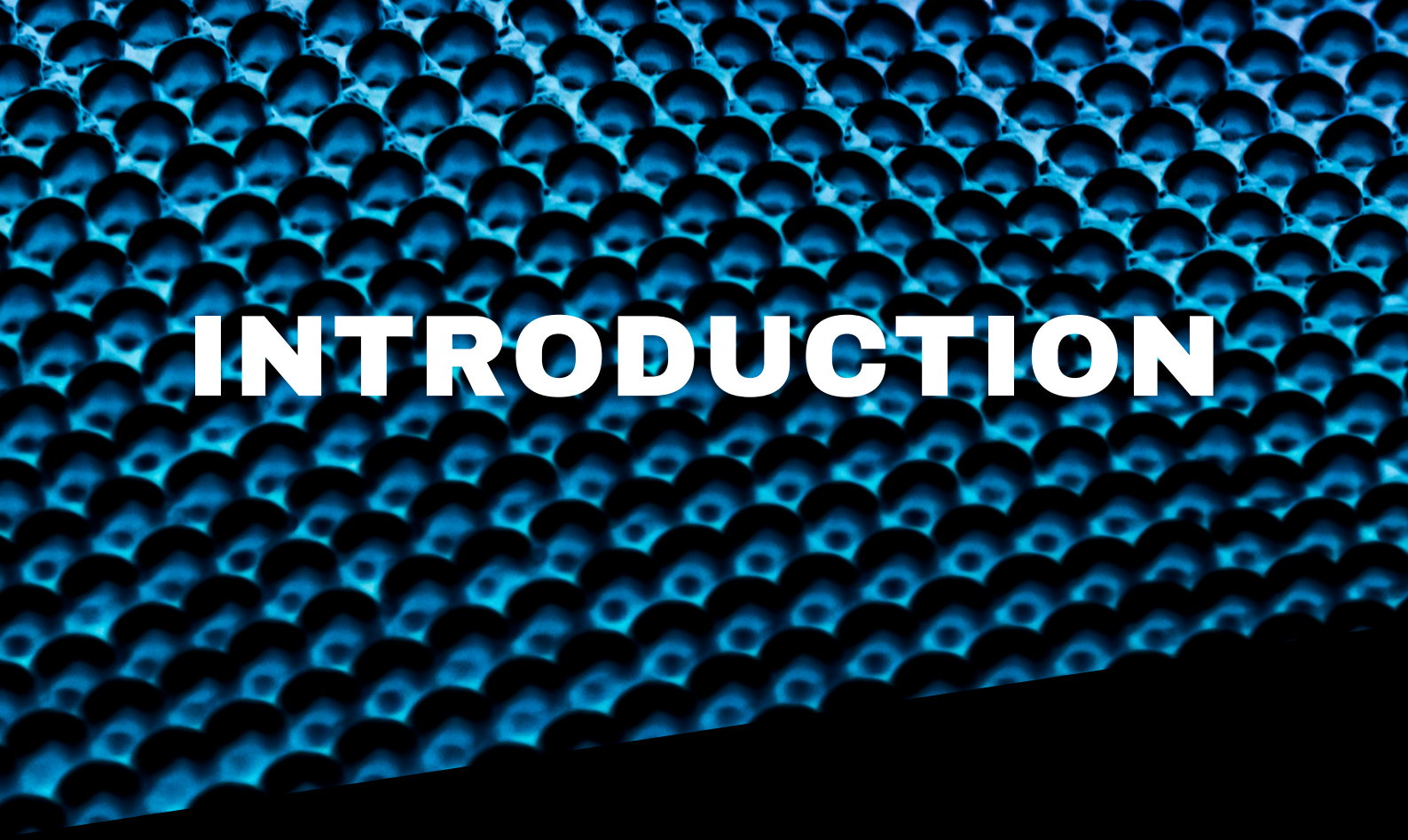
Authors:
Brendan Rowan, Martín Robles,
Sam Jones (BluSpecs)

The European IoT Hub

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

The content of this paper has been developed within the project EU-IoT, the Coordination and Support Action for the NGIoT Initiative funded by the European Union under Grant Agreement 956671. It does not reflect the views of the European Commission and as such the European Commission is not liable for any use that may be made of the information contained herein.

CONTENT



INTRODUCTION

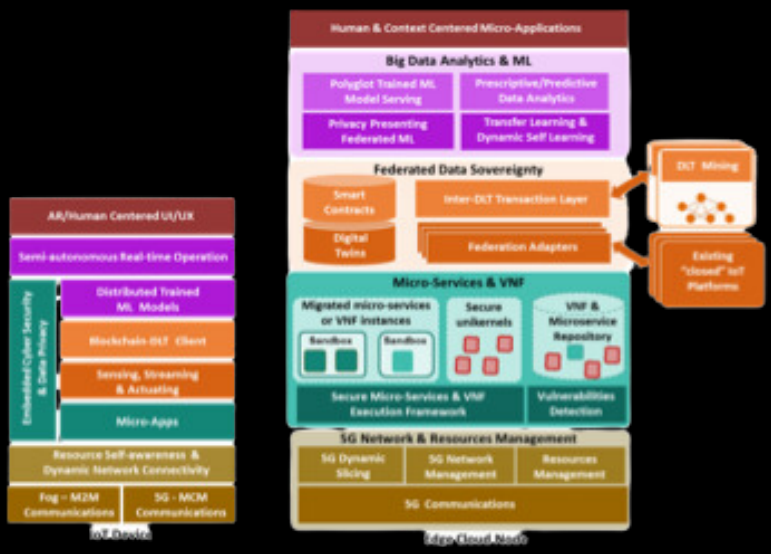
The exact definition of the IoT has been attempted by various bodies, from the IEEE definition based on a description of the constituent elements to the ITU's definition focusing on what it achieves. The definition used previously in the NGIoT Roadmap encompasses both, describing the IoT as "a system of systems that have (at least) the following properties: Sensing and actuation, Connectivity, Intelligence, Heterogeneity, Dynamicity, Scalability, Security".

At its most basic level, the IoT consists of a sensor which generates data, transmitted over a network to a central point for processing and abstraction of knowledge. But what differentiates the IoT from the NGIoT?

INTRODUCTION

The Next-Generation IoT is characterised by a set of properties driven by the convergence of the edge and cloud and which may include:

- Federated architectures are designed for distributed or swarm intelligence and federated services.
- Intelligent devices with hardware accelerators for on-device processing.
- Integration of microservices which support trust and security functions.
- Novel human-IoT interfaces such as AR and haptic responses.
- Leveraging of 5G management with network function virtualisation and slicing.
- Management of public cloud and edge environments in the same application.



High-Level Next Generation IoT Archtecture
IoT_NGIN Consortium

INTRODUCTION

Strategic Research and Innovation Agendas (SRIAs) are structured instruments that encapsulate the vision of an ecosystem of actors from research communities and industry bodies.

They provide a scoping of the key priorities for collective investment and coordinated action within their technology fields for the coming years and are built on the foresight and knowledge of experts actively developing the next generation of technologies.

As such, each SRIA represents the common views and opinions of hundreds of the leading European technology developers and provide a rich source for the identification of future challenges and priorities.

In order to provide the future progression from the NGIoT towards the already established Cloud-Edge-IoT Continuum[1], a meta-analysis of the relevant SRIAs here provides the guiding priorities and key trends for supporting the further deployment of the Horizon Europe and Digital Europe funding programmes.

[1] THE EMERGENCE OF THE EU CLOUD EDGE IOT CONTINUUM AND THE ROLE OF THE NGIOT IS ADDRESSED IN THE FOLLOWING PAPER FROM UNLOCK CEI: ROWAN, B, ÁLVAREZ, JE, & KUŠÍKOVÁ, Z. (2023). TECHNOLOGY SCOPING PAPER (1.0). ZENODO. HTTPS://DOI.ORG/10.5281/ZENODO.7821363

SRIAS WITHIN SCOPE

Within the scope of the NGIoT initiative, 6 SRIAs have been selected for analysis, cumulatively representing thousands of organisations and encompassing the spectrum from human to cloud.

In total 645 topics were abstracted, categorised and analysed across two cycles.

The resulting database is provided as a public output [1] for further analysis and reuse by the community and the construction of future trend mapping.

Within this paper, the latest versions of identified agendas were included in the analysis totalling 590 topics.

- AIOTI Strategic Research and Innovation Agenda (Jan 23)
- Networld Europe Strategic Research and Innovation Agenda (Dec 22)
- Electronic Components and System: Strategic Research and Innovation Agenda (Jan 22)
- European Industrial Technology Roadmap for the Next Generation Cloud-Edge Offering (May 21)
- Made In Europe: Horizon Europe Strategic Research and Innovation Agenda (Sep 2021)
- Strategic Research, Innovation and Deployment Agenda, ADRA Partnership, (Sep 2020)

[1] (2023). EU-IOTS CSA'S SRIA META-ANALYSIS DATABASE (V0.6) [DATA SET]. ZENODO. HTTPS://DOI.ORG/10.5281/ZENODO.7908640

METHOD

META ANALYSIS AND MAPPING

In performing the meta-analysis the following actions were taken to realise the comparison and data collection across the SRIAs and roadmaps:

Within the scope of the identified target communities for the EU-IoT project and NGIoT Initiative[1], the latest publications, roadmaps and SRIAs were revised and reviewed.

Selected SRIAs to be included met the following criteria:

- Relevance to the scope of the NGIoT and latterly the Cloud Edge IoT Continuum.
- Level of detail and structured representation.
- Specificity and actionability of the topics provided.

[1] D2.2 TOWARDS A VIBRANT EU IOT ECOSYSTEM V2.0, 2022

METHOD

From the selected agendas, individual topics were abstracted and categorised under the following fields to provide a comparative analysis and assessment:

- Type
  - Priority area: considered to be topics of strategic importance, encompassing multiple technologies and applications. E.g., Constraint-based planning and decision-making in complex natural environments.
  - Application: specific implementations of technologies either within a given context or addressing a defined goal. E.g., Data streaming in constraint environments.
  - Technology: a variety of different technical, electronic or physical systems, assets, devices or algorithms. E.g., Self-configuring and adaptive sensor nodes.
- Theme: definition of the common priority theme, taking a bottom-up approach and aligning with the NGIoT technologies.
- Position within the EU-IoT framework:
  - Layer: Tech, Market, Policy & Standards, Skills, All.
  - Context: Human Interface, Far Edge, Near Edge, Infrastructure, Data Spaces, All.

Finally, the analysis identified the key trends and themes across the contributing communities and the NGIoT framework.

Below provides highlights and insights, for full details see the deliverable 2.6 from the EU-IoT project

KEY INSIGHTS

Main Trends

Within the data, **it is evident the maturation of AI from basic principles to applications and the emergence of both Edge processing and the Computing Continuum**. Key concepts also observed across all communities include Green ICT, Sustainability and Tools.

AI is required to deliver the development and management of autonomous and intelligent systems, be human-centred and interrogable and evermore efficient.

There is an omnipresence for AI topics across all fields and a demonstrated need to provide the next-generation of processors, interfaces, domain-specific and cross-vertical agnostic models, niche and complex digital twins, the introduction of the concept of ´data for AI´, and **the advancement of hybrid, swarm and distributed intelligence**.

Federation, addressing heterogeneity in devices, data, networks and cloud environments, distributed systems, and the interoperability of such systems is a particular highlight. It defines the emergence of the continuum, underpinned by cognitive, flexible, and contextual computing.

AI and ML, are seen as the tools for delivering performance and trust across the continuum, providing **Self-X – self-organising, self-configuring, self-optimising, self-healing, self-adapting, self-management, self-updating** – in evermore complex and context-aware environments.

New topics are emerging under **Green ICT which seeks to reduce the impact of the deployment of technologies, networks and data centres** as well as putting technology to the service of society in realising a lower footprint across industries.

Similarly, the concept of sustainability of systems and devices is coming to the fore, addressing the **extension of the lifecycle through virtualisation and digital twins, integration and interoperability with legacy architectures and model**s, and improving the recyclability of physical devices at end of life.

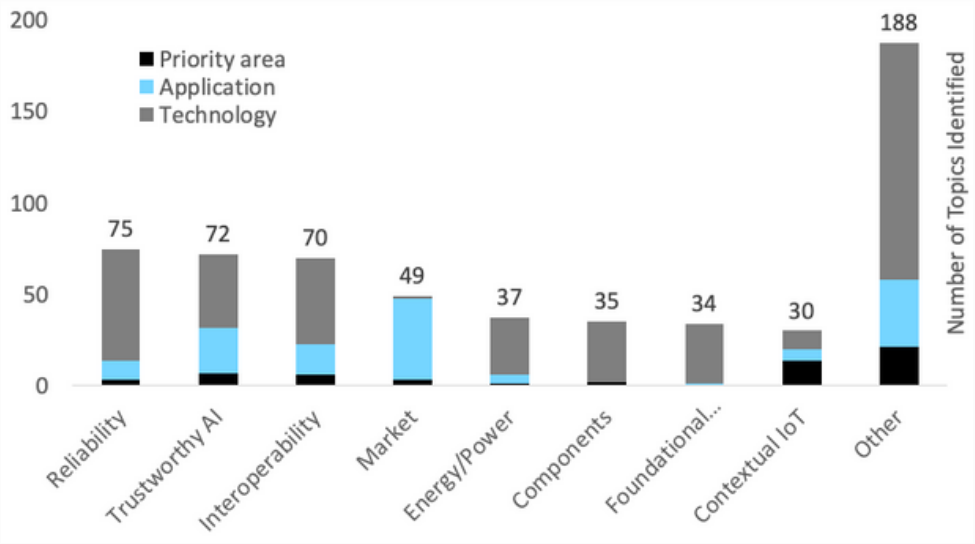
Finally, there is a **demand for the tools and platforms to achieve the adoptability** and application of the technologies. Developers require targeted support to deploy solutions on the emerging dynamic, secure, robust, and integrated systems, to build in off-the-shelf and programmable modules and components across software and hardware, supporting continuous delivery/continuous deployment

ALL SRIAS CONFIRM THE VISION AND DEMAND FOR THE CONTINUUM, BUILDING ON THE NGIOT, THEY SEEK TO ADDRESS FROM DIFFERENT ASPECTS THE NECESSARY TECHNICAL AND MARKET CHALLENGES

KEY INSIGHTS

Priority Themes

Across the 590 topics analysed, 8 key themes were isolated as common priorities which account for a combined 68% of the total set. At the top are the three themes of Reliability, Trustworthy AI, and Interoperability. In comparison to previous analysis [1], Reliability has risen over 8 positions with the latest dataset and Trustworthy AI 3 positions. The presence of Market (applications, use cases and approaches) has increased overall and represents the strategic and applied nature of the tech development within the Cloud-Edge-IoT and NGIoT community.



Reliability

Reliability and the technologies which provide this are a clear priority, especially within the network community.

Reliability encompasses the robustness of systems and the continuity of delivery, resource availability and performance.

Topics highlight the need to ensure the capacity for systems and solutions to perform at scale without loss of quality, latency and speed and the prioritisation of critical processes. Included is the security and safety, and long-term viability of deployments. Compared to the next priority theme, it is primarily composed of technologies.

Examples include:

- Design for (EoL) reliability: virtual reliability assessment prior to the fabrication of physical HW.
- Virtualisation of security functions and application of frugal cryptography and XDR.
- Managing and orchestrating wireless/cellular networks parameters to provide priority for resources based on QoS, safety-, mission-critical features for IoTS systems.
- Redundant, meshed, and flexible optical layer network architectures.
- Secure and intrinsically safe sensing systems.

[1] D2.5 EU IOT ROADMAP AND POLICY RECOMMENDATIONS V1, 2022

KEY INSIGHTS

Priority Themes

Trustworthy AI

A diverse category, which addresses the development and adoption of trusted AI and ML based solutions. It covers **both the leveraging of AI to support the functioning and security of systems and the increased confidence and adoption** of existing and future distributed AI solutions.

Topics look at improving the quality and management of data and knowledge in building models, the scaling and integration of existing models, the cross-vertical adaptations of trained models and the building of human interfaces as well as tackling decision-making processes. Within the theme of AI, there is a cross-cutting thread of promoting and tackling challenges around federated learning, swarm computing and edge intelligence.

Examples include:

- Understand the effect of system heterogeneity on the AI model aggregation efficiency.
- Ensure the applicability of traditional AI methods to swarm systems.
- AI/ML computing with and on transient/limited resources.
- Network Domain Automation via AI/ML assisted decision-making processes and issuing recommendations and improved resource allocation and function placement algorithms.
- Hybrid knowledge representation, techniques for hybrid decision making.
- Develop distributed and federated systems, using heterogeneous decision mechanisms targeted to specific QoS or vertical sectors.

Interoperability

The theme of interoperability looks not only at the level of devices, data and networks but across platforms, models (including digital twins), and whole systems.

The demand is for providing architectures, platforms, tools and networks that can **handle heterogeneity and provide functionality across software and hardware.**

Interoperability also intersects with the reliability of systems and the whole lifecycle management of systems with the application of modular architectures and virtualisation approaches.

Examples include:

- Develop algorithms for the management of heterogeneity of hardware, software and AI
- Engineering process for interoperability along the lifecycle of SoS
- Co-design: algorithms, HW, SW and topologies
- Horizontal and vertical integration of IoT Digital Twins models.
- Create Edge IoT platforms that combine distributed architectures converging mesh, DLT and AI technologies.
- Develop multi-protocol, multi-frequency modules for autonomous edge IoT devices and vehicles.

KEY INSIGHTS

Priority Themes

Market Applications

The theme of market applications is demonstrated by topics related to the definition of use cases, specific societal challenges to be addressed and benefits to be realised, domain-based outcomes and the development of cross-vertical applications.

It is composed principally by applications and more than half of the topics result from the ECS communities.

Examples include:

- Simulation and modelling (digital twins) covering the material processing level up to manufacturing system, and factory and value network level from design until recycling.
- Enhance access to personalised and participative treatments for chronic and lifestyle-related diseases.
- Zero-defect and first-time right production
- CI/CD automation use cases including organizational issues; Integration with business process.
- Vertical Specific Security Profiles:Completion of KPI set per vertical applications. This should encompass security levels and specific attack surface.
- Integrate swarms in multiple verticals sectors to demonstrate added value.

Energy/Power

Across chips, networks, cloud providers and IoT the increased efficiency of systems is a necessary focus.

There is a **need to reduce the cost and consumption per bit processed** to reduce whole sector energy demand, support the operation of constrained devices, promote distributed intelligence and ensure the scalability and business cases for edge and cloud.

Topics address thermal management, resource optimisation, low power and energy harvesting.

Examples include:

- Create new low-power and very low latency protocols for in-swarm communication.
- Exploring offloading of computationally intensive and delay- sensitive workloads.
- Battery-free operation and disposable devices. Low or zero energy systems based on ambient energy.
- Petabit/s energy-efficient interconnections; Cost per bit and power per bit reduction.
- Architecture and processor trade-offs (TPU, GPU, CPU, DSP, ASIC, FPGAs, ASIPs,...).

KEY INSIGHTS

Priority Themes

Components

Within this theme is the development of the building blocks for supporting the topics already identified above. Topics centre on the hardware and software components that are required for advancing the deployment of technologies and are key enablers.

Examples include:

- Programmable Integrated Photonic Processing hardware
- Ultra-massive MIMO
- Flexible and structural substrate electronics
- Embed advanced accelerator functionalities in edge devices
- Design hardware/software for next-generation intelligent, adaptive, and autonomous edge IoT systems.

Foundational Tech

This covers topics, that, unlike components, are in early TRLs of development and tend to have a long-term focus. It addresses quantum, silicon and radio frequency technologies and novel materials. For example, memory technologies towards the yottabyte area, 3D integration technologies, technologies for in-memory computing, and high-performance, ultra-low power 3D integration.

Other Topics

Across the remaining topics, the principal themes include Interfaces (XR and multimodal), Green ICT, Sustainability, Data Sharing, Approaches, Skills and Adoptability.

SUMMARY

SUMMARY

Federation and Heterogeneity

The advancement of the **NGIoT Initiative has been a significant contributor towards the federation of devices, systems, and intelligence.** The architectures, microservices, tools and use cases that have demonstrated the scaled deployment of collaborative and contextual IoT is reflected in the overarching theme of federation across all SRIAs.

The **demand for interoperability at all levels and the deployment across heterogenous devices and systems heralds the arrival of the Cloud-Edge-IoT continuum** and demand for distributed computing across networks and cloud environments. The flexibility provided is to answer challenges faced by businesses, linked to data sovereignty, control and management, efficiency, scalability of systems and guarantee of service with inevitable greater levels automation.

All SRIAs confirm the vision and demand for the continuum, building on the NGIoT, they seek to address from different aspects the necessary technical challenges from new, adaptive components and chips through to AI solutions to provide the autonomous management of whole systems at scale and ensuring the interoperability of data models. **The advancement of federated learning and distributed intelligence is a top priority as is privacy and trust.**

With the increased risk of the integration on a logarithmic scale of devices, edge nodes, 5G networks and shared or distributed models, **secure interfaces are to be ensured and the construction of active and proactive defences, including common standards, platforms, and software components**. Solutions and platforms must also consider how **physical devices and data models do not become threats and their legacy integration is part of the systems to be buil**t, ensuring the longevity of service to the working life of components.

SUMMARY

Trust and Resilience

The **Cloud-Edge-IoT paradigm**, while providing the promise of lower costs, and reduced emissions through orchestrated and distributed processing and the scaling of intelligence, **significantly increases the complexity and dynamic nature of the computing systems**.

The management of such complexity requires AI to support the development and execution of applications which comply and adapt to environmental and regulatory constraints and deliver resilience for the infrastructure on which it is based.

The application of robustness and self-organization in response to incidents and ensuring the continuity of service is fundamental to the federated future.

Without confidence in resource availability and assured redundancy, edge computing and distributed systems will remain solely in a research environment. **Resilience and reliability of systems and associated security needs further development** to deliver an industry-ready, continuous deployment environment.

WITHOUT CONFIDENCE IN RESOURCE AVAILABILITY AND ASSURED REDUNDANCY, EDGE COMPUTING AND DISTRIBUTED SYSTEMS WILL REMAIN SOLELY IN A RESEARCH ENVIRONMENT

Matched to this is the requirement for the platforms and tools to **support development on federated resources and with virtual devices and digital twins.** Investment is required to create the interfaces for developers and reduce the skills demand to be able to build and run their applications and access autonomous management and orchestration.

The human relationship with AI and the collaborative engagement with decision-making and devices like robots is an ongoing challenge. **Human operators must have the confidence and awareness of consequences when applying or responding to AI-generated prompt**s. This must also consider the multi-modality of human-device interfaces, through haptics, XR and similar.

How models are built and managed is just as important as how they are deployed, hybrid intelligence is an avenue for abstracting human knowledge and expertise and ensuring the applicability of outputs but also for acceptance. Added to this is the **emphasis on providing data for AI that supports ethical and secure model training** which reduces bias and improves performance, and also provides for where there is limited or inconsistent data available.

SUMMARY

Stimulating Competition

Distributed intelligence and federated learning is the guiding demand from the community which is being addressed in existing policy instruments.

Funded projects aim to provide the components, architectures, tools and platforms for realising the mass adoption of distributed intelligence. **Cross-cutting is the need to ensure the performance and creation of best-in-class by driving benchmarks** across federated systems for efficiency, frugal use of data, security, privacy and accuracy.

As evidenced, **there are already target use cases and market contexts where the computing continuum may provide an advantage** over existing cloud-based or closed system solutions. The **challenge remains to both clearly define and prove the business case** behind the solutions under development with billions of euros of investment.

This is indirectly referenced across all areas; market dynamics require advances in power, chip production, energy efficiency, developed HPC assets, etc. which are among the topics identified. Continued work needs to advance on the market demand and the preparation of the industry adopters who need to make the case for investing in edge computing and the active participation in the ecosystems being generated through off-the-shelf models, digital twins, and Data Spaces.

Skills and talent are wholly underrepresented across the board, and must be addressed in the context of commercial feasibility, it is a complex problem that requires whole ecosystem mobilisation and the engagement of new communities of education and training providers previously seen as further ‘downstream’ of tech development.

The emergence of a Cloud-Edge-IoT continuum also presents new opportunities for new business models. **Through the virtualisation of assets, it is feasible to explore new forms of revenue generation** and asset sharing, already under exploration through the delivery of micropayments and the tokenisation of renewable energy.

The implementation of the NGIoT across B2C environments in use cases such as in smart buildings, grid flexibility and EV charging involve a change in consumer behaviour, even a relinquishing of control. OEMs and service providers must be engaged to define not just new business models but the behavioural economics behind the deployment in society of the CEI.

SKILLS AND TALENT ARE WHOLLY UNDERREPRESENTED ACROSS THE BOARD AND MUST BE ADDRESSED IN THE CONTEXT OF COMMERCIAL FEASIBILITY,

SUMMARY

Convergence across the digital sphere

The Next Generation IoT is now the Cloud-Edge-IoT computing continuum, the themes and challenges addressed under the NGIoT are now underpinning the whole scale digital transformation of large and important value chains such as energy, manufacturing, or even aerospace. The demand for good data, good intelligence and effective investment in digital is driving the need for federated and trustworthy systems, new devices and new platforms. The eventual success, in part, of **the guiding twin strategic policies of Europe, Digital Decade and the Green Deal rely on the development of the Cloud-Edge-IoT.**

The confluence of data, intelligence and diverse processing resources is influencing the Horizon Europe programme and is evident across the domain-specific aspects of the programme. **This presents a risk of divergence between the communities, researchers and industrial partners in terms of standards, tools, methods, and approaches.** Both the digital and the physical world have encountered significant shocks and the demand for resilience and flexibility is obvious both within industrial ecosystems and the tech developer community.

The positioning of the Cloud-Edge-IoT and the development of the federated and autonomous system is evident as a **foundational pillar for the realisation of European aspirations to lead in digital.** There is an intercalation between the DIGITAL programme and the Horizon Europe activities which culminates in the Cloud-to-Edge Large Scale Pilots and the Reference Deployments.

The DIGITAL programme provides common structures, tools and platforms that should be guided and contributed to by foundational building blocks, use cases, and piloting at scale provided for by the cloud-edge-IoT community.

Within this decade, **the European Union**, across Horizon Europe (€15.3 billion), DIGITAL (€7.5 billion), Next Generation EU (€38 billion), multi-county projects and IPCEIs, **is putting its weight in the scale of billions of euro of investment** behind the creation of a digital infrastructure which promotes ethical use of data, data sovereignty, identity management, resilient and efficient networks, and the security of digital supply chains.

While historic and significant this coordinated investment, **the largest tech companies worldwide, are significantly outspending on their own R&D**. In 2022 alone, Amazon, Alphabet, and Meta spent 69.5, 37.5, and 33.6 billion euros respectively. The leading EU corporate, Volkswagen AG, only spent half, 18.9 billion, on its R&D in the same year which is not exclusively on digital.

There is an opportunity to take an integrated vertical approach to leverage the combined heavy weight of the EU funding instruments to make larger and bigger bets on the Cloud-Edge-IoT. It requires a stronger positioning to create building blocks that follows through onto domain-based applications in other Clusters and across the DIGITAL programme, leveraging at a cross-border level the R&D and innovation investments being made by MS under the Next Gen EU.

THE NEXT-GENERATION IOT

THE NGIOT INITIATIVE

The NGIoT Initiative is a portfolio of 6 Research and Innovation Actions (RIAs) tasked with developing and trialling next-generation architectures. These NGIoT architectures underpin the deployment and accelerated development of edge computing, distributed intelligence, federated microservices, collaborative IoT and tactile interfaces integrating holistically enabling technologies such as DLTs.

The 48 million euro investment supported the transition to the Cloud-Edge-IoT Continuum, driven by the orchestration of cloud and edge technologies which are in turn facilitated by the increased computing power available on chips and devices and the realisation of the collaborative IoT enabled by 5G technologies.

The work continues within the EU Cloud Edge IoT Continuum supporting cognitive cloud computing, metaOS development and swarm intelligence.

EU-IOT

The EU-IoT Coordination and Support Action aimed to transform the current IoT community of researchers and innovators in Europe into an increasingly cohesive, dynamic, participatory and sustainable ecosystem, as an essential part of a Next Generation Internet.

It provided a collaborative framework, including content, tools and processes, to engage all EU researchers, developers, integrators and users, fostering the creation of synergies, liaisons and exchange.

WWW.NGIOT.EU
WWW.EUCLOUDEDGE.EU

APPENDIX

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 service 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, allowing for diversity, while taking into account the specific requirements of different cases. Staying agile and being able to capture needs in a fast-changing context is a major factor influencing the design of the EU-IoT framework proposed below.

EU-IOT FRAMEWORK

The first axis addresses the points of interaction between the physical elements which make up the human-to-cloud continuum, reflecting the current and future structure of the IoT. This axis considers the points of engagement and identifies areas and progression between and across them. These are defined within 5 contexts across the continuum on which the EU-IoT will focus: Human/IoT interface, Far Edge (devices level), Near Edge (gateway level), Infrastructure (including networks) and Data Spaces (cloud-based and super level data sharing).

Within these five key contexts, which frame advances, discussions, and debates, EU-IoT addresses four main layers of interest grouping important transversal aspects, as shown below. Within each of these, there are several transversal themes and topics that will need to be addressed. These layers are:

- Technology: identifying novel and advancing enabling technologies.
- Market: analysing the applications, services, and models enabled by the technologies (both individual and varied combinations).
- Standards and policies: delving into common approaches, standards, and policies.
- Skills: analysing the current and future demands resulting from all the above.

RIGHTS AND OBLIGATIONS

Purpose	Main obligations
Data Act	
To prevent vendor lock-in with cloud and edge providers due to technical incapacity for switching limiting market growth and innovation.	**Data Processing Service Providers** • Port all digital assets of the customers – data, applications, virtual machines, etc. • Provide necessary support for successful completion switching. • Ensure, that where applications or similar cannot be ported, the customer achieves functional equivalence of the new services. • Prevent access to systems through robust cybersecurity practices. • Provide open interfaces for data processing services that are not tied to their infrastructure • Ensure compatibility with defined interoperability standards or provide the data in a structured, commonly used format
Cybersecurity and Resilience Act	
To enhance the security and resilience of digital products in the European Union by imposing essential security requirements on connected devices. The law is a response to the ever-increasing threat posed by cyber criminals, who continuously innovate and evolve their attack techniques.	• Manufacturers and developers of products with digital elements must meet specific essential cybersecurity requirements before their products can be made available on the market. • Manufacturers must factor cybersecurity in the design and development of the products with digital elements, and must provide security updates and support for a reasonable period of time. • Manufacturers must be transparent about cybersecurity aspects that need to be made known to customers and must provide up-to-date information about the end-of-life of the products and the security support provided.

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.