5G IA
INFRASTRUCTURE ASSOCIATION

Alliance for Internet of Things Innovation

Smart Networks and IoT

Common topics for research and innovation in Horizon Europe

5G IA
INFRASTRUCTURE ASSOCIATION

Alliance for Internet of Things Innovation

1. Introduction

The 5G Infrastructure Association (5G IA) and Alliance for Internet of Things Innovation Association (AIOTI) are collaborating closely on identifying the research and innovation topics that fall into a common scope of interest across the two associations. These topics are crucial for the successful development and deployment of Smart Networks and Services under the Horizon Europe programme.

The two non-profit organizations; 5G IA which comprises leading European players in the ICT value chain and addresses key areas related to 5G development and beyond, and AIOTI which works to stimulate the market uptake and deployment of Internet of Things (IoT) and its applications in Europe are working to develop a future vision giving direction towards Horizon Europe. In this vision, AI (aritificial intelligence) based control systems in critical application areas in society and industry will depend on data provided by billions of nodes in the IoT, communicating over high performance smart networks.

Continued collaboration between 5GIA and AIOTI on the topics identified in this document will, we believe, help to create economic value and justification for all stakeholders across Europe's smart communities, energy, industry, mobility, farming, healthcare and many other areas.

5G IA and AIOTI have already created a joint vision paper and in addition developed their individual positions on Horizon Europe priorities in the 5G-IA position paper and AIOTI position paper.

This latest "common topics" document summarizes the combined 5G IA/AIOTI work in progress towards developing a common Strategic Research and Innovation Agenda (SRIA) together with the Networld2020 European Technology Platform, for the advancement of Horizon Europe and related program discussions with all relevant external stakeholders.

This document offers a concise overview of research topics of common interest (section 3), starting from an application (use case) viewpoint in section 2, and also expresses the experience and relevance for end users and wider society in key example vertical domains. Section 4 addresses critical non-technical and socio-economic success factors for Smart Networks and Services. Finally, it summarizes important standardization-related and research- driven subjects.

We welcome further discussions and look forward to your engagement in establishing a successful collaboration program.

Colin Willcock
Chairman, 5G IA

Jürgen Sturm
Chairman, AIOTI Management Board

2. Empowering Verticals and Public Sectors: Examples

The IoT, underlying communication networks and security technologies are not goals in themselves.

Rather, they enable applications that contribute to the welfare and wellbeing of European citizens and empower the digital transformation of our industries, companies and public services. Traditionally, technology development and user-centric application development have not been strongly linked. The ever-increasing scope of digitization makes this issue even more acute.

A more holistic, end-to-end approach is critical for the socio-economic success of digitization across the entire value chain, building on expertise in, for example, sensing hardware, systems integration, communications, data storage and processing, artificial intelligence (AI) and its applications. Europe therefore needs to empower vertical application domains in industrial and public sectors and help to establish strong concurrent ways of working. This would increase speed and bridge the gaps as we move from ground-breaking technology, component and systems research, development and innovation into proof of concepts and large-scale trials for specific verticals.

This section describes a number of verticals and relevant topics (use cases) that requires high attention throughout Horizon Europe: it is not exhaustive and will be continuously updated. Nonetheless, these snapshots communicate the value and relevance of a common approach by identifying:

- Problems being solved - and how this contributes to society
- New business opportunities and job creation
- Innovative business models and ecosystem development
- Technical challenges

2.1 Smart Living - ageing at home with personalized remote virtual care

A modular and adaptable IoT solution is required to fulfill the diverse needs of ageing populations.

Digital care can have a strong impact in outpatient management and preventions. Indeed, using IoT and AI in health and care transforms remote patient management. Additional progress is required in enabling virtual visits and monitoring by Health and Social Care Providers, improving follow-up practices by collecting smarter streams of data and leveraging AI. IoT and 5G will enhance the hospital-home relationship, to help better manage the care of long-term patients who require most resources from a healthcare system.

2.2 Smart Manufacturing - safe unfenced human-robot interaction in assembly lines

We need safe and flexible solutions for Human-Robot-Interaction (HRI) in automated assembly lines that use heavy duty robots. Independent of specific robot types, this includes development of certifiable sensor systems in combination with real-time supervision and assessment tools for human safety.

Progress is required in creating accurate and real-time positioning systems, locating persons in harsh working environments and enabling a higher collaboration grade by reaching even shorter safety distances between human and machine. We also need to improve industrial-suited motion capturing systems, and develop safe wireless transmission systems for industry environments through the dynamic provision of secure and isolated "network slices". Finally, there is a need to develop risk assessment toolkits and safety-centric design methodologies for Human Machine Interaction.

Many of these topics will draw on 5G Ultra-reliable and/or Low Latency Communications (URLLC) in combination with edge computing, merging Information Technology (IT) and Operation Technology (OT).

2.3 Smart Mobility - autonomous and hyper-connected on-demand urban transportation

Every day, millions of people travel to and within large cities, which are becoming increasingly crowded and less sustainable. The opportunity is to revolutionize the mobility of people and movement of goods. On-demand smart mobility services can contribute by providing a single integrated platform, but on-demand services have not yet achieved a real-time 360-degree view of the customers and users.[1] And while autonomous vehicles are expected to make a strong contribution, they are not a mass-market reality yet, requiring more reliable, robust and extended wireless networks .

By combining ride sharing with car sharing in autonomous vehicles, for example, we may meet people's need for travel with far fewer vehicles. Traffic management will improve by connected vehicles interacting with their environment

[1] 5G: Evolution and Revolution. TMForum. April'19
[2] 5G and connected vehicles: communication and cooperation. Orange – Hello Future research blog 2019

(V2X), becoming smart objects in the IoT, with continuously improving routing, energy consumption and performance.

The ecosystem will therefore evolve towards new collaborative models among multiple stakeholders across Communication, Navigation, Car Manufacturing, Data Science and AI, Digital Skills and Cybersecurity.

Progress is required to create a more global and ubiquitous communications and networking core. This will not only require 5G capabilities but also next-generation mobile communications addressing new technical challenges in end-to-end network management, such as big data analytics, AI and advanced wireless capabilities.[3]

Creating this will require a massive concerted approach across a variety of subjects: operations support system/ business support (OSS/BSS) systems; radio resource and network management; intelligent mobility; modelling for connected vehicles; advanced wireless connectivity; predictive automation; cloud and edge high performance computing for mobile networks; massive scale of autonomous IoT networks; and novel cyber security concepts.[4]

2.4 Smart Farming and Food Security - autonomous co-operative robots in agriculture

Farm labour is increasingly automated, with evolving autonomous tractors/harvesters and smaller ground and air robots making farming and food production more sustainable, efficient and traceable.

To take these developments forward, industry requires greater scale allied with a more granular approach in sensing, monitoring and actuation.The data provided can also support "digital twinning" in production, employing AI to deliver state-of-the-art virtualization of farm and food chains, extending to "living objects" and with more granular models

Progress is required in the interactions between robots and humans. For example: low-latency, reliable communications and supporting autonomous decision making "at the edge" based on embedded AI and low cost (CAPEX and OPEX) devices, with autonomous low power operations over longer periods and massive machine-to-machine (M2M) communication at low data rates.

2.5 Smart Cities and Smart Communities – cross-vertical collaboration justifying platforms

The smart cities and smart communities of tomorrow require new operating models that drive innovation and collaboration across vertical silos.

Traditional operating models for cities are based on functionally-oriented service providers operating as unconnected vertical silos. However, with smart cities and communities becoming the crossroads for consumer IoT, industrial IoT and enterprise IoT, a "platform of platforms" is necessary. This means not only empowering verticals but also empowering communities and cities by enabling an integrated approach across verticals. The ability to share and re-use data from different domains simultaneously is critical. To replicate and scale up smart city/community solutions, it will be necessary to provide common elements to all alongside tailored solutions for individual cities.

Systems currently being offered follow a narrow vertical framework, simply because such systems are easier to develop. This comes at the cost of duplication of effort, non-value added diversity, lack of critical mass and high maintenance costs. This will also hamper the economic justification and viability of 5G network infrastructures.

Progress is required in developing horizontal collaboration to create innovative systems development for IoT. Work on semantic interoperability is promising but far greater efforts are needed. Technology is not the only bottleneck, but also emerging business models (including the role for 5G), data ownership and security, distributed ledger applications, trust with citizens, open data, open standards, readiness of 5G infrastructures etc. More than anywhere else will cross vertical alignment provide the basis for vertical applications and the economic justification the required 5G and beyond infrastructures.

2.6 Smart Water Management – maintenance, operations, quality and consumption optimization

The value of water to individuals, society and the economy is immense; huge challenges must be overcome in terms of maintenance, water quality, and the robustness and optimization of infrastructure and consumption. Promising technologies are becoming available to support such efforts including connected devices with embedded intelligence, aggregate resource management, advanced AI, and always-on utility networks based on smart connectivity infrastructures.

Monitoring and controlling water infrastructure is highly challenging due to lack of measurements, difficult access and high cost to access several parts. Real-time monitoring is not provided. Progress can be made in this area by introducing new sensors with improved power management (operational and standby) plus low power data transmission protocols. For time-critical utility applications, there is a need for low latency communications.

For real-time water quality assessment and consumption optimization, leaks in urban water supplies cause important losses that need to be detected by comparing consumption and inflow with a fine-grained sensing network. Water quality should also be measured and guaranteed during its lifecycle and real-time changes need to be detected to find and solve pollution. Progress is therefore needed in deploying large numbers of sensors in diverse locations, energy management optimization in those sensors to provide a long lifespan, collecting massive amounts of data and processing in the edge, fog or cloud with subsequent application of AI algorithms, and more. Dedicated network designs will be required and close alignment between domain and infrastructure specialists.

Real-time prediction and management of consumption habits can also create savings in overall water consumption at the utility level; this is the rationale for advancing personalised water services. Smart water grids need to become fully operational based on a trusted large network of smart sensors and actuators with real-time interactions.

2.7 Smart Energy Management

Energy systems are also vitally important to our society and economy;, the energy sector is undergoing a complete transformation. This is based on the transition to decentralised (solar and wind) renewable sources, energy buffering and storage, supply and demand optimization, the rise of electric vehicles and (EVs) and smart charging networks, dynamic bidirectional networks and the trend towards a prosumer (production by consumers) market with dynamic pricing.

Future smart grids will need to optimize supply and demand, manage energy flows between millions of nodes, enable dynamic pricing and transactions, anticipate weather and consumer behaviour, all in a sustainable way with high levels of integrity, security and resilience. This is not possible without AI based on high quality IoT, networks and data.

Progress is required in many areas: intelligent end-nodes (edge) systems for supply, demand and storage of energy; sensing and sensing data; local and global real-time communication networks serving a smart grid; micro-payment platforms to support a prosumer energy market; establishing a data market to optimize overall energy generation and consumption; security systems; and predictive modelling systems using AI.

2.8 Smart Buildings and Architecture – connected, software-defined, cognitive and human-centric buildings

Buildings are a fundamental component of cities; to create sustainable and liveable smart cities, those buildings need to become connected across multiple systems. These systems include CCTV, access control, environmental monitoring, lighting, HVAC (heating, ventilation and air conditioning), audio/visual distribution, resource management, smart vending machines, and parking. Progress is essential in terms of enabling interoperability and data exchange through standard protocols and application programming interfaces (APIs).

The Software Defined Building (SDB) strand focuses on creating "digital twins" that enable buildings to be comprehensively monitored and controlled by IoT devices and Cyber-Physical Systems. The SDB is the evolution of the connected building and gains can be expected in substantial resource optimization (space, energy, waste, water) with an improved experience for residents.

With Cognitive Buildings, the software rules in an SDB are not written explicitly by a facility manager. The platform itself provides algorithms to adapt and react to changes, and pursue objectives defined at a higher level (e.g. energy optimization and comfort). Progress is required to develop apprpriate autonomous strategies for optimization, learning systems, IoT implementation and convergence of data.

Ultimately, a human-centred building includes an AI based focus on the comfort and productivity of inhabitants in all aspects in and around the building at the lowest operational costs and footprint. This area is still at its infancy and significant progress is required in the next decade supported by IoT, future networks, data and AI.

2.9 IoT-enabled Data Marketplaces

All of the topics and use cases mentioned here will require the development of data and data sharing/markets to reap the benefits of IoT and future networks, justifying in economic terms the underlying technologies. Data as a Service (DaaS) offerings have been available for years but IoT is not a mere extension of DaaS. IoT brings together Information Technology and Operational Technology, often in relation to critical industrial processes. This complicates the task of making IoT data available to third parties, given concerns around potential threats to privacy, security, safety and the confidentiality of commercial intelligence. This is why Europe must investigate and address the many aspects required to build trust in IoT-enabled Data Marketplaces.

Significant progress must be made in creating new EU champions able to operate and innovate around the (data) marketplaces, and creating new leaders in data science based on proven European know-how in AI and Machine Learning (ML). This will help to strengthen the competitiveness of EU industries based on fresh and representative data, and generate new revenue streams. It will require orchestrating and stimulating the value chain at several points: platforms, data generation, analytics and cross-leverage in the data market.

2.10 Relationship Between IoT and Public Safety

The link between public safety and IoT is largely a missed opportunity today: there is a strong rationale to address this issue, with a view to saving lives and avoiding damage to

[3] Inclusive Radio Communication Networks for 5G and beyond (IRACON project - Jan'16-Jan 2020)
[4] Atos secures communications in connected vehicles, Jan 2019

infrastructure. Identifying the industry challenges associated with integrating IoT and public safety (e.g. calamity handling) and the role of smart networks is an area that requires extensive research, innovation and development before this synergy can deliver real-life benefits. Issues to be explored and resolved include interworking and interoperability at cloud levels, governance, citizen engagement, device certification and policy incentives.

3. Research Topics and Challenges

This section summarizes priority research to be undertaken to enable the applications and benefits described in section 2 to be achieved. The research will take into account and be driven by high-level societal missions. The below sections first present research topics triggered by generals trends such as digital service transformation and higher attention to societal and human-centric aspects as well as the need for network technology agnostic services. A closer look follows considering network and communication systems as well as edge cloud and end-to-end views. Furthermore, increased automation through effective platforms, federation and delivery are addressed, while also considering applications, user experience, privacy and security. The section concludes by suggesting research that will facilitate attention towards human factors and societal missions.

3.1 Digital Service Transformation

Telecommunication networks are an essential pillar of modern infrastructure. Each successive generation of mobile networks (GSM, 3G, LTE, 5G) goes beyond a simple increase in speed or performance, bringing unique new service capabilities.

The latest trend is the convergence of future networks, cloud computing, all types of connected object and the strategic use of data and analytics in end-to-end (all encompassing) platforms. We expect clouds, networks, IoT and data to form dynamic and intelligent collectives (swarms) featuring localized, timely interactions between compute nodes, each with their own autonomy but working together for to benefit the collective community. Examples of this Swarm Computing can be found in autonomous vehicles and many other domains.

Communication Service Providers (CSPs) will need to adapt rapidly to this trend, offering new services over digital channels in areas including consumer entertainment, mobile banking and autonomous transportation, creating strategic alliances with vertical sectors to build and offer powerful and persuasive B2B2X propositions.

A world where CSPs provide services to any number of end users, whether they are enterprise, retail, partner, government, suppliers or consumers. An opportunity also exists for CSPs to offer new networks as self-service platforms by using a high degree of operational automation and complete customization. This will bring additional technical challenges to ICT infrastructure

We need to start "adapting the legacy" now, to be ready for the new digital economy and to smoothly manage the ICT continuum. These end-to-end management platforms should be:

- Modular with a high level of resource abstraction, based on multiple vendor combinations
- Offer "service capability exposure functions" via open APIs to enable CSPs to partner with enterprises in vertical sectors

3.2 From Software-Centric to Human-Centric Services

Today's techno-social revolutions should be helping customers and citizens to become more innovative in how they live and work, and help in the continued evolution of digitalization. New innovations are as much about social inclusion and personal wellbeing, for example, as they are about the digital transformation of industries and businesses.

These changes will require a flexible and programmable architecture to satisfy the large diversity of use cases and applications. In addition, the next generation of networks beyond 5G will go from software-centric towards the concept of human-centric: considering human skills, activities and behaviours first, and using automated functions to support them. The benefits can include reduced risk, higher rates of compliance, enhanced management support and improved interaction with users.

We envision that future networks will interact in more human ways. Network interfaces will recognize not only voice commands but also gestures and moods, reacting to them as in human-to-human communications. This may be just the start: interfacing with multiple sensors and applications as part of service coverage. All these cases will demand future networks go beyond issues of greater bandwidth, almost zero latency, global coverage and always-on connectivity. Connectivity limitations, should they exist, can be avoided via "follow me" networks.

3.3 Network-Agnostic Vertical Services

5G networks were conceived to support a variety of use cases by "slicing" the physical network into several logical networks or slices. Higher levels of abstraction are envisioned to be in place to make this process fully automatic and network unaware to a vertical stakeholder, including individuals.

Vertical applications will have to be completely network-unaware, which leads into a fully automated "from human to network" translation process. Future mobile intelligent applications will learn in the computing infrastructure and get balance deployments from the edge to core. Using AI and machine learning will continuously improve application service delivery. To support this, future service architectures will have to comprise an intent-oriented service definition over abstracted infrastructure, real-time telemetry of services and massive correlations, and proactive adjustment of parameters to meet service intents.

The network will literally be "always-on" and automatically carry out "follow-me" actions. This continuum will be a self-driven platform also able to perform fault isolation and prevention, deal with trust areas, and hybrid orchestrations for the optimization of services at scale. The combination of an intent-driven approach and AI/ML techniques for managing both network and services will bring enormous gains in service efficiency and functionality, which also poses a big data challenge that must be resolved.

3.4 Network and Communication Systems

Impact of IoT on Network and Services: a huge amount of effort in the next decade will be directed at the seamless integration of earlier generations of network and communication architectures. This will require applications to access IoT resources through some kind of identifier, independently of their native platform, their hardware characteristics and protocols. The required services will become major components of the network itself and solutions will be designed so they can support the next leap forward in IoT evolution, in which individual IoT resources are not bounded to a specific isolated platform. Users will become prosumers of IoT services, requiring new authentication and accounting solutions.

The major feature will be wide diversity (dissimilar elements) across access technology, identification, naming and addressing schemes, traffic patterns, deployment extensions, device capabilities, and so on - with a flexibility well beyond what is possible to achieve with current software defined networking and network function virtualization. Slicing, one of the major concepts exploited to support several logical networks with heterogeneous behaviours on top of the same physical infrastructure, has to profoundly evolve in the IoT context. Moreover, the volume of data generated by the IoT is expected to increase at a magnitude higher than available data rates. This trend is not sustainable unless radical changes in the Internet infrastructure are introduced. Largely a communications infrastructure today, the Internet must transform into a computing and communication infrastructure capable of executing data processing and fusion in any of its components. Increased interest in edge cloud and edge computing moves in this direction but more is required. By turning all network switches/routers into computing nodes, the anticipated open multi-service Internet will become a huge and pervasive network of middleboxes, at the same time challenging many current assumptions. It is clear the true IoT revolution will only happen if reasonable levels of security can be guaranteed, for which substantial efforts are required.

Network and Services enabled by ML and AI: artificial intelligence and machine learning will enable innovative features when provisioning future digital services for homes, businesses, government, transport, manufacturing and other verticals, and for smart cities. This will drive the move of computational and memory/storage resources from huge data centres towards the edge of the network, so changing network designs. At the same time, we expect a significantly increase in the amount of machine-to-machine (sensor) communications monitoring smart cities, Industry 4.0, smart energy, etc.

AI will play an increasingly important role in network management - reducing costs, increasing productivity, and driving more value and an improved customer experience. A range of learning techniques will be used to predict the behaviour of the network. This will lead to better provisioning of resources, avoiding the typical situation today where networks are over-dimensioned. In terms of OPEX optimization, with energy consumption one of the major cost items for Network Operators, AI/ML will enable "data lake" approaches to support performance analysis and optimization methods for energy consumption versus quality of service. New services powered by AI/ML will also bring significant socio-economic impacts together with improved sustainability models for Network Operators. Personal data platforms tightly connected with network services will allow Internet users to control their data. Future networks will of course have to address security challenges with a new perspective; integrated AI/ML will provide new instruments to mitigate the risks. Applications of AI/ML are also likely to require multi-domain orchestration of distributed processing, meaning end-to-end interoperability is a must. This requires greater standardization efforts and further progress in the functional architecture of 5G networks and beyond. Hardware and software vendors will need to participate in standardization bodies and collaborate with Open Source communities.

Application Level Networking: The continued growth in video applications including augmented reality (AR) and virtual reality (VR) requires new approaches and solutions. Surveillance and monitoring further complicate the space, as will the growth in real-time sensor data e.g. for industry and smart cities. The ongoing shift of TV distribution from broadcast to the Internet will accelerate, requiring at least a 10x increase in video traffic volume with increased performance and resolution. The implications on application level networking are tremendous: we will need to integrate video services with the web content framework, delivery model and APIs, with effective use of ultra-dense and diverse wireless networks. Video provenance will become a key issue to combat "fake news" and the effects of AI/ML-generated video that can subvert legitimate content. Strong security and integrity of applications, network transport and in-network processing will be required. The security challenges are immense.

Applications (Components) in the Network: A key development in the network architecture is the deep integration of application and service functionality pervasively within the network. The concepts of fog computing apply, but also software-defined networks, network function chaining, virtualization and container provision. There are numerous challenges in developing this vision:

Service discovery is essential. Existing mechanisms are not sustainable and alternative routing algorithms may help scale the routing infrastructure, but there are many open questions on how these will work. For example, the architecture will have to become far more dynamic, since the network of the future will be addressing billions of sophisticated data management and processing services. Service provisioning, management and security are critical. We must learn how to effectively manage billions of devices, ensuring they are suitably configured, running appropriate software, kept up-to-date with security updates and patches, and run only properly authenticated and authorized applications. Security models must evolve. Secure boot, code signing and cryptographic verification of the execution environment will become critical, alongside tools to manage and control data access, management and provenance.

Authentication of services and service providers, while accounting for resource usage, is an essential part of the economics of the network of the future. Micropayments will become a key part of the system as the infrastructure to support in-network services and applications is not free.

Privacy and data management, and the location of processing and data to match legal and moral restrictions on data distribution, access and processing, will be increasingly important. Many of the services and applications will operate on, process and deal with personal data that is increasingly (and rightly) subject to strict regulation, control and limitation. Strong tools do not exist to describe in human language, legal language or code how data can be processed, located and distributed. Policy descriptions, rules and constraints will need to be specified in a form that can be enforced by the infrastructure on the services, since direct human oversight is not feasible at this scale. In addition, novel programming models and languages are required to support all of these services, applications and deployments.

Devices, Dynamic Network Adapation and support of Open Device Management: Deploying and managing a large set of distributed devices with constrained capabilities is a complex task. Moreover, updating and maintaining devices deployed in the field is critical to keep the functionality and the security of the IoT systems. To achieve the full functionality expected of an IoT system, research should be done in advanced network reorganization and dynamic function reassignment. Research is also needed for providing new IoT device management techniques that are adapted to the evolving distributed architectures for IoT systems based on an open device management ecosystem.

3.5 Cloud and Edge Cloud Computation and End-to-end Communication

Converge of Protocols and Software Defined Networks/ Network Function Virtualization: Several technological trends will affect protocol development. These include ultra-low latency end-to-end communication, capacity of access links and diversification of infrastructure for underlying 5G networks (e.g. Visible Light Communication links, mm-wave links, new WiFi standards). At the same time, Internet communication patterns are changing, and increased flexibility of in-network devices and networking software in end-hosts is becoming the new norm. Security, privacy and trust have also moved from being an afterthought in the design of new communication protocols to an absolute necessity in the face of an evolving cyber threat landscape. Several of these trends conflict with the traditional layering in the Internet and TCP/IP protocols. Some developments that partially address these issues have surfaced, such as Information Centric Networking (ICN). Mainly US industry has been developing methods to improve performance, security and flexibility of the Internet's transport layer but it is unclear whether these point solutions will satisfy the needs of upcoming and future applications, and be suitable for 5G network technologies and beyond. Greater flexibility in end systems and inside the network is a necessity, and Internet transport protocols will have to be exchangeable at run time. Improved interplay between applications and the underlying network will also be necessary. AI/ML and data analytics will be key drivers of self-adaptation and self-management, but such solutions are still in their infancy and require focused research efforts.

Edge, Mobile Edge Computing and Processing: These approaches require responsive network connectivity to allow "things" and humans to touch, feel, manipulate and control objects in real or virtual environments. Edge processing in the architecture is essential for ultra-low latency and reliability, while the AI processing is transferred at the mobile/IoT device. Research challenges in this area cover open distributed edge computing architectures and implementations for IoT and integrated IoT distributed architectures for IT/OT integration, heterogeneous wireless communication and networking in edge computing for IoT, and orchestration techniques for providing compute resources in separate islands. In addition, built-in end-to-end distributed security, trustworthiness and privacy issues in edge computing for IoT are important, as well as federation and cross-platform service supply for IoT.

3.6 Future and Emerging Technologies

Nano-Things Networking: The many "things" we are interconnecting are progressively extending to the micro level i.e. computational and service elements running on small/tiny and non-intrusive things. Nano-communications will extend the reach of smart control to a molecular and cellular level, with unprecedented impacts in areas including medicine and materials manufacturing. Combating diseases via autonomous nano-machines, ultra-fast degradation of toxic waste, self-healing and self-monitoring materials are among the many visionary applications. Recent research on nanomaterials and nano-network architecture components (nodes, controllers, gateways) are opening new prospects of usage. Despite promising results, there is a pressing need for a more in-depth view and for modelling of the network architecture and communication mechanisms in this field. Critical research challenges include classifying nano-communication paradigms per application scenario, validated application-specific communication channels, solving power supply and battery charging, cost-effective massive nano-node integration, hardware/software co-design, and security and safety.

Bio-Nano-Things Networking: The novel paradigm of the Internet of Bio-Nano-Things (IoBNT) stems from synthetic biology and nano-technology tools that allow the engineering of biological embedded computing devices. A cell can be effectively utilized as a substrate to realize a so-called Bio-Nano-Thing through the control, reuse and reengineering of biological cells' functionalities (sensing, actuation, processing, communication, etc.). Reliable mathematical models and computer simulations need to be developed to capture the peculiarities of underlying biological processes, which have intrinsic non-linearity and noise. Reproduction and mutation pose extra challenges. The main challenges in communication of BNTs lie in the mapping into the classical communication systems, and in the use of tools from systems and information theory with the final goals of modelling and analyzing the main telecommunication characteristics and performance, such as range, delay (latency), capacity and bit error rate. A further challenge for the IoBNT is the interconnection of heterogeneous networks i.e. composed of different types of Bio-Nano-Things.

Quantum Networking: Quantum communication (QC) will play a central role in the creation of the next generation of secure telecommunication networks. It relies on the use of quantum resources to achieve tasks that cannot be reproduced with classical theory and involves numerous technologies, platforms and application. Recommendations on protocols, components and infrastructures require continuous updates. Quantum Key Distribution protocols are currently the most advanced among the secure quantum communication protocols. However, to be competitive with existing security technologies, two main areas of development have been identified, concerning the practical implementation of security and performance (capacity) of QC in applications. Other quantum secure communication protocols should be extended beyond laboratory proof-of-principle demonstrations.

3.7 Platform, Federation, Automation and Deliver

IoT Platforms: IoT platforms require interoperability at multiple levels and a federation of platforms will optimize the use of resources, improving service quality and most likely reducing costs. Research on IoT platforms and integration of the functions of the platforms in the intelligent infrastructure, as well as research on a layer-oriented approach and semantic interoperability in heterogenous systems, are required to address interoperability at all layers. The inclusion of a programmable, software defined network layer is critical for merging IoT and 5G and future architectures.

Emerging industrial IoT applications, Tactile Internet and autonomous/robotic systems solutions will require far faster reactivity at the edges of the networks as it becomes increasingly inefficient to extract insights from the cloud with growing numbers of IoT devices. Research priorities include the development of new open integrated horizontal platforms for mobile edge computing and edge analytics solutions.

Extreme Automation and Real-Time Zero-Touch - Service Orchestration: In a few years, social machines, smart contracts and other types of more advanced interaction will be a reality. Some machines will be indistinguishable from people from the perspective of business processes and interactions, with higher capacity of decisions, the ability to orchestrate common actions, make requests, etc. Future networks will therefore require higher demands on real-time network service management and a high degree of automation. The challenge is how, without breaking overall end user experience. Several topics are to be addressed, including:

- Enhanced policy management including huge data analytics
- Artificial intelligence driven orchestration
- Cloud-native management applied to Network Function Virtualization orchestration

Service Injection Loop: The creation of services should be reinvented for the new digital area. Architectural micro services provide modular, distributed software components that can be deployed in any environment with a standardized infrastructure, allowing distributed applications to be installed on a cloud infrastructure while maintaining maximum flexibility. Research is required into new ways of describing the entire platform in metamodels. This innovation should be driven not only in the network transformation but also in the creation of a catalogue of new services. These services interoperate with platform capabilities and can automatically adapt to the needs of the user, and will involve new business models in pay-for-what-you-use services.

IoT Distributed and Federated Architectures Integrated with 5G architecture and AI: Further research is needed in novel IoT distributed architectures to address the convergence of (low latency) Tactile Internet, edge processing, AI and distributed security based on ledger or other technologies, and the use of multi-access edge computing. Research challenges include serving the specific architectural requirements for distributed intelligence and context awareness at the edge, integration with network architectures, forming a knowledge-centric network for IoT, cross-layer, serving many applications in a heterogeneous networks (including non-functional aspects such as energy consumption) and adaptation of software defined radio and networking technologies in the IoT.

IoT and Artificial Intelligence (AI) Methods and Techniques: AI techniques and methods are necessary for IoT in an edge computing environment to provide advanced analytics and autonomous decision making. AI encompasses various, siloed technologies including Machine Learning, Deep Learning, Natural Language Processing, etc. In future IoT applications, AI techniques and methods are increasingly embedded within several IoT architectural layers to strengthen security, safeguard assets and reduce fraud. Research challenges overlap with topics identified earlier in this summary but it is worth mentioning AI-IoT integration subjects at the "edge" such as new energy- and resource-efficient methods for image recognition, edge computing implementations (neuromorphic, in-memory, distributed), distributed IoT end-to-end security, swarm intelligence algorithms, etc.

3.8 IoT Applications, User Experience

Digital Twins for IoT: Digital twins are virtual representations of material assets. While current solutions for IoT platforms have mainly been for the representation of physical objects, features such as simulation, manipulation and optimization are missing. Digital twins can be used, for example, to trigger and simulate threat scenarios, and help to optimize the security strategy to handle such scenarios if they occurred in the real world. Research is needed to address the Integration of IoTsdigital twins Into IoT/5G industrial platforms.

Tactile and Industrial-Tactile IoT: Research priorities in this area focus on real-time sensing/actuating using haptic interaction with visual feedback, and the integration of IoT systems supporting not only audio-visual interactions but also involving robotic systems to be controlled with a real-time response.

3.9 Privacy, Network and Service Security

IoT Privacy, Safety, Security, and Trust: Security in the IoT is a growing concern, given the increasing penetration of IoT systems in industrial applications and the vast number of nodes involved. Further research is needed on distributed IoT security technologies. Ensuring IoT operating systems are secure and detecting if they have been compromised (attestation) is as important as ensuring that code executed in these environments is reliable and trustworthy. We must be clear about what can be protected in the privacy domain using the toolkit of security, and what has to be protected by other measures e.g. judicial measures against attacks in the content of messages. A further step for IoT applications, beyond security and privacy, is trust. Establishing trust in the technology and in the organizations involved in delivering IoT products and services is essential, and can be supported by appropriate and effective standards. The scale of IoT applications require the concept of trust is scalable as well.

IoT and Distributed Ledger Technologies (DLTs): Further research is required on DLTs integrated with distributed architecture and edge processing to support the regulatory requirements of business/industrial IoT applications and moving from a centralized to decentralized transaction model. Adoption of these technologies faces challenges across scalability, performance and storage. The research challenges include techniques for increased scalability (DLTs and blockchains do no scale as required by IoT applications for use in a distributed systems), solutions for dealing with processing power constraints against requirements, simplifying implementations, and interoperability between DLTs.

3.10 Human and Socio-economic Factors, Regulation and Institutions

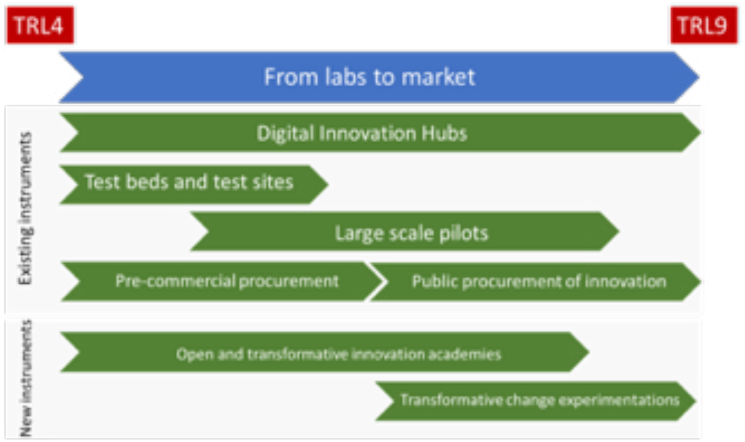
Beyond the technical measures that can underpin IoT and future networks, another critical value driver is that these systems are supposed to act in the interests of society at large and humans in particular. What defines a human-centric digital world and defines socio-economic success is a dynamic often non-rational process. This means research must be conducted from various angles including socio-technical systems and domestication perspectives along with application development and technology adoption processes. This will allow a complementary appreciation of societal opportunities, impacts and challenges, to address how technologies and network services can enable solutions for and impact on specific social challenges. Topics considered must include trust, privacy, education, work/life balance, health, natural resources, environment, climate and more.

Such work will also form the basis of regulations, as these cannot be developed "from behind a desk" but need to be validated in practice. As such, this research should be included in Large Scale Pilots (LSPs) that can form the basis for new, trusted authorities. This will allow studies into how Smart Networks and Services, IoT platforms and applications can evolve as technological innovation systems, interacting with the formal and informal societal and industrial governing mechanisms and institutions that will attend to and regulate the emerging infrastructure. Cross-disciplinary research will strengthen collaboration across our broader community and help to ensure the anticipated socio-economic benefits and a stronger ecosystem development.

Cross-disciplinary research will strengthen collaboration across our broader community and help to ensure the anticipated socio-economic benefits and a stronger ecosystem development.

4. Ensuring Socio-economic Benefits

The Smart Networks and Services Partnership will use current best practices (H2020) and organize new implementing instruments to support innovation in various stages of maturity, working with start-ups and SMEs to access new markets. These instruments are complementary, as shown in the figure below [5]:



The partnership will deploy new instruments targeting transformative change, cutting across vertical industries and blurring boundaries.

These instruments will stimulate the emergence of new uses cases, business cases and lifestyles, stemming from cross-disciplinary innovation. They will support deployment and testing of visionary, disruptive applications. This may disrupt existing vertical ecosystems or spur creation of new ecosystems. They will deal with highly uncertain innovation, rooted in the intertwining of technology and society and environment. For that, methodological approaches to support disruptive innovation will be elaborated and applied in innovation ecosystems, involving value creation, new ways of open innovation, data sharing and trust.

The partnership will have a dedicated chapter on the research agenda focused on assessment of social, economic and environmental responsibilities of the smart networks, services and applications. As part of this chapter, methodological approaches for designing human-centred and low-energy consumption systems, recycling and reuse strategies will be created and feed the technological research.

4.1 Building on existing implementation instruments to accelerate business development

4.1.1 Testbeds and test sites

Tests and demonstrations either accessible online from anywhere or a physical site are essential to validate new technologies and solutions, and accelerate their adoption in the market. The 5GIA-AIOTI cooperation will promote the establishment and maintenance of a wide European networks of open testbeds/sites not only for enabling technologies (smart networks) but also for smart services and applications that are aligned with the needs of key industrial sectors in Europe.

Services provided by those testbeds/sites should encompass technical validation, interoperability, conformance and security. Access should be open, transparent and non-discriminatory but also offer a protected and trusted environment to participants in e.g. data sharing. Test beds are instrumental for standardization and interoperability.

[5] IFor more information about TRL's please see here under G: https://ec.europa.eu/research/participants/data/ref/h2020/other/wp/2018-2020/annexes/h2020-wp1820-annex-ga_en.pdf

4.1.2 Large-scale pilots

Large-scale pilots (LSPs) test technologies and services in close-to-operational environments, involving stakeholders from the integral value chain (including end users) in real business cases. A large-scale dimension must be understood in terms of geographical coverage, number of users, number of devices, volume of data, etc. and with an emphasis on linking multiple vertical domains. LSPs specifically include non-technical aspects such as business cases, acceptance, trust, cross-border issues and scalability. They serve as the breeding ground for lasting partnerships. While many LSPs are not designed to continue after the duration of Horizon2020 projects, we believe that future LSPs should be, supporting continued development and commercialization of results.

4.1.3 Digital Innovation Hubs (DIHs)

DIHs ensure that all companies in Europe, regardless of their size and technical level, have access to and can realize benefits from digital technologies. Services include access to infrastructure for (disruptive) technology testing and proof of concept, access to funding both private and public, training in digital skills, expertise on business model design, and market intelligence. DIHs have a local or regional dimension, and thus are instruments for ensuring take-up of digital technologies in the real economy. In the context of the 5GIA-AIOTI cooperation, DIHs will serve local SMEs as the access point to understand the benefits from Smart Networks and Services, gain hands-on experience with those technologies and solutions, and receive advice on their use/integration with own products and/or business models.

4.1.4 Pre-Commercial Procurement (PCP) and Public Procurement of Innovation (PPI)

PCP and PPI are public-private cooperation instruments where the public sector acts as an early adopter from the demand side, requesting to the private sector the development of innovative tech-based solutions for solving specific needs in public services. Through this cooperation, the public sector and society in general obtain a direct benefit from the improvement and modernization of public services, whereas the private sector gains a first customer reference. There are numerous sectors where Smart Networks and Services are called on to support or enable public services and so would be strong candidates for PCP/PPI: healthcare and assisted living, smart cities, smart buildings, smart energy, etc.

4.2 Implementing new instruments to support societal transformations

Technology will play a key role in the transition towards a sustainable low-carbon economy. To achieve this, technological innovation has to be embedded in social and organizational innovation and accompany a change in lifestyles.

4.2.1 Open and Transformative Innovation Academies

These are spaces for multi-stakeholder collaborations across various disciplines and backgrounds to solve urgent societal and environmental challenges, where technological innovations and disruptions are drivers. The academies will organize and facilitate new forms of engagement and collaboration between diverse stakeholders in a wide range of capacities such as entrepreneurs, legitimators, intermediaries, citizens and consumers.

4.2.2 Transformative change experimentations

Building on the backbone of large-scale technological deployments and infrastructures, the transformative change experimentations will set the pace towards shaping new production structures, user environments and markets in which new types of demands and use preferences will be dominant. Such socio-technical system experiments will cover technological innovations deployment along with transformations in skills, infrastructures, industry structures, products, regulations, user preferences and cultural predilections.

4.3 Social, economic and environmental responsibility of research

Historically, the social, economic and environmental aspects of technology research were subjects for "other" researchers, to be addressed in other disciplines. But a human-centric approach to digitalization, the Internet of Things and Smart Networks and Services requires technology research to become human centric. The 5GIA-AIOTI cooperation will proactively address this and propose that technology research programs be augmented with social and economic scientists to have, for example, early stage considerations on impacts on jobs, health, environment and inclusion.

5. Technical Standard Areas

Since architecture, standardization and interoperability will play a critical role in establishing a successful IoT ecosystem based on smart networks, this section provides an overview of important topics and challenges in key standards areas.

IoT Essential Characteristics: The Smart Network architecture will be software defined and enabled by 5G and IoT, providing features that go significantly beyond traditional connectivity. New architectures, standards and interoperability solutions will have to be developed.

Artificial Intelligence and Edge Computing: Applications and services are enabled by IoT, 5G, AI and computing at the edge. This triggers the need for standardization support in the areas where data and information is exchanged between edge and cloud computing resources.

Approaches to IoT Interoperability and Standardization: The role of standardization in interoperability solutions is key. The value that IoT can provide will be based on agreements that enables the interoperability of systems across domains, creating a network effect. AIOTI will continue to drive the convergence of standards and has published several papers on interoperability and standards

IoT Platforms and Interoperability: IoT platforms, architectures and protocols were developed during the last five years. There are currently more than 1,000 IoT platforms available to develop IoT systems but none are the de facto standard. A multitude of such platforms co-exist and are distributed over various physical infrastructures, dedicated to different geographic areas, services or providers. The challenge is to connect these platforms so they can communicate and exchange information.[6]

IoT Identification Technology: An identifier system must be developed/selected from those available in order to identify each device in a unique way. In addition, there should be no limitation on the number of devices that can be connected due to the lack of identifiers. The number of identifier codes must be large enough to accompany all current and future devices.

IoT Architecture Technology: Various means can be used to achieve interoperability, including models, definitions and well-defined vocabularies that have to be agreed by IoT stakeholders to ensure a common understanding about the concepts. This is also a preamble to standardization. AIOTI has developed a High Level Architecture (HLA) for IoT.

Semantic and Syntactic Interoperability: Semantic interoperability is achieved when interacting systems attribute the same meaning to an exchanged piece of data, ensuring consistency of the data across systems regardless of individual data format. Semantic interoperability must be supported in order to exchange not only data but also information and features related to the source of the information (e.g. location, status, technology associated) - thereby facilitating the disappearance of the vertical information silos of the heterogeneous platforms that current IoT data lakes represent.

IoT Relation and Impact on 5G: With the introduction of 5G, vertical industries will embrace digital transformation, to move beyond traditional service approaches, on an unprecedented scale. This will be a new engine for economic growth and social development. A core element of 5G IA/AIOTI cooperation will be identifying the key requirements imposed by vertical industry sectors to anticipate relevant trends in IoT use cases and apply the knowledge gained to define their impact on the 5G architecture and features.

Standardization of Combined/Integrated ICT and Operational Technology (OT): Enabling technologies like 5G and IoT, edge computing and artificial intelligence are needed to support vertical industry enabled smart networks. Currently, there is a strict division on standardization focusing on ICT (Information and Communication Technologies) and that focusing on OT. Maintaining this separation makes it challenging to provide integrated standards for the ICT/OT needed to support vertical industry enabled smart networks. The 5G IA/AIOTI cooperation should therefore investigate and promote combined/integrated standards for ICT and OT.

6. Afterword

A European Digital Society that brings welfare and wellbeing for all, and includes all, will not be accomplished by siloed programs that are made up of independent technology projects.

Not only is a strong orchestration required to link the individual technology building blocks into a viable working system, but a more integrated approach across the entire value chain in vertical application domains is called for. This includes many non-technical aspects such as business models, trust, liabilities and involvement of end users.

We need to consider many different application domains ("verticals") with unique domain knowledge, language, processes and interests.

These value chains are too long and too complex to manage in a single organization, and collaborative partnerships along the chain can make all the difference: "separating concerns" and building on expertise while bringing stakeholders with very different interests together to help secure sustainable value creation for all.

That is why 5G IA and AIOTI are proposing a value-led, forward-looking program for transformative technologies under Horizon Europe: Smart Networks and Services. The aim is to support the development of ambitious Internet of Things technologies and solutions to address known and as-yet unknown advanced societal needs: building on the strengths of both organizations to help enable a huge variety of new and improved applications and smart network solutions to deliver socio-economic benefits in the public and private sector alike.

August 2019

[6] Several IoT platform interoperability solutions have been proposed, see EC H2020 Create-IoT, EC H2020 AUTOPILOT.

5G IA
INFRASTRUCTURE ASSOCIATION

Alliance for
Internet of Things
Innovation

5G IA
INFRASTRUCTURE ASSOCIATION

Alliance for
Internet of Things
Innovation