Alliance for
Internet of Things
Innovation

Research and Innovation Priorities for IoT

Industrial, Business and Consumer Solutions

August 2018

AIOTI-20180817/01

Table of Contents

Executive Summary

This document is the product of a collective effort to describe, identify and collect research trends and to define innovation challenges in areas relevant to the Internet of Things (IoT) and the Industrial Internet of Things (IIoT), both in daily life and in industrial contexts. Its aims are to evolve current research technologies and to incentivise industrial adoption in order to provide the elements needed to address emerging challenges, prepare for IoT digital-market transition and support further advances and IoT services.

Contributions from the AIOTI WGs comprise the basis of this document, which presents the chief IoT challenges and introduces evolving activities that may inspire future European research, innovation programmes and calls for proposals that will be developed into the Strategic Research and Innovation Agenda (SRIA) document.

The SRIA outlines the guiding principles and identified research priorities for the future while making them accessible to the various stakeholder groups, including policymakers, regulatory agencies, researchers and end users representing both the demand and supply sides and the citizenry.

The SRIA is conceived and generated to direct future research on IoT technologies and applications and to guide development and innovation in Europe. The document sets out specific research, development and industrial-innovation priorities and actions, identifying specific needs and gaps that require action. The SRIA will contribute to the 2020–2027 vision by outlining a full range of research, development and innovation, including a broad spectrum of activities from IoT research to industrial innovation.

The document targets the AIOTI's stakeholders, including industry, academics and entrepreneurs, with the aim for presenting the IoT research and innovation priorities that have been identified for aligning with digitising industry strategy and promoting, circular economy, economic sustainability, growth and job creation.

In this context, the paper addresses the research and innovation priorities for the future IoT technologies and applications that will drive changes across industrial sectors, the European economy and society in general. These priorities include convergence with next-generation tactile/cognitive IoT; decentralised technologies and distributed architectures; IoT knowledge-driven edge processing; artificial intelligence (AI) and trustworthiness.

In past years, the IoT field has evolved rapidly in addressing the grand challenge of developing human-centred IoT technologies and applications, which require high levels of communication and coordination amongst the many competent decision-making authorities, end-user stakeholders and experts in the IoT field. In this context, the SRIA addresses several main themes:

- Defining a human-centric approach
- Addressing societal needs and creating awareness
- Digitising IoT industries and defining market needs
- Sustaining and extending the European IoT space
- Defining IoT industrial leadership
- Developing IoT-driven energy efficient technologies and solutions
- Establishing a cyber-security strategy for safeguarding IoT technology
- Ensuring safety, security, privacy and trust in IoT technologies and applications
- Prioritising IoT research, testing capabilities and education

All of the above have been discussed and selected as a result of consultation amongst various stakeholders, research groups and industrial organisations.

The first priorities for IoT research and innovation in the next years are in the areas of IoT distributed architectures, edge computing, end-to-end security, distributed ledger technologies (DLTs), AI and the convergence of these technologies. IoT and edge computing will see innovation and wide adoption in both consumer and industrial IoT, enabling better security practices and reducing connectivity costs. As IoT technologies are increasingly adopted, more and more devices will be connected to IoT applications, and, as the network expands and the volume of data increases, more information will be at risk.

An increased use of IoT must be accompanied by new distributed architectures and end-to-end IoT security. In order to identify and thwart data breaches, layered machine-to-machine authentication, new human biometric logins combined with AI, machine learning and high-performance analytic techniques must be implemented.

In this context, the convergence of connectivity, IoT, edge computing, AI, and DLTs will be essential to next-generation Internet applications and advancements.

The themes presented in this paper still need to be addressed in greater detail to improve the European IoT ecosystem's sustainability and to address human wellbeing, in particular for developing safe, secure and trustworthy IoT technologies.

1. Introduction

IoT/IIoT technologies and applications are developing quickly, and a vision of the future integrates the full IoT stack [14] in everyday solutions. As result, a combination of connected devices, connectivity, software, platforms, partners, various stakeholders' data and apps, aligned with business goals and a human-centred approach, is expected to emerge not only in industrial markets but also in home and consumer markets. In recent years, we have witnessed an explosion in the number of IoT/IIoT solutions and products in the consumer market, each of them with its associated IoT platform(s) and most of them with proprietary (silo) application(s) and/or service(s).

The IoT has entered the next stage of development, bringing value, convergence/integration and IoT-enabled platforms along with a broader business vision of the IoT as a combination of connected devices, connectivity, software, platforms, stakeholders, information and apps in an integrated IoT ecosystem.

IoT technologies and applications have been moving toward a network of intelligent objects with social capabilities that must address interactions between autonomous systems and humans. IoT technology coupled with AI can provide a foundation for improved and, eventually, entirely new products and services. The powerful combination of AI and IoT technology brings new challenges in addressing distributed IoT architectures and decentralised security mechanisms.

The European Commission (EC) has played a dynamic role in enabling high-quality research in the IoT field since the creation of the Internet of Things European Research Cluster (IERC), where overall horizontal research activities were addressed to create a critical mass of knowledge for Europe regarding the IoT. Subsequent initiatives include the Internet of Things European Platform Initiative (IoT-EPI), where vertical solutions were aligned to define, identify and develop blueprint platforms for Europe; the IoT European Large-Scale Pilots Programme (IoT-LSP), concerned with major European ecosystems in the most relevant economic areas, which today continues expanding to other domains; and recently the IoT European Security and Privacy Projects, which address overall security and privacy gaps.

The numerous European initiatives and their outcomes in the form of hardware/software solutions, platforms, services and IoT solutions have inspired not only other researchers but also industries to launch their own products and solutions in various industrial sectors and economic markets. Existing IoT platforms and their products are expanding to the consumer and/or industrial market with the objective of generating their own ecosystems and a supporting model for sustaining those ecosystems.

The Alliance for Internet of Things Innovation (AIOTI) is developing and supporting dialogue and interaction among various IoT players in Europe. The overall goal of the AIOTI is the creation, expansion and nurturing of a dynamic European IoT ecosystem to unleash the potential of the IoT.

2. IoT Technological Research and Innovation

The IoT area is growing rapidly and the IoT technology continues to evolve at an incredibly speed. Every day the IoT is more societally accepted by its potential and extraordinary driving force towards enabling the digital market and thus, it is expected that sooner than later the IoT will be immerse not only in industrial environments but in our daily personal and work activities. The IoT is today seen as the disruptive technology enabling new opportunities to innovate and create new technologies, developing new services and put in the market new products. In the short future those emerging opportunities will be business success in industry and consumer markets.

Societal challenges, IoT technologies and applications

IoT solutions and its applications shall be understood as the modern tooling to incentivize the current industries and entrepreneurs to transform the current deployed systems into a networked and connected model, the challenge is that IoT requires new legal frameworks and research programs due that it cannot be managed with the current policy frameworks and research programs, a vision of top bottom approach.

IoT technology can be seen as a layer of connected infrastructure and data generation support, as possible accessible to everybody and enabled to interconnect different technologies, an infrastructure prepared for on-demand services and with a pay-as-you-go economy model, in this way promote more budgeting participation in the IoT ecosystem, a vision of bottom up approach.

The IoT applications are the link amongst those different approaches where top down and bottom up converge to provide a set of useful particular services, in the longer term the IoT applications shall be the ones that act as the main outcome and linkage between the societal challenges and the IoT technology progress, first as a demand for managing better the societal services and second as breakdown in managing technology development in an socially inclusive way.

Expected grow for IoT business until 2027

IoT is defined as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities using intelligent interfaces for seamlessly integrating into the information network. In the IoT, 'things' are expected to become active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment by exchanging data and information 'sensed' about the environment, while reacting autonomously to the 'real/physical world' events and influencing it by running processes that trigger actions and create services with or without direct human intervention. Interfaces in the form of services facilitate interactions with these 'smart things' over the Internet, query and change their state and any information associated with them, considering security and privacy issues.

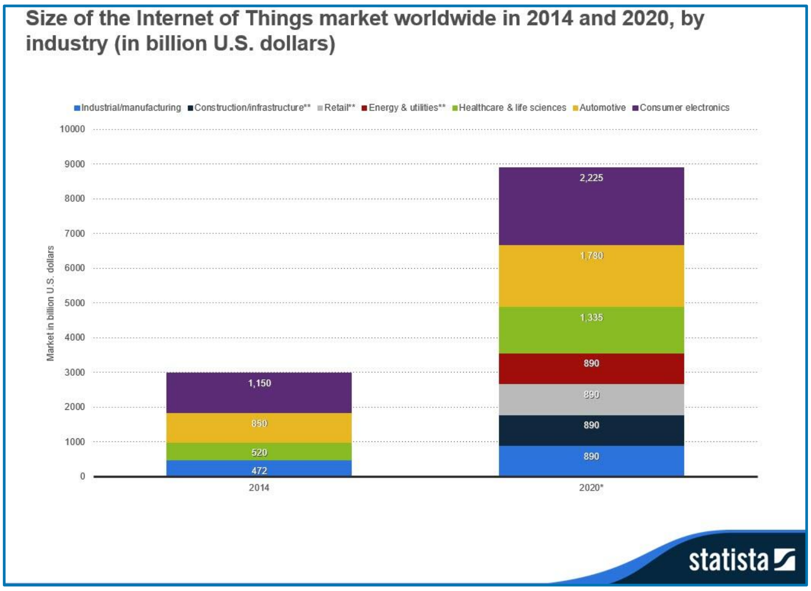


Figure 1 Size of the IoT market worldwide in 2014 and 2020, by industry (in billion U.S. dollars) (Source: Statista)

Recently in 2018 ReportLinker mentioned that the IoT market is expected to grow from USD 170.57 billion in 2017 to USD 561.04 billion by 2022, at a Compound Annual Growth Rate (CAGR) of 26.9%.

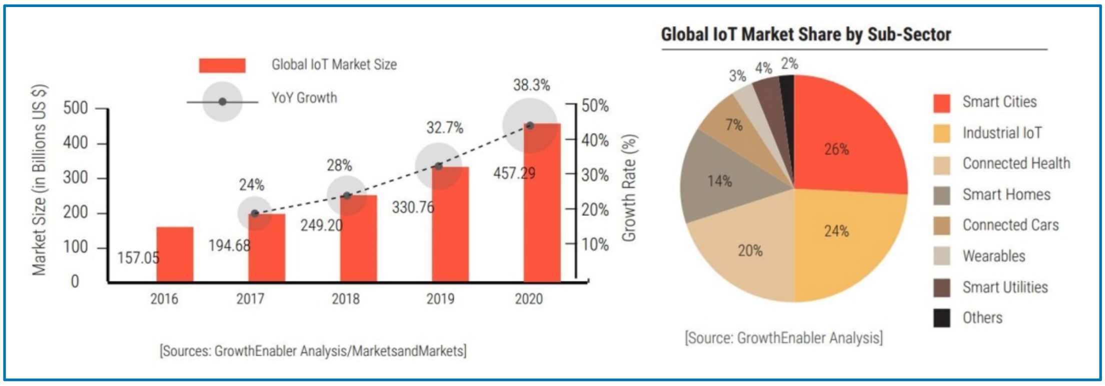


Figure 2 Market Pulse Report, Internet of Things (Source: GrowthEnabler)

The report considers 2017 as the estimated year for the study and the market size forecast is done from 2017 to 2022. As announced back in 2010 by Statista, the global IoT market was projected to grow from $2.99T in 2014 to $8.9T in 2020, attaining a 19.92% Compound Annual Growth Rate (CAGR). Industrial manufacturing is predicted to increase from $472B in 2014 to $890B in global IoT spending. Healthcare and life sciences are projected to increase from $520B in 2014 to $1.335T in 2020, attaining a 17% CAGR these two reports reflect in common the fact that there is a continuous global growth.

IoT represents a network made up by billions of heterogeneous physical devices, such as smart meters, smart locks or wearables, connected to the Internet.

These devices collect and share data about their surrounding environment to favour automation and optimisation of different tasks related both to people's daily life and to industry.

The adoption of the IoT will enable new opportunities to innovate and create disruptive technologies, services and products with a high impact in the future of industry.

Accordingly, the automation demand of IoT connected devices will increase across the industrial domains, so that these devices are been developing with partially or fully robotic layers that will connect humans, things/machines and businesses. In this sense, such layers will make use of interfaces based on new IoT technologies that include AI-enabled mechanisms, modules and systems.

The IoT platforms development will move to the next phase with the emergence of Tactile Internet and the intelligence at the edge, creating interactive, conversational IoT platforms with new user interfaces to engage with things and humans. This will create real-time control, physical (haptic) experiences, interactive, context aware, event-driven IoT ecosystems with intelligence at the edge, where the applications combine edge computing, the IoT and mobile autonomous systems using AI technologies as functionality enablers. In this sense, the proliferation of IoT solutions imply the development of these novel platforms that will cope with the limitations of sensor/actuation devices and mobile devices, by offloading computing complexity onto the network. The computing abstractions can coexist, and novel intelligent, dynamic and holistic coordination strategies are needed, above all considering highly connected scenarios after the 5G adoption and the potential appearance of new computing models.

According to this perspective, main research topics will be:

- Efficiency improvements in energy management and power consumption systems.
- Develop new distributed architectural paradigms at the device and system level to include neural processing units and AI and distributed ledger-based architectures for edge devices that allow parallel processing with ultra-low power consumption.
- Alleviate processing and storage issues of emerging IoT deployments in a ubiquitous way through intelligent coordination among planes.
- Development of new microcontrollers supporting advanced and complex AI and edge computing for IoT applications including deep learning inferences (e.g., related to energy savings, smart home or smart surveillance).
- Integration of IoT solutions for real-time, image, pattern, voice, object recognition, analysis, deep learning, integrated processing, storage and communication capabilities.
- Reduce the bandwidth used by IoT devices to carry out their communications to avoid network overloads.
- Support the inherent dynamicity of mobile and highly connected environments, supporting the change of processing needs, network capabilities, service requirements or number of users.
- Assess the security risks and propose countermeasures to guarantee the correct operation of this orchestration (e.g., authentication mechanisms, data encryption).

Furthermore, research topics must consider certain aspects inherent to IoT environments, which are detailed in the next sections.

2.1. IoT Enabling Technologies

Identification Technologies

The IoT applications require "things" that are identifiable when offering services, interacting with other "things" and humans or updating the information in real time to the "digital twin".

The things can be required to be uniquely identified, or to be identified as belonging to a given class. The identification methods today use methods to physically tag the things by means of passive/active wireless/optical devices (i.e. RFIDs, QR code, etc.) or by providing the things with its own description and identity. The identity in the case of IoT wireless devices is communicated to other devices, IoT applications or services as part of the interactions in an IoT application and IoT platforms.

The analysis of the identification needs and related standardization for IoT are important topics for future development of IoT technologies and applications. Research and innovation in the area of IoT identification technologies are recommended considering the convergence of technologies such as IoT, DLT and AI using new distributed architectures.

Energy Efficiency

As energy is limited, it is of utmost importance to utilize it efficiently considering the exponential increase of interconnected "things". Efficient power conversion with IoT based energy management is one key element herein. Energy-efficiency requirements must be applied not only to energy generation and conversion, smart sensors/devices and appliances, but also to gateways, antennas and edge/cloud computing farms. Together with methodologies like Life Cycle Cost (LCC) and Life Cycle Assessment (LCA), this will improve sustainability at large of IoT environments deployed for environment applications including smart farming applications.

The deployment of IoT in many industrial applications is being hindered because of power limitations, either because electricity is not available in the surroundings, or because replacing/recharging batteries is simply too inefficient or inconvenient. Therefore, enabling of numerous industrial applications will only be possible by significantly reducing the dependency of IoT devices from external power sources. This way:

- New approaches to increase autonomy of self-powered devices need to be devised.
- Advances in battery technologies with special focus on ultra-low leakage, long-term energy storage and increased capacity need to be accelerated.
- Energy harvesting techniques based on vibration, thermal gradients, solar cells or wireless charging should be explored, as well as ultra-low power and efficiency increase in microcontrollers and sensors.
- Energy-efficient requirements must be applied not only to smart sensors/devices and appliances, but also to gateways, antennas and edge/cloud computing.

The impact of the network standby energy consumption of connected IoT devices on worldwide annual energy consumption is expected to be significant and research is needed on energy efficiency techniques, algorithms and architectures across all the layers of the IoT layered architecture, from edge devices, communication protocols, processing algorithms, storage techniques to analytics and IoT platforms at the edge or in the cloud.

Multi-disciplinary research is needed for highly integrated devices that include new energy sources, storage, energy harvesting, sensing/actuating, communication, processing, data storage technologies and energy efficiency algorithms for IoT applications.

Power Management

It is not feasible to replace the sensors' battery frequently, not even recommended in wearables, medical devices and monitoring environments for various IoT applications. The wearable health and care sensors need to be energy efficient for long-term monitoring. Therefore, their lifetime is crucial, and it highly depends on transmission among sensor nodes and energy consumption. To minimize the impact of this issue, there are sensors and actuators with embedded energy harvesting technologies that can effectively increase the running time of the ambulatory devices. Energy-harvesting technologies with power management ICs eliminate the need for batteries by using power generating elements such as solar cells, piezoelectric elements, and thermoelectric elements to convert light, vibration, and heat energy into electricity. These technologies can be developed since semiconductors have achieved a balance between the improving performance of power generating elements and falling power consumption of active devices. Hence, power management ICs designed for energy harvesting, as well as low-power MCUs, will help advance the growth of the IoT in wearables and medical/healthcare, wellness environments for various applications, allowing less constraints therefore a better acceptance of IoT based services.

Configuration and Orchestration

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. The distribution of configuration and updates to devices has already been studied, but there is still much room for improvement in how to orchestrate the operation of semi-autonomous nodes to provide higher level functions. To achieve the full functionality expected of an IoT system, research should be done in advanced network reorganization and dynamic function reassignment.

Operating Systems and Software

Further research is needed on the development of software for parallel processing and distributed architectures. As more and more processing capacity is pushed to the network edges (to gateways and intelligent devices), the devices that used to run without an OS are embracing new OS implementations develop for IoT considering the AI and distributed security features.

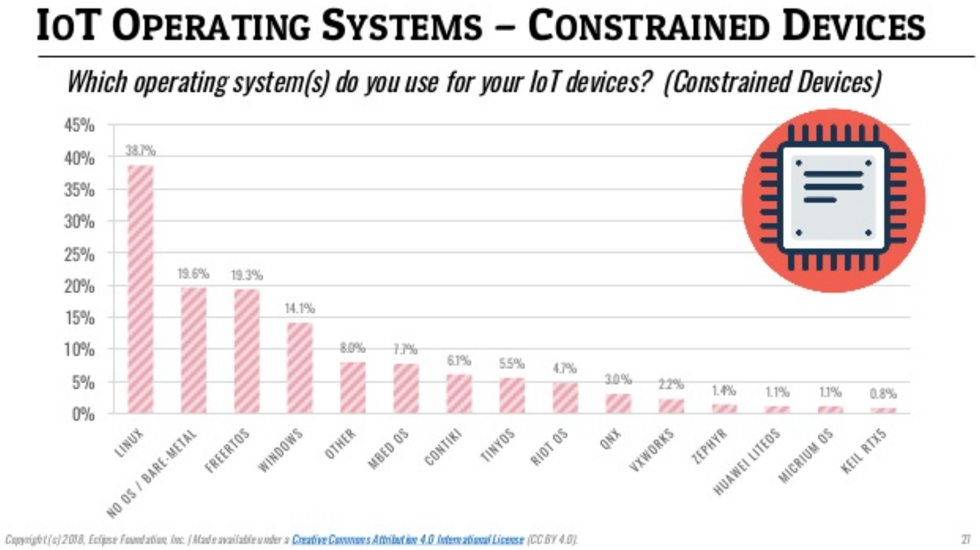


Figure 3 IoT operating systems

In this way, the IoT distributed OSs evolve from embedded OS by addressing the extra constraints through the integration of new technologies.

The OSs use for IoT requires several features that include the capabilities to be embedded and real-time. Using real-time operating system (RTOS) and IoT devices data can be processed without buffering delays, while the RTOS include the ability to multitask, to schedule and prioritize tasks, and to manage the sharing of resources among multiple tasks.

Development on IoT operating systems such as RIOT OS, Contiki, Zephyr, Mbed, TinyOS, Ubuntu Core, MyNewt, LiteOS, Fuchsia OS, FreeRTOS, Nano-RK, Azure Sphere OS etc. requires the integration of new features to address the development of the IoT devices.

Mobile Edge Computing and Processing

Mobile edge computing and processing requires responsive network connectivity to allow things and humans to touch, feel, manipulate, or control objects in real or virtual environments using haptic interaction that allows real-time control and automation of dynamic processes in such areas as industrial automation, manufacturing or traffic management. The research requires the move from centralized solutions to a more localized, distributed real-time form of data holding and crunching addressing multi-access edge computing for heterogenous and distributed IoT systems.

A new computing model – edge-cloud computing – is currently evolving. Three major constraints are driving this trend. Data is increasingly produced at the edge of the network, which creates this model based on data-processing at the edge of the network. The privacy protection requirement will pose an obstacle for cloud computing in IoT.

And most of the end nodes in IoT are energy constrained things. The wireless communication module is usually very energy hungry, so offloading some computing tasks to the edge should improve energy efficiency.

This feature makes the cloud computing paradigm unsuitable for a smart home. One of the specific benefits edge computing offers is the collaborative edge e.g. the opportunity for stakeholders to share and cooperate data across a predefined service interface composed of complex services for end users.

The gateway system will adopt AI technologies to assess the safety, security and environment of the home and control the smart devices to provide the occupants with better services. The AI technologies implemented in the gateway will allow the smart devices in the smart home to be controlled to adjust the home environment according to the occupants' requirement.

Edge intelligence towards no explicit user interface, as IoT makes manual data input largely obsolete and machine learning, and AI take over decision-making, user interfaces are no longer required.

However, human machine interaction mechanisms are still needed. In this sense, mobile edge computing makes possible user-friendly, intuitive and personalized multimodal interaction mechanisms (that is, adapted to the people individual profile) and context aware solutions, adapted to the situation, are emerging to facilitate a seamless communication between people and automation/automation applications trying to compensate possible limitations and favour better use of resources.

These multimodal interfaces are promoting the interaction of humans and autonomous systems to take advantage of mutual strengths and introduce new challenges that must be addressed (e.g. autonomous robotics systems interoperating with humans in scenarios with growing levels of complexity and security demands).

Among others, people inevitably have a variable range of physical and psychological preferences and abilities that can influence in their performance and reactions when interacting with the automation mechanisms.

IoT technologies will then provide the necessary context awareness, supported by a wide range of AI technologies, where knowledge representation (environment and people profiling), reasoning capabilities (personalization issues) and incremental learning (learn by use) are key enablers.

Next Generation IoT Devices

The capabilities provided by the micro and nanotechnologies will allow the development of a new generation of IoT devices with higher levels of integration (including processing power and higher embedded storage capacity), miniaturization, low power consumption, more embedded functionalities including AI capabilities, machine learning, smart actuators and smart sensors fusion at reasonably lower system cost (so they can be widely adopted even by users with limited financial capacity). Advances in this direction will enable new monitoring applications (e.g. at crop-level in the field for precision agriculture, or at product-level traceability) where the size of IoT devices is a limiting factor, will provide low-cost IoT devices easier to deploy, and facilitate the transition from cloud-based IoT analytics to distributed (i.e. in devices) analytics, thus increasing responsiveness to events, scalability and system resilience.

Besides, one key factor for the success of IoT adoption depends on the ability to provide added value components for example integrating new devices (sensors, light sources, displays etc.) to expand the functions of the devices. Despite this can be performed through conventional electronics, flexible electronics (organic, printed or hybrid flexible electronics), which are lighter, thinner and have a lower power consumption, will allow for better fulfilment of the requirements (less weight products, higher flexibility for aesthetic design, component cost, etc.). So that, flexible electronics are much more appropriate to be integrated into final products thanks to their conformable characteristics that can be adjusted to the shape of final product structure, providing the industry the opportunity to create multifunctional components in large-scale fabrication as well as giving more scope to the aesthetical designers. Wearables (shape body adjustments) and industry and manufacturing (integration of electronics in the manufacturing processes of the CPS) are some of the multiple examples of domains that can be benefited of the inclusion of flexible and hybrid electronics.

2.2. Sensing and Actuation IoT Technologies

The intelligence and value from an IoT system is based on what information is collected at the edge, how the information is connected and processed and what applications and services are generated. Sensors are the source of IoT information while actuators are acting based on the data processed.

Sensor and actuators technologies are driven by new innovations in materials and nanotechnology, by developing devices with increased accuracy, decreased size and cost, and the ability to measure or detect things. The physical world at the edge requires many different types of sensors to measure different types of parameters such as flow, temperature, voltage, humidity, gases, light, pressure, etc. and different actuators to act on the environment. There are multiple ways to measure the same parameters, while different applications call for different ways of measuring the same thing.

Smart homes are equipped with environmental and physiological sensors and actuators that facilitate remote monitoring of the home environment (e.g., temperature, humidity, smoke…) including vital signs (e.g., heart rate, body temperature, blood pressure…). In addition, these devices also allow to monitor human activities in a wearable platform by using small, simple to use and low-power devices such as accelerometers, gyroscopes and magnetometers. Indeed, wearables, mobile and connected devices can help to manage conditions outside of a health facility. Hence, they can also communicate with the remote healthcare facilities and caregivers, thus allowing the healthcare personnel to keep track of the overall physiological condition of the occupants and respond, if necessary, from a distant facility. This is particularly adapted to the needs of elderly, who require prevention and emergency management.

Accordingly, there are several sensing technologies that enable significantly this transformation. In particular, "Time of Flight" cameras, providing for instance gesture and user detection, are bringing new use cases into different domains IoT. In addition, they are also bringing new possibilities in the field of interactions between a machine and humans, bringing another level of smartness in living environments. In this sense, note that other motion detectors, such as passive infrared sensors, can be used to detect the location of the subjects in the house. On the other hand, voice first devices will allow us to interact with our devices the same way we talk to one another. We entered in the "Voice first revolution" - with new familiar wake phrases including "Hey, Siri" "OK, Google," "Hey Cortana," and "Alexa" to voice-enabled platforms in the form of smart speakers and will end up in Voice First platforms - basically no interface - with a crucial importance of Voice Analytics. Finally, the first field tests related to sensing technologies are using sensor fusion – augmented hearing, motion sensing, gesture and pattern recognition, etc. with embedded AI.

2.3. IoT Connectivity Technologies

The connectivity in IoT networks needs to be the 'always on' type as applications, and in many applications will require continuous, uninterrupted connections to effectively capture and communicate data in real-time. To carry out such data communications, the adoption and further development of low-power wide area network (LPWAN) technologies like Sigfox, NarrowBand IoT and LoRa MESH networks is required, for data transmission with high efficiency and low power consumption. Satellite IoT solutions are frequently the best or only options for remote and rural locations not served by any terrestrial communication networks (or where their deployment is not cost-effective), or areas where no easy network roaming is available. However, current satellite systems do not fully fulfil the "low-cost, low-power, small-size" criterion and, in some cases, they simply act as a backhaul for terrestrial networks. Effort needs to be made to solve challenges related to the cost and complexity of terminals and antennas, the use of non-GEO (LEO and MEO) satellites, the scalability of the network, the reduction of power consumption and the interoperability with terrestrial LPWAN networks.

Other aspect to be considered by communication technologies is mobility of devices in certain IoT environment. In this sense, further support is needed from LPWAN technologies to offer a reliable communication link when monitoring mobile devices. New scenarios such as Internet of Vehicles (IoV) should be considered, where the IoT paradigm is used in mobile devices or even mobile environments such as a whole bus. In these cases, it has been detected that LPWAN technologies suffer from high packet loss ratios when the transceiver is moving, due to physical and layer-two issues. Urban mobility applications could require in the future the monitoring of green means of transport such as bikes or skates, and IoT communication technologies supporting moving objects will be a must.

Accordingly, for what we are concerned, IoT communication technologies can be classified into the following three categories:

Short Range

ABI Research forecasts that by 2021, so-called "the age of the IoT", there will be 48 billion devices connected to the internet. Among those 48 billion devices, 30% are forecasted to include Bluetooth technology. Bluetooth Low Energy (LE) has been actively evolving to make it a key enabler of the IoT, especially for fitness and medical devices. In addition, there are other communication technologies, such as ZigBee, Z-Wave, Thread, 802.15.4 and 6LoWPAN. However, their deployment in smart living environments might be rather difficult as interoperability is often not possible due to configuration differences and key management.

Low Power Wide Area Networks

LPWAN technologies provide long battery life, extensive range, are reliable and associated with low costs. No other technology offers these four characteristics in combination. LPWAN fills an unmet need in IoT connectivity. By 2022, most IoT applications will be able to use LPWANs, which will expand connectivity choices. By 2025, according to ON World's Research, there should be 1.3 billion LPWA connections worldwide and NB-IoT will make up over half by this time therefore challenge unlicensed LPWA networking technologies, such as LoRa and Sigfox (5G might still not be widely available at that point). In this sense, number of NB-IoT applications is growing rapidly including solutions for healthcare, smart buildings and wearables such as health monitors and smartwatches that will increasingly compete with short range wireless technologies such as Bluetooth and ZigBee.

Cellular

5G systems will allow to move from algorithms based on static information to those that can be optimized in real-time using data from the user. In addition, they will provide data centres at the edge and the possibility to implement Specific networks enabled by virtualization and software-defined networking principles are developed. By the introduction of 5G systems, it is expected that vertical industries will embrace the digital transformation that will move beyond traditional people-centred service, on an unprecedented scale. This will be a new engine for economic growth and social development, since vertical industries will have an enhanced technical capacity available to trigger the development of new products and services. Enabling technologies like 5G and IoT are needed to support the industry digitization that relies, in several scenarios, on the robust connectivity of trillions of devices and the open sharing of data that will subsequently be generated. Therefore, identifying the key requirements imposed by vertical industry sectors, can anticipate relevant trends in IoT use cases and at the same time can be applied to define their impact on the 5G architecture and features. Identifying the IoT relation and impact on 5G is an important activity and it is recommended that the 5G and IoT convergence is the key enabler for the digital transformation and therefore must be addressed.

2.4. IoT Platforms

IoT platforms can coordinate and manage connectivity issues, and to guarantee the security and privacy of the data exchanged, by many networked devices while overcoming interoperability issues. The use of a pre-defined set of protocols to share certain services, a federation of platforms will allow optimizing the use of the resources, improving service quality and most likely reducing costs. IoT platforms address both technological and semantic interoperability issues among heterogeneous IoT devices and need to minimize the complexity of collecting and processing large amounts of data generated in IoT scenarios.

The IoT platforms need to address scalability, security issues and guarantee that the developed solution is built upon commercial or open-source software based on open specifications that allows portability and reduce product development costs, while encouraging creativity and collaboration among the various IoT stakeholders. IoT platforms need to provide solutions to assimilate data from multiple vendors and support open API interfaces across platforms. This requires taking into consideration issues such as openness, participation, accountability, trust, security, privacy, effectiveness, coherence, etc., while offering innovative solutions that enable self-governance, self-management, and context aware scalability.

Communication between nodes of IoT platforms is one important future challenge for IoT technologies and applications. To draw a parallel – equivalent to X2 interface in 4G (or Xn in 5G). Typically, data exchange between two nodes in IoT systems is going via hierarchically higher nodes, and (as in move from 3G to 4G) we could benefit on decreased latency is horizontal link between those nodes is possible. If those two nodes are belonging to different IoT service providers, and served by two different slices, everything becomes more complicated. So, security needs to be also supported by design on: "D2D-slice" between nodes, "D2Dconnectivity between slices", and discovery across IoT platforms.

IoT platforms need to be and act as a complete IoT/IT/OT ecosystem converging the consumer/business/industrial applications by collecting and sharing data broadly within an organization, sectors, and IoT applications. This need to be converted into an IoT platform strategy, based on open specifications, strong interoperability principle, security and standardization.

IoT Platforms are key for the development of scalable IoT applications and services that connect the physical, digital and virtual worlds between things, systems and people.

Developing and deploying IoT technologies and applications require using a federation of IoT platforms and a strong IoT ecosystem of integrators, aggregators, service providers, RTOs across various industries. These ecosystems need including industrial, consumer, business stakeholders that enable customers/end-users/stakeholders to create managed services offerings, co-create value (products, services, experiences) based on new business models and exchange data thus unlocking the true data value chain to deploy solution for digital single market.

The research priorities need to support for development of new open integrated horizontal platforms for mobile edge computing and edge analytics solutions. As the number of IoT devices grows, it will become increasingly inefficient to extract necessary insights in the cloud. Emerging industrial IoT applications, Tactile Internet and autonomous/robotic systems solutions will require much faster reactivity at the edges of the networks. To support these requirements, analytics algorithms will have to operate in a distributed context between edges and cloud with heterogeneous capabilities. Apart from the algorithmic, AI and M2M learning advances, this requires much more sophisticated frameworks in place to enable effective synchronisation and adaptability.

2.5. IoT Distributed and Federated Architectures

Further research is needed in the area of novel IoT distributed architectures for addressing the convergence of Tactile Internet, edge processing, AI, and distributed security based on ledger or other technologies and the use of multi-access edge computing.

The IoT architectures have to consider scalability and the impact of latency on haptic control by implementing predictive and interpolative/extrapolative techniques closer to the edge of the network for heterogeneous IoT Tactile applications. This has to consider the existing architectures enabling new possibilities to serve the radio networks and to co-exist with other virtualized network functions. This will need to consider the network agnostic principle, while delivering flexibility, scalability and efficiency to multiple sites using existing interfaces and innovative Ethernet-based or other type of fronthaul. Move from data/driven architecture to new type of concepts.

The development of IoT edge processing capabilities and platforms require that the intelligent nodes at the edge make decisions locally and communicate with more than one external source based on the data collected. Autonomous systems, autonomous vehicles require IoT devices onboard to make decisions in real time, without the support from a centralized compute source.

A distributed IoT architectural model has to consider the distributed edge computing and storage of resources, distributed communication, intelligence, and security.

The combination of decentralized IoT architecture and blockchain platforms could form the framework for facilitating transaction processing and coordination among interacting IoT devices at the edge. The concept of next generation IoT evolves in the direction of decentralized, autonomous intelligent things and distributed platforms at the edge.

2.6. Tactile and Industrial-Tactile IoT

IoT applications that integrate computing at the edge using intelligent IoT devices combining sensing/actuating, AI, processing requires novel mobile communication technologies and IP/non-IP based solutions as enabler for the Tactile Internet, providing throughput and higher capacity, lower latency, ultra-high reliability, higher connection density, while assuring the increased requirements for security, trust, identity and privacy. This allows to provide the convergence of the concept of system of systems with the networks of networks infrastructure for remote physical interaction in real time, that requires the exchange of closed-loop information between virtual, digital, cyber and/or physical objects based on new paradigms as AI (i.e., humans, things/machines, and processes).

The research priorities are addressing the Tactile IoT enabling technologies based on real-time sensing/actuating using haptic interaction with visual feedback, and integration of IoT systems supporting not just audio-visual interaction, but also that involving robotic systems (Internet of Robotic Things - IoRT) to be controlled with a real-time response that require low latency in combination with high availability, reliability and security.

The Tactile IoT development is linked to virtual reality (VR) technology advancing by providing the low-latency communication required to enable shared haptic virtual environments where things are physically coupled via a VR simulation and the things digital twins are interacting.

2.7. IoT and Distributed Ledger Technologies (DLTs)

Further research is needed on DLTs integrated with distributed architecture and edge processing to enable the regulatory requirements of business/industrial IoT applications and moving from a centralized transaction model to a decentralised one by addressing the challenges such as scalability, performance, and storage to the adoption of these technologies. In addition, it is necessary to achieve an alignment with distributed shared architectures to interconnect, authenticate, monetize distributed IoT intelligent "things" at the edge. Distributed ledgers are used to bring transaction processing capabilities and intelligence to devices everywhere.

Distributed ledgers used in IoT applications allow reducing significantly failure points in networks, providing for secure traceability. The use of distributed architectures, cryptographic signatures, smart contracts, identity authentications, public and private permissions, strengthen security of IoT edge devices and applications. Decentralised technologies and distributed architectures allow for intelligent edge devices in the various communication networks to maintain low latency, and high throughput and provide scaled solutions.

It is required to research on blockchain and IoT converging techniques for supporting IoT intelligent devices integrity and IoT device level trust through, device identity, transactions (i.e., secure methods to authenticate and automate the exchange and settlement) and interactions (unique follow up of interactions, events, and updates associated with IoT devices).

Distributed ledgers allow IoT devices to adopt complex forms of computerized interactions, allowing them to process safe and reliable data exchanges. Security, trust, and identity are addressed in a distributed manner and solutions based on blockchain are used to manage data from IoT edge devices, which can use DLT to validate or update communication contracts.

2.8. IoT and Artificial Intelligence (AI) Methods and Techniques

AI encompasses various technologies including Machine Learning, Deep Learning, Natural Language Processing, etc. In the future IoT applications it is expected that AI techniques and methods are increasingly embedded within several IoT architectural layers and create artificial intelligence of things (AIoT) applications. The AI segment is currently fragmented, characterized with most implementations focusing on a silo approaches to solutions. Future trends include solutions involving multiple AI types and integration with IoT and DLTs/Blockchain. AI can be used in IoT to strengthen security, safeguard assets, and reduce fraud. AI techniques and methods are necessary for IoT in an edge computing environment and can be used to provide advanced analytics and decision making. This can be applied in IoT solutions involving real-time data as AI will be used to make determinations for autonomous actions.

The integration of AI-based algorithms at different IoT architectural layers to process IoT data for autonomous decision making creates intelligently interconnected IoT ecosystems that can be combined with new technology (AI, bots, automation, AR/VR) to create cognitive solutions through federated IoT cognitive platforms. The IoT applications Implemented can continually learn, interact, and augment human capabilities and increase the real-time cognition capabilities of machines/things to support the processing at the edge.

2.9. IoT Interoperability

IoT interoperability at different levels considering the new development in the area of IoT horizontal platforms, the convergence of technologies and the use of distributed architectures [16].

IoT platforms require interoperability at multiple levels, which implies finding the characteristic functionalities of each layer and defining meta-protocols that can be mapped on the ones used in the platforms (i.e. on the level of syntactic interoperability, the characteristic functionality is resource access).

Research on a layer-oriented approach is required to address providing tighter interoperability at all layers of IoT systems (device, network, middleware, application, data and semantics) with a strong focus on guaranteeing trust, privacy and security aspects within this interoperability.

This interoperability approach also provides modules covering quality of service (QoS) and device management, service integration, external system services, storage and virtualisation.

Regarding semantic interoperability, current work focuses on defining and standardizing common vocabularies in given domains (e.g. iot.schema.org). Interesting direction is also the effort towards domain-agnostic aspects of any IoT object, following the Web of Things (WoT) approach (with interaction patterns, links and security). However, standardization of models is not always a viable option. Therefore, research should also focus on techniques that enable semantic interoperability even if different information models are used like semantic mapping.

Layered approaches for interoperability allow the stakeholders or platform operators to select the best mechanism for interoperation. Management of such options provides coordination between layers, enhances cooperative solutions (e.g. gateways and network) and enables security management.

With regard to gateway interoperability, the inclusion of a programmable network layer based on software-defined networking (SDN)/network functions virtualisation (NFV) is critical for merging IoT and 5G and following the existing architectures. Using a programmable network has two advantages: management of mobility and management of QoS for massive IoT management. The most promising aspects of a common framework for IoT interoperability are finding common approaches to resource access, resource discovery as well as semantic interoperability.

Further research is needed to address interoperability in the systems-of-systems view where all devices, 'things' and other information systems should be able to interoperate at the level of Internet protocols (TCP/IP, etc.) or even at the World Wide Web (WWW) level (HTTP, WebSockets, etc.). This signifies that lower-level protocols (ZigBee, LoRa, etc.) are abstracted away behind 'wrappers' and services using a limited set of IoT standards [10].

2.10. IoT Data Graphs and Analytics

Data is produced by every IoT device from a simple sensor detecting our presence and an actuator providing a message or activating a door to be opened to a more complex system running expert computing like in economy or stocks markets where the data defines the rise or down of the economic indexes. The elements that make the data so useful and rich are "analysis and interpretation". It is necessary to provide meaning from the data and most of the time transform it into information and then eventually in knowledge enabling intelligence, thus data volume is not all, else to make these data useful.

Data representation has evolved and the use of graphs defining data structures that facilitates the search and access to data is widely used, e.g. in the domain of web services and particularly search engines take the benefits from indexed structured graph data bases. It is expected that IoT benefits from using a distributed world-wide graph data base, where the service benefits are exponential and highly evident, what makes powerful this approach is largely the structure of the data. In IoT the idea is to have relevant and useful information and the structured data and at the same time accessibility to the information using semantic annotation and all its advantages from data structures in the form of graphs.

Analytics today is a capacity, a feature to understand data and the best way to materialize value (including economic) to the data. The big diversity on analytics tools has made the analytics area so rich in vocabulary that today it is even difficult to differentiate if there is one or multiple type of analytics. It is expected that IoT analytics grows making analytics so different and rich full in content in order to improve the performance of IoT systems.

2.11. IoT Privacy, Safety, Security, and Trust

Security in the IoT field is a growing concern, given the increasing penetration of IoT systems in industrial applications. The move to edge, the growth of IoT and AI, and the distributed architectures require new security architectures and concepts. Therefore, further research is needed on distributed IoT security technologies on user (machine/human) - centric end-to-end design while integrating autonomous recognition of identity through machine learning, AI and swarm intelligence.

Today there is a risk "that the European economy is falling behind in its ability to tap into the promising emerging IoT markets due to the lack of trust in smart and connected devices from businesses and consumers" [9]. In this sense, if "security" is a general requirement for IoT systems, is the domain which will draw a special attention as special efforts will be needed.

As in all digitalization, cybersecurity becomes a necessity to be solved. New generation digitalization needs secure exchange of data. If not solved properly, cybersecurity issues may become show stoppers. Networked businesses also bring along hesitations of trust: how can companies in an open-like digital environment trust each other in a constructive way. The whole world is now on fingertips for everyone creating the needs of new business culture, contract bases, legislations, market places, business models, i.e., new conditions for growth and success.

The area of smart living environments introduces several issues related to the security of medical data and the protection of user privacy. On the one hand, user privacy refers to an individual's right to control the collection, use, and disclosure of his/her personal health information and/or personal information in a manner that allows health and care providers to do their work. On the other hand, security is about ensuring the medical information gets to the right person in a secure manner. Thus, the potential issues can be categorized within several fundamental data management concepts, for instance, trustworthiness of data sources, integrity of aggregated data, data privacy, anonymization of data providers, location privacy, etc. In this sense, ensuring strong data encryption, database security as well as secured communication channels is critical for smart living environments.

Furthermore, agriculture is other example, where data captured and managed by IoT devices can have a serious impact in farm operations, insurance services, prices, etc. One of the needs is related to the necessity of ascertaining the validity and veracity of the information and services provided by the IoT devices. Although mechanisms to secure communications and to detect intrusions or potential attacks have already been proposed, additional research is needed to provide mechanisms to verify the correct operation (attestation) of IoT devices in the field.

Ensuring that the 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.

Moreover, safety should be considered from the perspective of developing methods to guarantee that IoT actuators (e.g. in tractors or implements) are providing the right system operation to avoid damage on the field or person injuries due to the automation. Research should go from collaborative systems to fully autonomous safe-by-design systems.

A further step for IoT applications, beyond security and privacy, is trust. Due to concerns and challenges related to security and privacy, the acceptance and growth of IoT applications is hindered.

Therefore, increasing trust in the technology and in the organizations involved in delivering IoT products and services is essential, so that users are convinced to enrol in data sharing initiatives in complex value chains. In addition, this can be supported by appropriate and effective standards.

Accordingly, safety, privacy and security are key aspects that must be addressed by IoT systems, particularly as they are used for automation of processes with impact on people's health and wellbeing, the environment, and the different critical infrastructures (transport, energy, banking, water, etc). It is essential to maintain a human-centred perspective, both in terms of the role of people in the operation of IoT systems and in the impact of these systems on people's quality of life. The classifications of existing IoT security architectures considers seven dimensions: user/human factors, data, service, software/application, hardware, authentication, infrastructure and network. It is recommended that IoT security, privacy and trust are IoT key enabling technologies and that they need to be considered in the future research and innovation programs and calls.

The scale of IoT applications require that the concept of trust is scalable as well. Scaling trust using traditional engineering techniques could be expensive, and difficult to implement. In next generation IoT privacy and anonymity must be integrated into its design by giving users control replaced the centralised solutions with decentralised and concepts such as security through transparency.

2.12. IoT Standardisation

The global dynamics and landscapes of IoT SDO, Alliance and OSS initiatives analysis can be used to leverage on existing IoT standardization, industry promotion and implementation of standards and protocols, as well as to provide a guideline for the proponents of future project proposals associated with future IoT related calls financed by the EC on the positioning of these initiatives within these landscapes.

The value that IoT can provide will be based on agreements that enables the interoperability of systems across domains, creating a network effect. The agreement represents a standard whether it is a formal or a de-facto standard. To be able to utilize IoT information and to derive further information and knowledge, there needs to be agreement on concepts, which can be formalized in the form of ontologies on the semantic level. This is the basis for achieving semantic interoperability. Different syntactical representation of the same concepts can be transformed from one to the other, whereas non-matching concepts or unclear matching between concepts prevent the utilization of information. Thus, a focus should be to build on existing standards, for instance, oneM2M, W3C WoT, NGSI-LD and SAREF, especially concerning the conceptual modelling of information. In addition, gaps need to be identified and effort needs to be directed at filling, contributing to the relevant standardization activities.

It is recommended that the research and innovation support actions that should be defined on key topics, such as safety and cybersecurity, reliability and performance etc. co-engineering, IoT, IIoT, M2M, AI and machine learning, IACS, Transport domains, towards highly automated and autonomous systems of all kinds, to be selected/defined, etc.

A list with IoT standardisation gaps has been provided by AIOTI [2]. This list is also provided in Table 1 and Table 2. It is recommended that actions should be defined that can be used to solve these IoT standardisation gaps.

Table 1 lists several gaps that have been considered in ETSI TR 103 376 [3]. The gaps that are written in bold are considered as being key gaps. More details on the description of these key gaps can be found in [2].

Table 2 shows the results of an assessment documented in [7] and [2] regarding the criticality of the gaps listed in Table 1 which are perceived by 5 EC H2020 IoT Large-Scale Pilots.

Table 1: Main STF 505 gaps and key gaps

Domain	Gaps
IoT Architecture	• Multiplicity of IoT HLAs, platforms and discovery mechanisms
Connectivity	• Fragmentation of the standardization landscape • Large number of heterogeneous & competing communications and networking technologies
Integration / Interoperability	• Global-level standards (international vs. regional level) • Fragmentation due to competitive platforms and standards
Device /Sensor Technology	• Quality assurance and certification • Device modularity
Service and applications	• Data interoperability: lack of easy translation mechanisms between different specific models. Need of a global and neutral data model. Seamless inter-working between data systems • Interoperable processing rules: lack of definition for advanced analysis and processing of sensor events and data to interpret the sensor data in an identical manner across heterogeneous platforms • APIs to support application portability among devices/terminals • Specific solutions at Service Layer to enable communications between the platforms (e.g., plugins to oneM2M platform)
Applications Management	• Usability [Societal gap] • Applications tailored to individual needs: evolution, flexibility of the components • Harmonized Identification • Interoperability between IoT HLAs, platforms and discovery mechanisms

Domain	Gaps
Security / Privacy	• Privacy and security issues can be a blocking factor for user's acceptance and prevent large scale deployments. Security and privacy are addressed on an isolated basis for part of the applications • Lack of highly secure and trusted environments • Liability for data privacy
Deployment	• Safety • Deployment tools
Regulation	• Regulations for frequency harmonization and usage
Business	• Collaboration between vertical domains, siloed applications • Lack of a reference for business cases and value chain model to guide choices for deployment • Lack of knowledge about potentialities of IoT among decision makers, users
Societal	• Green Technologies • Ethics. Transparency and choice for citizens • Not everything should be smart

Table 2: Some standards gaps and overlaps and their perceived criticality, based on [7]

Nature of the gap	Type	Criticality
Competing communications and networking technologies	Technical	Medium
Easy standard translation mechanisms for data interoperability	Technical	Medium
Standards to interpret the sensor data in an identical manner across heterogeneous platforms	Technical	High
APIs to support application portability among devices/terminals	Technical	Medium
Fragmentation due to competitive platforms	Business	Medium
Tools to enable ease of installation, configuration, maintenance, operation of devices, technologies, and platforms	Technical	High
Easy accessibility and usage to a large non-technical public	Societal	High
Standardized methods to distribute software components to devices across a network	Technical	Medium
Unified model/tools for deployment and management of large-scale distributed networks of devices	Technical	Medium
Global reference for unique and secured naming mechanisms	Technical	Medium
Multiplicity of IoT HLAs, platforms and discovery mechanisms	Technical	Medium
Certification mechanisms defining "classes of devices"	Technical	Medium
Data rights management (ownership, storage, sharing, selling, etc.)	Technical	Medium
Risk Management Framework and Methodology	Societal	Medium

The standardisation should aim at categorising IoT products, as one can see in Bluetooth standard evolution.

In this sense to categorise products, a matrix approach could be proposed: a categorisation by profile, and by application, as shown below with some examples.

Table 3: Research priorities categorization by profile

IoT Layers	Requirements	IoT research priorities
Business	Registered as well as unregistered users and devices Full support for autonomous systems Cross-domain interoperability of information and knowledge Inter-city interoperability of public services	Distributed trusted identity management Semantic interoperability (data, processes, functions) Real-time processing Seamless integration of new devices and systems, even unregistered ones Embedded, high-precision location
Data	Privacy and data protection Data openness	Data privacy technologies Data interoperability Anonymization techniques
Computing and platform	Performing of autonomous decisions (e.g., drones) Exploitation of collective intelligence of systems	Analytics and IA in the edge and in the cloud for cooperative systems
Communication and network	Continuous operation Ad-hoc connectivity Underground communications Support for autonomous systems	Wireless, low-power, short-range and wide-range technologies Low-latency, high speed communications
Devices	Recyclable and last for life Wireless power or energy scavenging Upgradeable, reconfigurable Universal, multipurpose	From dedicated systems to multi-functional, platform-type systems (third party, downloaded apps in the device, for instance) End-user programmable Software defined behaviour Natural language processing Virtualized, multi operating systems Energy-efficient processors

The main objective is to have, at first, a standardisation of the communication protocol and then to make appear hardware architecture typologies according to the applications. Depending on the application, the hardware solutions put ahead could be connectivity (wired or wireless), security, low consumption, high integration, lifetime, among other.

3. Application Areas and Industrial Developments

IoT applications application areas are expanding and several industrial domains are investing in IoT technologies and applications. This section further explores the current use state of the art, the technologies and the developments beyond state of the art from the perspective of the AIOTI WGs.

3.1. Healthcare

State of the Art

The healthcare IoT market is all set to hit $117 billion by 2020, while the combined IoT market adds much more than $117. By 2025, it is expected that the maximum value from healthcare would be valued at $2.5 trillion, followed closely by the manufacturing industry at $2.3 trillion. About 30.3% healthcare is designed to portable health monitoring, electronic record keeping, and pharmaceutical safeguards.

New IoT technologies for tele-medical treatment using edge haptic feedback, based on development of new human-to-machine interaction (HMI) real-time techniques including AI and human machine interactions.

Health- and fitness-oriented wearable devices that offer biometric measurements such as heart rate, perspiration levels, and even complex measurements like oxygen levels in the bloodstream are also becoming available. Technology advancements may even allow alcohol levels or other similar measurements to be made via a wearable device.

The ability to sense, store, and track biometric measurements over time and then analyse the results, is just one interesting possibility. Tracking body temperature, for example, might provide an early indication of whether a cold or the flu is on the way.

Standardization is a key limiting factor for application in IoT healthcare systems. IoT solutions state of the art solutions address security, privacy, wearability, and low-power operation Issues.

Technologies

The IoT devices can apply complex algorithms and analysing them so the patient receives proper attention and medical care. The collected patient information needs to be stored both at the edge and in cloud. Through remote monitoring, patients can significantly reduce the length of hospital stay and, even hospital readmission.

Advantages

- Protein research and composition analysis benefits from IoT as researchers can analyse the accuracy of the equipment, and it rewards them by shortening their work-ow through quantitative and reproducible analysis of proteins.
- When large numbers of array of devices are connected, healthcare industry can provide scalable solutions to its patients. In this context, many healthcare apps providing cutting-edge personalized solutions are released to them.

Beyond State of the Art

IoT is one of the technologies that can address the challenges in the healthcare system the population continues to age and is expected that by 2025, 1.2 billion of the 8 billion people on the planet to be elderly, that implies more healthcare issues and increasing costs. The life expectancy rises, and the healthcare costs follow suit.

IoT and portable diagnostics systems can analyse and report the findings of different tests taken remotely without requiring a visit to the doctor's office. This will support the remote caregivers to ensure the safety of elderly people with wearable devices and learn the regular routines of the person who wears the device and issue a warning if something seems outside of normal parameters and behaviour.

For many applications if there is any interruption in the activity of a person, alerts would be sent to the service providers and this require.

3.2. Wearables

State of the Art

Some functions that wearable devices are already delivering are related to identification and security. Some advanced badges even include some biometric capabilities (such as fingerprint activation, so only the badges owner can use it to open a locked door) to improve security.

Badges can also include capabilities for location sensing, useful in emergencies to make sure everyone has successfully evacuated the building. A wearable bracelet provides a more reliable indication of location since it is less likely to be left in a jacket on the back of a chair.

Stare of the art IoT wearable devices (e.g., the Fitbit health monitor, Pebble smartwatch, and Google Glass) are facilitating self-management and self-monitoring and are integrated with electronic health records and office systems by means of sensors/actuators and IoT platforms.

Technologies

New technology developments and sensor/actuators-based components for interaction with proximity through IoT service environments using multi-access edge computing and techniques to combine AI, distributed security with virtual or augmented reality for sensory and haptic/actuating controls.

Advantages

- Allows to stay better engaged with the environment
- They aid and assist the user in real time
- They are light and easy to wear

Beyond State of the Art

For now, health and fitness wearables represent the first step that consumers will take into the wearable's future. However, consumers are confident that wearables can break away from health and fitness as a category, and from just extending smartphone and tablet experiences.

Consumers are not sure that the wearables industry has found the use cases that will drive mass adoption though; and hence they believe the wearable technology inflection point stands well beyond 2020 today.

3.3. Farming

State of the Art

Smart farming based on IoT technologies enable farmers to reduce waste and enhance productivity ranging from natural resources, energy, water, the quantity of fertilizer utilized to the number of journeys the farm vehicles have made.

Smart farming means the use of capital-intensive, high technology systems including IoT for growing food cleanly and sustainable for the small and large-scale production.

In IoT-based smart farming, the system is built for monitoring the crop field with the help of sensors (light, humidity, temperature, soil moisture, etc.) and automating the irrigation system. The farmers can monitor the field conditions and animal stock and take better decisions and optimise the use of resources.

The state of the art IoT applications relates to precision farming (i.e. farming practice controlled and accurate for raising livestock and growing of crops), agricultural drones, variable rate irrigation, water use efficiency, livestock monitoring IoT applications to collect data regarding the location, well-being, and health of livestock, smart greenhouses etc.

Technologies

Wireless IoT applications are used to gather data regarding the health, well-being, and location of livestock. The communication technologies used range from radio frequency identification (RFID) or near field communication (NFC) for tagging, Bluetooth or Bluetooth Low Energy (BLE), low power, wide-area network (LPWAN) sub-GHz technologies, GPS and 4G/5G mobile technologies.

Advantages

Potential of IoT in facilitating sustainable agriculture. Support and help farmers decrease production costs and waste by optimizing the use of inputs, while increasing yields by improving the decision-making with more and accurate data at the edge.

Beyond State of the Art

Real-time collection, processing and querying over time-series data streams from edge devices across the different farming applications and federation of IoT platforms. Integration and use of heterogenous IoT devices, (i.e. sensors, actuators, cameras, weather stations, etc.) from various applications to reduce device installation and maintenance costs, while providing for easy upgrade to newer and more advanced devices. The use of federated IoT edge platforms that support scalable data analytics that can continuously process large crop, livestock et. performance data, while offering tools that allow farmers/growers and other stakeholder in the value chain to analyse and visualize farm performance data.

3.4. Cities and Communities

State of the Art

A successful city is a great place for living, studying, working, visiting or getting older. It provides value for its citizens. And "value" has a wide range of meanings for citizens, city authorities, local businesses or community groups, such as:

- A city that is better in terms of liveability, security, safety, housing, comfort, care, accessibility, compactness, openness, health, affection, cleanliness, simplicity, etc.
- A city that is socially and economically stimulating, dense, vibrant, dynamic, cultural, technological, entertaining, educational, rich both naturally and historically, etc.
- A city that is socially and environmentally responsible, sustainable, circular, resilient, inclusive, solidary, etc.

IoT technologies and solutions must contribute to create this type of value for cities in different ways. Even if their contribution varies on different levels (municipality, urban, citizenship) or domains (security, social, mobility, environment…) there are some broad areas where IoT technologies and infrastructures have a differential impact over other technologies: public services orchestration, citizen empowerment and inter-city, public services interoperability.

Simultaneously, the emergence of new interaction methods among citizens (and their wearables), urban systems and city services provides new opportunities for citizen engagement and participation in better services; ranging from passive roles, such as transparency & monitoring (e.g., air quality, transport utilisation), to more active ones, such as data provision (as mobility data) or even public service provision (social services, car sharing, etc.).

To enable the digital transformation of legacy public safety and emergency management systems into IoT-based Next Generation Emergency Services (IoT based NGES) several challenges need to be resolved. This transformation is tightly coupled with the increased penetration of Smart Cities in the forthcoming years.

This will be allowed by leveraging on the inherent data produced, processed and disseminated by sensors, connected devices, and smart objects of Smart Cities such as environmental sensors, smart transport, smart water, smart energy, e-health/smart hospital, CCTV, robots, UAVs, wearables, social Media etc. The transformation of these data into actionable intelligence (in some cases enabling automation) is of utmost importance during emergencies. The main aspects in IoT based EWS is the time-criticality of sensor data exchange, scalability, and support of semantics to support context awareness of crisis events and to support data and service interoperability.

Technologies

To this end and to set the research and development needs for successful deployment of Smart Cities IoT based NGES several aspects need to be taken into considerations and further studied.

- A classification and mapping of IoT devices and smart objects that can act as enablers of Smart Cities IoT based NGES needs to be performed considering real-time requirements, quality of information (such as accuracy, availability, origin of data, granularity of data etc.), security etc. Furthermore, context information management to enable the exchange of data from various smart city domains with NGES should be addressed.
- Smart Cities IoT based NGES that may initiate emergency calls need to be classified and studied. It is crucial to investigate the point of initiation of emergency calls, as well as the events that will trigger automated emergency calls, considering all critical parameters (such as location, origin of data sources, call routing, etc.) for automated emergency calls.
- Integration aspects of Smart Cities IoT based NGES with Early Warning systems should be studied. Issues that to be addressed are scalability, time-sensitiveness of data exchange and processing (i.e. heterogeneous Smart Cities data sources), resilience to changes in crisis zones, context-awareness of crisis events and service interoperability.
- Refinement of existing architectures that incorporate the integration and interworking of Smart Cities IoT based NGES with legacy public safety and emergency management systems need to be performed.
- It should be studied how edge computing nodes and gateways in the overall Smart Cities architectures can act as and/or host emergency services analytics applications that fulfil certain edge intelligence based on the type of IoT devices/smart objects/data types, location, observed events/incidents etc. The capabilities provided by the advances in 5G

technology and ETSI-MEC (Multi-Access Edge computing) should be examined and investigated.

- Interoperability between the Smart Cities IoT based NGES and existing public safety and emergency management systems should be studied. The interoperability layer should follow a modular and flexible approach and may be defined as an emergency services gateway layer.
- Smart IoT based NGES should incorporate suitable virtualization and orchestration techniques as well as management features of services and micro services of the different emergency services provided (at different layers: device, edge, analytics layer), e.g. for various smart city domains and emergency use cases.
- Security and privacy of Smart Cities IoT based NGES need to be fully compliant with public safety and emergency management system regulations and GDPR. New threats and vulnerabilities that might arise should be studied and suitable mitigation actions should be proposed.

Advantages

- Increased situation awareness of the emergency scene
- Reduced response time and improved response capabilities to emergencies
- Increased operational efficiency and better coordination among different public safety agencies
- Efficient mission planning and dispatching of first responders
- Improved decision making
- Efficient notifications for citizens (both mass notifications and personalized notifications)
- Improved interaction of citizen with public safety agencies and city communities
- Improved safety of citizens

Beyond State of the Art

- Edge computing and 5G technology will solve challenges of exploding data velocity, variety, and volume and will further provide low latency and location awareness, which are critical for public safety applications and emergency management services.
- The transformation of legacy PSAPs into IOT based PSAPs will enable the initiation of IoT based emergency calls, which will be further extended to support IoT sensor data (including video broadcasting).
- Big data analytic and AI techniques tailored to the needs of emergency management will enhance the situation awareness and decision-making process. Analytics as a Service and Artificial Intelligence as a Service (AIaaS) are emerging concepts, where Smart Cities NGES can be either a service provider or service consumer.

3.5. Smart Mobility and Autonomous Vehicles

State of the Art

Development of IoT and AI based solutions for autonomous systems to increase the safety and provide high reliability of data transmissions, while integrating the internet of vehicles application with various Tactile Internet applications. Autonomous vehicles are the next innovation in the automobile industry. It aims to control traffic jams, avoid crashes and accidents, while making the commute easier.

Technologies

New IoT technologies and platforms for integration of the edge computing and the use of software defined networks (SDN) and network functions virtualisation (NFV), combined with new architectures to support direct communication between autonomous vehicles/devices, by reducing the use of intermediate nodes such as base stations or access points for relaying data transmissions between autonomous devices.

Research on new distributed security and safety mechanisms for autonomous vehicles and systems. Work on concepts and architectures to optimise the bandwidth, storage, time and costs by limiting the data that needs to be transmitted, while processing and taking intelligent decisions locally in real-time.

With AI, IoT and autonomous vehicle technology, machine learning with human-in-the-loop AI will become an area that has to address both the technology and the ethical design rules.

Advantages

- IoT provides improved access and security
- IoT provides improved control over vehicle status and driving
- IoT sensors improve vehicle safety
- IoT helps avoid traffic and congestion

Beyond State of the Art

Nowadays, people can have their car in their pocket, but this is just a taste of how IoT is transforming the automotive industry. Cars that can be parked with a single tap of an app button, circular economies where automobiles are shared and rented as a service through mobile apps, and the era of completely autonomous vehicles are not far away.

3.6. Water Management

State of the Art

Issues around water management need to be addressed from several angles. In particular the following approaches are to be considered:

- The imperative societal need to make best use of a scarce good
- The geographical characteristics that require tailor-made approaches
- The technological trends that are enablers to improve water quality, ensure access, realize better water management and ensure adequate pricing

Technologies

Regarding technological and infrastructure research, smart water management sees the following IoT domains as the most promising:

- Intelligent devices for smart sensing applications
- Connectivity
- Artificial intelligence
- Blockchain and the embedded intelligence and cognition at each IoT architectural layers and applications.

In this field there is a higher demand for smart sensors and the specialised sensing applications for chemical, biological and physical parameters. Technical solutions are addressed in the context of opportunities for "hard sensing" and "soft sensing". This in particular to detect e.g. leakages and pollution and to enable citizens to make full use of their water infrastructure. Technology around smart sensing will enable predictive maintenance of infrastructure and to make informed decisions based on water quality and quantity. Besides that, there are well established and long-standing water management systems, the trend is to integrate the new technology and to ensure interoperability.

In the context of current economic and market trends, scarcity of high-quality water is the predominant challenge and strategic issues to be addressed. Consequently, water management work puts emphasis on contributions to address on the one hand the pressure to minimize pollution and on the other hand the pressure to optimize efficiency. Closely related to this is the question to the social and economic value of water. The notion of "full cost pricing" needs to be put in perspective to ensure that access to water remains a human right. One interesting point in this regard is the issue in how far data creation from water infrastructure and use of water could become part of the equation to determine adequate pricing. Water management creates data which has value, the question who owns and has access to this data is to be assessed. Moreover, water infrastructure is critical infrastructure. An attack to harm a municipal water infrastructure is likely to result in unprecedented harm for people and environment. Protection of the system against physical and virtual attacks is key.

Advantages

The use of IoT for water management and distribution combined with optimization techniques, as well as predictive analytics can bring efficiency and cost reduction for water management operations. In addition, the use of IoT devices with sensing/actuating capabilities offering a lower price and with battery powered networking solutions for LPWAN, can improve water management solutions in the following ways:

- Water leakage detection
- Efficient systemic water management
- Water quality and safety monitoring
- Quality control on water reserves
- Transparency on consumption
- Prescriptive maintenance on infrastructure

Beyond State of the Art

IoT technologies can offer further solutions for predictive maintenance combined with AI techniques to help in scheduling the maintenance as well as the shutdown of pumps on a regular basis. The optimization techniques can be applied to a city or to irrigation systems. These solutions support the activities on the conservation of resources and energy.

3.7. Industry and Manufacturing

State of the Art

The digitization of the Manufacturing Industry is one of the most relevant pillars of the so-called fourth Industrial Revolution (Industry 4.0 - I4.0), where most advanced world economies have recently made huge investments to keep their competitiveness high, in the global market landscape characterised by low wages and insufficient socio-environmental sustainability. I4.0 enabled smart products, I4.0 connected factories and I4.0 new business models represent the tangible outcomes of this fourth revolution also in Europe. Among the so-called I4.0 technologies, IIoT is considered a backbone enabler for any I4.0 business process (global and local, factory automation and 'product lifecycle, open and confidential, operational and decisional) together with data analytics and AI. IoT provides a digital infrastructure for communication, integration, interoperability, human machine interaction and remote operations enabling a huge ecosystem of cloud services, also based on data analytics and/or AI.

One of the advantages of Industry 4.0 is the massive usage of heterogeneous sensor nodes integrated on machines, environment and infrastructures. Sensor nodes data analysis enable monitoring of working parameters and ensuring a fast failure detection and short repair time while reducing maintenance cost.

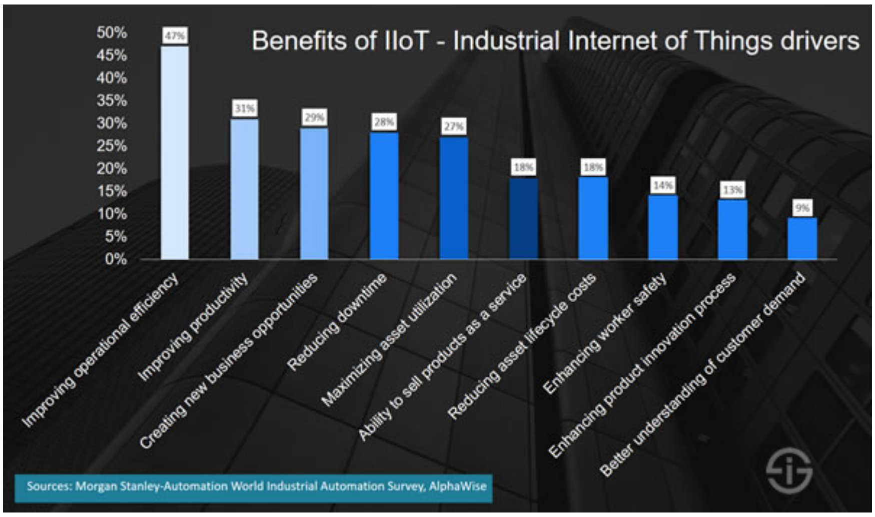
Technologies

IIoT is the equivalent of consumer IoT with industrial specifications, to be compliant to a stronger working condition.

IoT based real-time enabled cyber-physical systems (CPSs), integrated into manufacturing, engineering, material usage and supply chain and life cycle management to provide flexible and self-organized smart manufacturing spaces, which deliver services and applications provided by cyber-physical system platforms that connect people, objects, and systems to each other. Convergence of industrial IoT, AI, robotic manufacturing, autonomous vehicles, and augmented reality (AR) requires new architectural concepts for processing massive amounts of near-real-time IoT information. Continue the research on distributed security mechanism to address the converging of IT, OT (component of Industrial IoT) and AI where a lot of information is analysed and leveraged, in real-time at the edge.

Advantages

Predictive maintenance by using Deep Learning technologies and big data analysis allows schedule maintenance, prevents unplanned and expensive stops, helps planning investments on manufactory capacity.



Sources: Morgan Stanley-Automation World Industrial Automation Survey, AlphaWise

Figure 4: Benefits of IIoT drivers

Beyond State of the Art

Deep Learning technologies and big data analysis coupled with edge computing and remote monitoring are key factors for predictive machine maintenance. IoT sensor nodes embedded with DL engines perform local analysis, properly aggregating heterogeneous data to be further processed by High Performance Computing (HPC) systems.

3.8. Energy

State of the Art

The smart grid as an energy generation, transmission and distribution network is enhanced by IoT technologies offering digital sensing, control, monitoring and communication capabilities. By supporting automated, bidirectional flow of information and communication, IoT technologies enable real-time sensing and control for two-way flow of electrical power. Among others, IoT solutions support load balancing, supply from diverse volatile distributed generation sources, while controlling the distribution network, by creating an intelligent and interoperable grid for the establishment of virtual power plants from clusters of distributed generation installations including renewables, enabling the control from a central or local control facility. The IoT embeds connectivity into the energy ecosystem and domain-specific equipment and devices, connects such devices in intelligent networks, and facilitates data analytics to extract meaningful and actionable insights and distributing computing intelligence throughout the energy infrastructure.

Technologies

The energy sector IoT communication technologies include protocols to transmit data in different environments, ranging from home area networks to industrial area networks, and protocols to transmit data externally back to a central location. The communication technologies include GSM, 3G, LTE, LTN, WANs, and eventually 5G. The IoT technologies support load balancing, volatile supply from diverse distributed generation sources, while controlling the distribution network, by creating an intelligent and interoperable grid for the establishment of virtual power plants from clusters of distributed generation installations including renewables, enabling the control from a central or local control facility.

Advantages

IoT technologies facilitate deploying monitoring and control solutions that support sensing, actuating and computing across the energy infrastructure, including energy generation, distribution and consumption monitoring systems.

Beyond State of the Art

Development of IoT based solutions for energy system network consisting of distributed energy resources (DER) and multiple electrical loads and/or meters, operating either in parallel to or islanded from the existing power grid. IoT technologies and edge computing for energy management and operation of microgrids and virtual power plants. Energy storage systems (ESSs) at the LV grid, facilitated by IoT solutions and distributed architectural approaches, security mechanisms and frameworks. AI-based IoT solutions for real-time demand/response and peer-to-peer energy and flexibility trading.

3.9. Buildings

State of the Art

Research on IoT technologies for smart buildings and building management systems using an end-to-end view considering the move of processing to the edge in highly sensors/actuators-intensive and information-intensive building environments.

Building Automation and Control Systems (BACS) exist for years and enable to monitor and control the functions of a building, including electrical systems, Heating Ventilation and Air-Conditioning (HVAC), lighting control, security and surveillance, alarms, lifts etc. Therefore, connecting devices and actuators on the field for taking relevant decisions and actions is not new. What IoT brings is the capability to connect almost everything at a very large scale and compute huge amount of data at every level, from smart devices up to the cloud, for delivering better services, optimizing operation and maintenance, and breaking the silos between the different functions.

If within commercial buildings the emphasis can be on 'rational' systems (more control/maintenance etc.), a different approach is needed when it comes to residential building: within residential building, also depending on whether stand-alone or build as series the emphasis is on experience, imagination, etc.

In both case the development of innovative sensors enables to measure and monitor many parameters of the buildings related to the comfort: temperature, humidity, air quality, CO_2, light, etc, related to the activity within the building: presence detection, movement detection, intrusion, door/windows opening detection etc. and related to the use of resources: water, electricity, gas, etc. Edge control and analytics running on-premise and/or in the cloud are used to provide the required level of comfort while optimizing the resources consumed by the building. In the best cases, new buildings can be energy positive when they associate state of the art construction materials, local energy generation and storage. Occupants can interact with the building and have some control functions accessible through apps on their smartphone such as lighting control or setting the temperature of a room for instance.

However, all the buildings are not yet "smart" and most of what is described above remains devoted to large buildings where complex and costly Building Management Systems can be deployed. The technologies used in these systems remain diverse with a lack or limited interoperability preventing the exploitation of the full potential of the building knowledge. Wireless connectivity remains limited with too many non-compatible protocols.

Finally, the digitalisation of the buildings is quite advanced, with lots of automation systems, autonomous decision making, however they are not open enough the create a collaborative ecosystem and offer to third parties the possibility of exploiting these resources for developing innovative applications and services.

One issue however should be addressed: there still is a difference between private, i.e. residential- and (semi)public, i.e. commercial buildings when it comes to issues of privacy. Exploiting resources should be carefully measured between what is controlled by the inhabitant and what is controlled by users.

Technologies

IoT is amplifying the capabilities of intelligent buildings as well as accelerating advanced control and sensors in commercial building today. Connected sensors that communicate via open protocols through a scalable and secure platform of IoT are providing new data streams and fine-grained controls of building to maximizes efficiency and occupant satisfaction. A list with the technologies developed in smart buildings Is given below:

- Sensing technologies and ultra-low power wireless connectivity with energy harvesting enables to better sense the environment on the field and deploy high number of sensors.
- Networking technologies with self-forming, self-healing capability facilitate the deployment of the devices on the field at a large scale.
- Distributed intelligence through the combination of software technologies at the various levels: device, edge, cloud, enables to optimize globally the system, provide resilience, secure critical functions.
- Wearables add information from the occupants for tracking comfort levels and presence
- Building Information Model (BIM) provides a digital representation of the building all along the building lifecycle, from design and construction down to the end of life and facilitates exchanges between the multiple stakeholders.
- Semantic technologies such as ontologies and associated languages. SAREF4BLDG (SAREF for Building) which is an extension of SAREF and uses the IFC standard is very interesting in that perspective.
- In the future, software using AI and ML and Deep learning technologies will provide actionable insights thanks to the data reported by the sensors on the field.
- New technologies like AR, VR, voice control, etc. will provide multiple and powerful ways to interact with the building for various needs.

Advantages

- Internet-connected wireless sensing and control devices have made it possible to aggregate and communicate data streams from distinct building systems to cloud-based analytics and deliver actionable insights for facility improvements.
- Open standards, wireless communications and analytics are optimizing operations and maintenance processes and generating significant financial benefits through energy efficiency and better capital planning for equipment retrofits.
- Facilitates adaptation to changing needs and requirements over time with better flexibility and modularity.
- Much better knowledge and understanding of the environment inside the building and of the activity of the occupants thanks to the data reported by the sensors.
- Improved security and comfort for the occupants.
- More efficient, more cost-effective operation and maintenance of the building.
- Reduces resources consumption, making the building more sustainable.

Beyond State of the Art

The IoT trend is changing the process of acquiring building data. Internet addressable and multifunctional sensors now are providing intelligence at the edge; in other words, these data sources are gathering comprehensive data throughout the intelligent building. They are becoming cheaper and are being installed in equipment such as wall switches and lighting fixtures. These advanced devices gather data around a range of building conditions such as temperature, humidity, lightning levels, and occupancy counts thereby providing a comprehensive data set that historically would have been gathered in silos. Such data can then be communicated via open wireless communications networks to edge-based and/or cloud-based analytics. The bottom line is that an IoT platform approach delivers actionable information, not just more data.

In addition, sensors integrated in the buildings enable features like predictive infrastructure and building monitoring and maintenance preventing critical structural damages. Big data analysis and deep learning will ensure real time monitoring, predictive anomaly detection and in advance structural maintenance.

While more and more people are living in cities every year, having smarter, sustainable, energy efficient buildings is essential. IoT is a key lever thanks to its intrinsic ability to understand a context and environment, adapt, learn, and ultimately deliver what people expect. In that perspective, it is essential to put human in the centre and have IoT as a tool to improve life of the people living or working in buildings.

The use of AI and machine learning capability can help for adapting to variable needs over time and avoiding cumbersome programming while delivering what people expect. Building on all the data reported thanks to the IoT, it is possible to improve comfort, better optimize the use of energy and resources, facilitate the operation, predict failures, reduce costs and ultimately make life better for the occupants.

The building itself contributes at a larger scale (district, city) to a more sustainable world, being connected and sharing information, exchanging energy, delivering services…etc.

The digitalization of building and architecture environment offers many opportunities; however, this is populated by different standards and data models that must be harmonized. IoT technologies as data sources and the services exploiting novel data analytic techniques in many ways, will benefit from the definition of common ontologies for buildings. In this sense SAREF4Buildings extension can play a key role, but in any case, open environment should be adopted to foster and boost the development of new services.

A second aspect is that building impact, in terms of IoT goes beyond sensors for physical parameters inside the walls.

Digitisation implies that virtual representation of physical systems can be easily integrated in wider pictures (cities, electricity, heat or water networks, mobility or garbage collection among many). In the future, buildings will not be neither designed nor refurbished without considering the digital footprint and the impact it could have in its environment in terms of services for existing inhabitants. Additionally, wearables can be a supportive tool to evaluate comfort levels confronting sensors and human response, providing the specific conditions to each person that maximize their wellbeing, both in living and working spaces.

IoT has a huge potential to track the construction process assuring that all the mandatory steps and the management of the materials have been done accordingly to specifications and design, and in case this doesn't happen, identify who is responsible and liable in case of future problems.

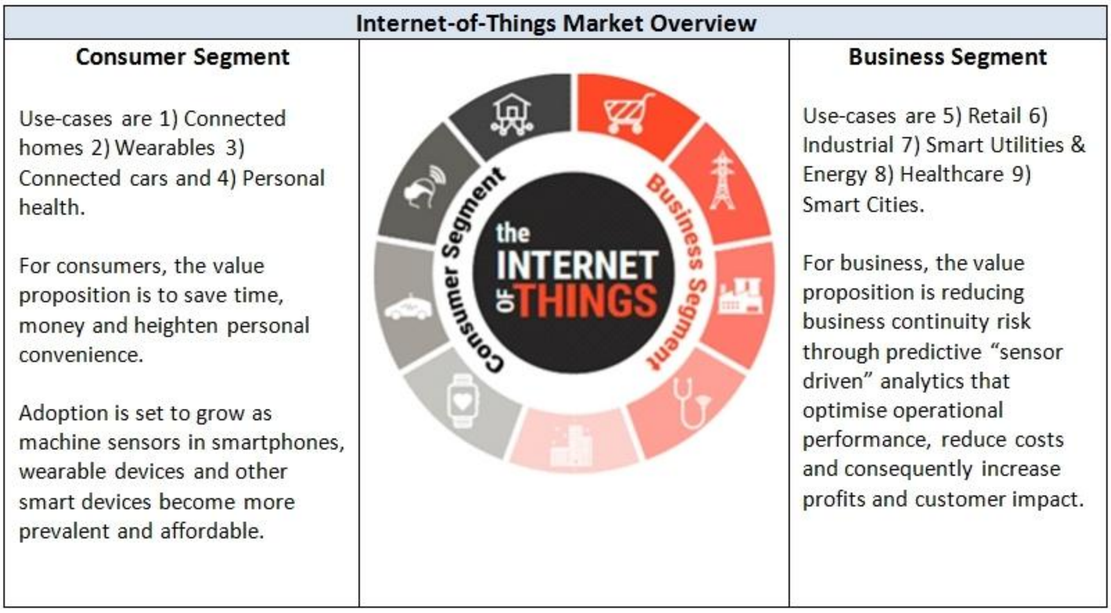
4. Economic and Market Trends

This section includes the identified scenarios as emerging areas and their applications in the use of IoT technologies, business models, market places and the factors that make economic issues imperative for IoT services and applications in different industrial domains.

In this context, developing IoT systems and services require holistic approaches including engineering, management, economic and market aspects that ensure efficiency and optimality in various IoT applications.

Identified main impact markets:

- Automotive incl. electromobility, connected and autonomous vehicles
- Energy generation, distribution and consumption
- Industrial automation, production and robotics
- Security
- Smart homes
- Smart cities
- Infrastructures



Internet-of-Things Market Overview		
Consumer Segment		**Business Segment**
Use-cases are 1) Connected homes 2) Wearables 3) Connected cars and 4) Personal health. For consumers, the value proposition is to save time, money and heighten personal convenience. Adoption is set to grow as machine sensors in smartphones, wearable devices and other smart devices become more prevalent and affordable.		Use-cases are 5) Retail 6) Industrial 7) Smart Utilities & Energy 8) Healthcare 9) Smart Cities. For business, the value proposition is reducing business continuity risk through predictive "sensor driven" analytics that optimise operational performance, reduce costs and consequently increase profits and customer impact.

Figure 5: IoT market overview (Source: Growth Enabler Market Pulse Report 2017)

Trends In different application areas:

- Efficient power and energy management
- Secured digital energy infrastructure
- Connected automated and autonomous driving
- Intelligent and connected production

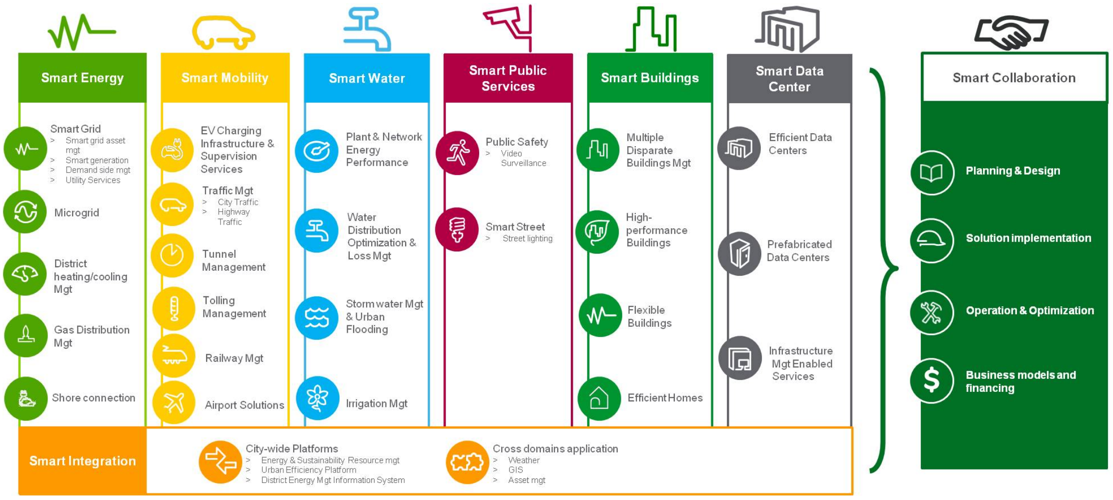


Figure 6: Segments and impact on using IoT technology for smart collaboration

4.1. Smart Healthcare

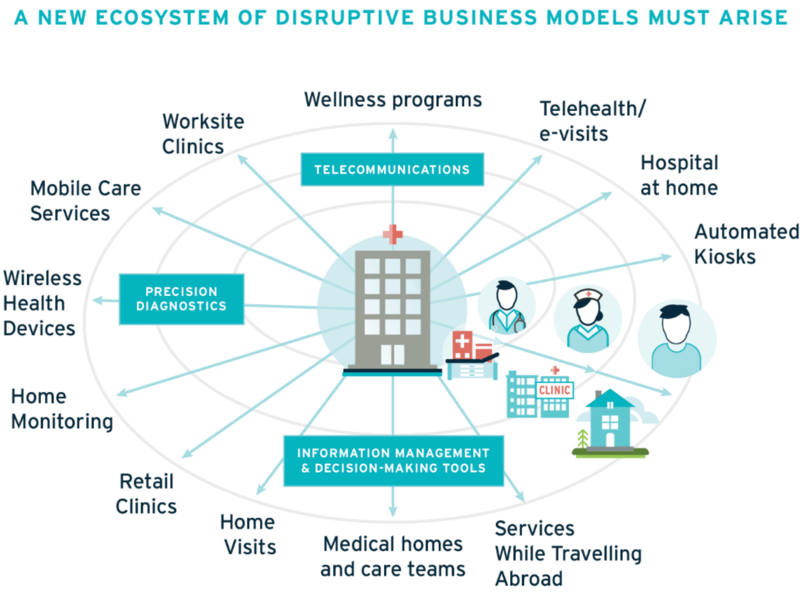
Healthcare has suffered a swift in the way the use of technology is perceived, from being the monolithic environment in a hospital with specialised and prohibitive equipment to a more open ecosystem where people are influenced by accessibility to information and understanding about the technology and can select their healthcare program.

The increasing implementation of diverse equipment (Diagnostic as well as therapeutic) in detecting and maintaining the health outcomes of patients is one of the major factors that drive the growth of the global IoT Healthcare market.

In major developed countries, IoT has been successfully implemented in remote monitoring of diabetes and asthma patients, coupled with high penetration of fitness and wellness devices owing to which the sales of the IoT Healthcare systems will grow in the future years.

The immersion of healthcare and wellbeing programs for remote monitoring and healthcare records integration remains a challenge, the integration of daily tracking activity with healthcare data can potentially open the door to new discoveries in healthcare and diseases identification and treatments , in the way to solve this gap there are running initiatives in Europe but close to solve the problem it is only paving the way towards better services and easy integration, the challenges remains beyond the IoT technology and the society but more into the policies and regulations around the use of the IoT technology and the data generated with it.

The healthcare ecosystem is changing the shape, form traditionally isolated hospitals or institutions to a more global-connected healthcare system where the main role is the patient with awareness of IoT technology and the systems and subsystems around themselves demanding integrated services and contributing with live (real time) data for better health detection and in a future more accurate and profiled/personalised prescriptions.



Source: The Innovator's Prescription: A disruptive solution for health care 2008

Figure 7: Modern Smart Healthcare Ecosystem (Graphic: Innovator's Prescription)

Several types of components are being used in the manufacturing of healthcare IoT devices. The systems and software are having a huge demand in the Global IoT Healthcare Market owing to increasing applications in all the medical devices, as it is the skeleton of medical devices to perform its actual functioning of interconnection between two devices. Systems and Software segment is expected to grow with a CAGR of 12.6% over the forecast period.

Telemedicine is the most recent application utilizing the IoT technology in maintaining the patient data and tracking the where about of the patient. Hence Telemedicine is a leading Application type segment in Global IoT Healthcare market. The telemedicine application segment is likely to cross-market value of USD 4164.3 million by end of 2022 and is growing at a CAGR of 12.7% over the forecast period.

4.2. Smart Wearables

The growing need to remain connected has led to an increase in demand for more connected products. IoT is one such avenue that captures data from the surrounding stimuli and ensures that various products are connected.

IoT and smart products have created revolutionizing expectations about data and connectivity while opening new channels of business value. One such channel is the creation of industrial wearables.

Connected devices such as smart glasses, wrist computers, ring scanners, and wearable scanners are types of industrial wearables that are used by industrial workers across various end-user industries.

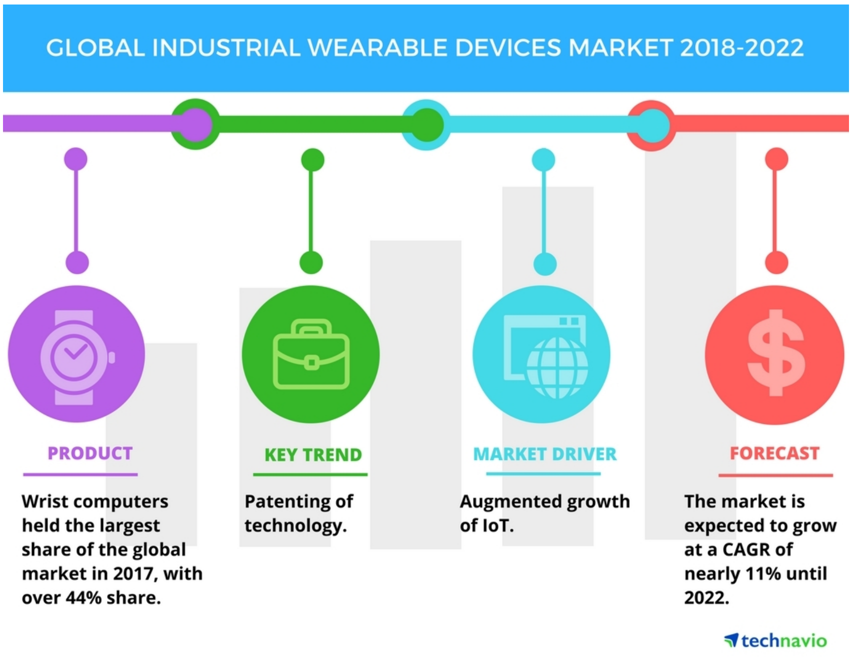

GLOBAL INDUSTRIAL WEARABLE DEVICES MARKET 2018-2022
PRODUCT
Wrist computers held the largest share of the global market in 2017, with over 44% share.
KEY TREND
Patenting of technology.
MARKET DRIVER
Augmented growth of IoT.
FORECAST
The market is expected to grow at a CAGR of nearly 11% until 2022.
technavio

Figure 8: Global industrial wearable devices market from 2018-2022. (Graphic: Business Wire)

Connectivity costs and embedded sensors no longer deter companies from adopting the smart technology as the prices of hardware and electronics are falling in the global market. Connectivity solutions such as Wi-Fi, mobile networks, and broadband communication are ubiquitous and capable of supporting large volumes of IoT connectivity at a little incremental cost to companies and consumers.

The wearable external medical devices are dominating the Global IoT Healthcare Market in medical devices segment due to the increased adoption of IoT technology in advanced healthcare and fitness devices. The remote patient monitoring experienced a huge leap in 2016. Total 7.1 million patients were enrolled in some form of digital healthcare program featuring connected medical devices that used the patient's own mobile devices. Owing to the rising popularity and increasing demand, the segment is likely to grow at a higher CAGR of 11.3% over the forecast period.

4.3. Smart Farming

The United Nations Food and Agriculture Program has noted that global production of food, feed and fibre will need to increase by 70% by 2050 to meet the demands of a growing global population. This means that, to optimise crop yields and reduce waste, the agriculture and farming industries will need to rely heavily on IoT and M2M technologies moving forward.

IoT data value

IoT is just starting to unveil its potential for the real economy of Agri-food. However, deployment of IoT technologies in smart farming applications must lead to quantifiable benefits such as increase of productivity, waste reduction or efficiency in the production, thanks to data-centric management. Large-scale experiments involving multiple stakeholders must be carried out to identify and quantify such valuable benefits. Presenting results of the analyses in comprehensive and useful ways to final users is a must.

Application of machine learning and data analytics techniques contributing to add value to data captured by IoT devices is also a need in smart agriculture. The devised solutions must evolve from ad-hoc solutions for specific scenarios, developed by qualified people, to generic solutions easily configurable and usable by the end-user. In general, the "one size fits all" approach does not meet the diverse requirements of the agri-food sector; therefore, solutions to be applied in agriculture need to be adaptable in highly diverse contexts (such as geographic locations and/or crops).

IoT data market places and business models

IoT disruptive nature promises economic data availability, easy re-exploitation to gain further value out of them, and thus creation of cross-domain win-win synergies for currently fragmented stakeholders. To provide innovative and viable business models around the IoT there is still place for R&D in mechanisms to correctly ascertain and maintain appropriate rights management (including ownership) of the data produced by the IoT ecosystem and keep track of transactions among the different actors involved in the ecosystem.

This challenge includes not only technical aspects, but also legal and ethical issues that must be solved for parties to be able to monetize data production and data analysis in global shared markets. Therefore, a future IoT agenda for smart agriculture shall address the creation of non-siloed data solutions, EU-wide uptake and expandable business models that embed (open) data aggregation and sharing mechanisms. Decentralized solutions (e.g. resorting to block-chain or similar) must be considered to reinforce trust in the whole system.

Smart Farming Apps Marketplace

The app business model had a big impact in the smartphone market. With enough level of standardization of IoT technologies and protocols, this same business model could be applied to the IoT across many industry sectors, including smart agriculture. Thus, open SDKs and friendly APIs, as well as servitisation of the IoT, have to be achieved so third parties are able to develop apps in the same way they do for smartphones.

IoT as real and handy technology

Research agendas and specialized press is full of lines about the capabilities of IoT. In other sectors, IoT technologies are perceived as technologically ready to be implemented in real scenarios.

In the Agri-food sector, it is perceived as a technology for the near future. Lots of farmers are unaware about current and available IoT technology, and the real benefits its implementation could have in their farms. More real and closer demonstrations have to be implemented. Not many demonstrations are shown in fairs or promoted by farmer associations. IoT should be included in technological agendas of clusters or associations to spread these capabilities.

Customer-centric agri-food industry

While millennials mature, the Agrifood industry shall consider the differentiations they bring in consumption habits and in society in general. Coupled with emerging environmental pressures, this puts IoT solutions at the centre of what it is mostly challenging: systemic transparency and organisational sustainability in respect to the Agrifood industrial developments. A future IoT agenda here may focus on self-explicit product lifecycles, mass products' customisations and novel ways of customer-centric interactions with the brand/ Agrifood product.

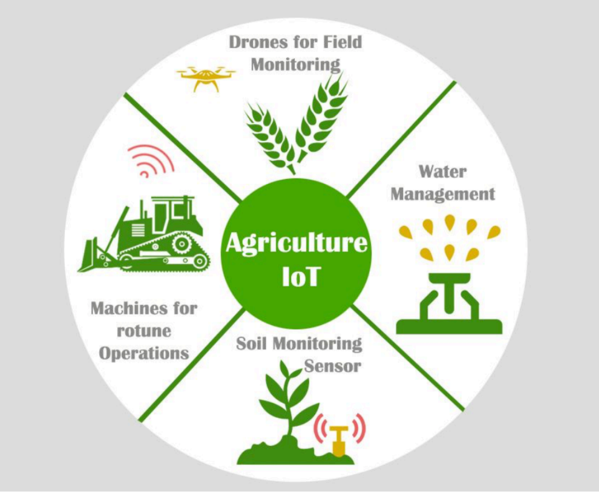


Figure 9: IoT Influence on Smart Farming

4.4. Smart Cities

Value from Smart City projects will only be realised if projects can be delivered and demonstrated as successful. To do so, the application of smart technologies must have a strong business case for investment. New stakeholder relationships, operating practices and deviation from the ‘tried and tested’ solution will raise concerns due to the perceived additional risks. However, these risks should be viewed in comparison with the risk of not innovating and being left behind in an emerging and evolving market.

Furthermore, the wide range of applications of a robust data infrastructure platform means that value to the city can be created in many ways.

Only if a business case is found and value identified can projects scale

The distribution of required investment expenditure and benefits / savings / revenue, which form the essential components of a business case, varies over time.

A conceptual model of this principle is based on the stages below, which breaks out the development of smart city infrastructure projects into four stages:

- Proof of concept;
- Expansion;
- Transformation;
- Maturity.

The conceptual model informs how expenditure, value and profitability change over time, and highlights the typical roles of public and private sector investments to enable projects to follow the value pathway from concept to maturity.

There is a role for bigger and smaller players alike

There is an increasing momentum for Smart Cities to become cognitive and process data streams (including video) in real time. What might be considered a niche market for a big player (i.e. providing IoT platform and cloud infrastructure), could be a huge opportunity for a smaller start up or academia data scientists who could develop optimized algorithms for solving specific issues.

No Single IoT platform will dominate

Cities will combine infrastructure from telco operators, mobility operators, public safety agencies, utilities, etc. and the cities themselves who will run, or commission different legacy and platform based IoT deployments. It would be naïve to think a single IoT platform will dominate, therefore IoT platforms will increasingly need to exchange data to address needs from cross application use cases.

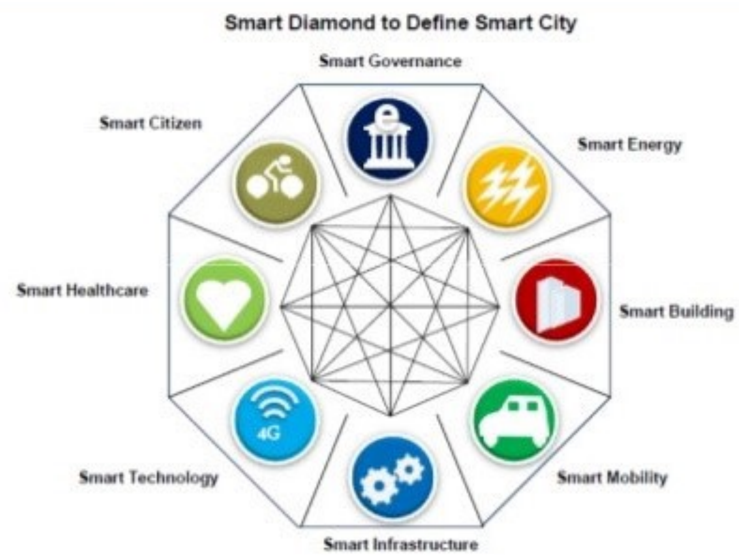


Figure 10: Smart City Segments as potential for IoT Innovation

Public safety use cases emerging big time, they will have a major impact on IoT platforms for smart cities: spending for public safety is projected to grow over time, considering the dramatic increase in terrorist attacks and natural disasters. Several use cases rely on real time and distributed processing of continuous data streams including CCTV video. IoT platform must evolve to become distributed, real time and dimensioned for streams processing including video.

4.5. Smart Mobility and Autonomous vehicles

Most of the electric vehicles are connected through the IoT and part of the so call Internet of Vehicles (IoV) applications, where the sensors in the vehicles constantly communicate with mission control (the OEM), sending data on the status of components in real time. Analysing this data, by using the context of historical data, mission control can predict component failure and optimise the costs of maintenance and increase reliability and safety.

The business models in the case of autonomous vehicles that are safer and more reliable will result in disruptions in different sectors such as insurance industry. With increased safety and reliability and fewer accidents results in lower risk and lower insurance premiums. As the vehicles on the road are autonomous, connected and controlled via IoT devices the insurable entity could shift from the person driving (who is now a passenger) to the operator of the network (presumably the OEM or mobility service provider).

The increase in mobility service providers will shift the ownership patterns, resulting in an optimal asset utilization, where vehicles that are more reliable can be used on an almost 24×7 basis by spreading usage across individuals. This in turn requires fewer vehicles on the road, which would alleviate congestion and change the auto industry business models dramatically. Less vehicles on the road that are in use all the time will reduce the need for parking. That in turn open-up urban space in the form of unused lots and garages.

4.6. Smart Water Management

In the context of current economic and market trends, scarcity of high-quality water is the predominant challenge and strategic issues to be addressed. Consequently, water management work puts emphasis on contributions to address on the one hand the pressure to minimize pollution and on the other hand the pressure to optimize efficiency. Closely related to this is the question to the social and economic value of water.

The notion of "full cost pricing" needs to be put in perspective to ensure that access to water remains a human right. One interesting point in this regard which merits careful and profound attention is the issue in how far data creation from water infrastructure and use of water could become part of the equation to determine adequate pricing. Water management creates data which has value, the question who owns and has access to this data is to be assessed.

Moreover, water infrastructure is critical infrastructure. An attack to harm a municipal water infrastructure is likely to result in unprecedented harm for people and environment. Protection of the system against physical and virtual attacks is key.

4.7. Smart Industry and Manufacturing

IIoT will be a significant part of the market. This segment includes self-optimizing production, automated inventory management, predictive maintenance, remote patient monitoring, smart meters, track and trace, connected cards, distributed generation and storage, fleet management, and demand response, all of which can be achieved by using "sensors, computers, robots and other machinery that interact with each other and their environment over a network, transmitting real-time data that, with the aid of an analytics platform, can be used to improve manufacturing processes."

The structure of the automation pyramid and the IT-OT frontiers are blurring. The connectivity among devices, production assets and information systems are achieved in a horizontal level thanks to the evolution of cyber physical systems that allows establishing interoperable communication among systems regardless IT, OT or whichever level within the automation pyramid. A real connected asset (machine) can achieve upstream and downstream connectivity and communication. Thus, the new era in digital automation leveraged by IoT and Interoperable communication standards is starting to bridge silos in the shop floor and factory.

IoT at machine component/device level is growing fast, sensorized spindles, linear planes and ball screws are starting to be commercially available with innovative, low power and low-cost sensing technologies. The component providers and machine tool builders will face new challenges regarding data interchange and cloud2cloud integration to build machine data-driven business models. For example, maintenance, machining optimization or some other service and condition monitoring needs real data from the factory, machine and devices. The creation of value based on data will be the next big challenge. Digital infrastructure and micro services leveraged by IoT will change business models towards selling added value as a service.

The creation on knowledge-driven services will be enacted by AI and IoT. Condition based monitoring is the major pillar to provide insights about the availability, performance and quality of production assets involved in manufacturing processes. The real time monitoring of industrial equipment that is a precondition for condition monitoring, relies heavily in data intensive processes such us IoT connectivity with high frequency data acquisition from sensors and machine learning techniques to classify the condition of a component. In this process, it is necessary to combine quantitative approaches and methods (e.g. using machine learning, historical data/data analytics) with qualitative ones provided by machine and process experts to achieve a higher level of prediction accuracy and find more types of problems/issues.

Moving forward to cognitive services, machines will be able to self-diagnose the condition of their components, identify problems, explain their cause, optimize maintenance by anticipating problems, thus resulting in greater Overall Equipment Effectiveness (OEE).

Providing connected intelligence to the digital factory is a real challenge bearing in mind that the "no one size fits all" is not applicable in industrial scenarios with conditions and constraints. Even more when the qualitative approach provided by experts is the cornerstone of the solution where IoT, data analytics and AI are just enablers. The interdisciplinary between application domain experts and technology providers will be crucial.

In modern machine tool builder to end-customer recent and ongoing research and development or industrial pilots are aiming at delivering many kinds of after-sales services to the end customers. Most typically, such services include condition monitoring, operations support, spare parts and maintenance services, help desks, troubleshooting, and operator guidance, performance reporting, as well as and increasing in demand, advanced data analytics and prognostics-based decision support. The markets for this service are still in its infancy.

The importance of service business in the future is evident as the service business enables revenue flow also after the traditional product sales and, more importantly, the service business is typically many times more profitable than the product sales itself. The service business markets are becoming more and more challenging, while the high-income countries are focusing on high-skilled preproduction and after sales life-cycle stages. In the global service business market, Europe can differentiate by using its strengths: highly skilled workforce, deep technology knowledge and proven ICT capabilities, but the success needs new innovations and industry level changes.

4.8. Smart Energy

IoT offers increased solutions to the energy sector by providing the tools they need to leverage data from connected equipment and devices to improve grid reliability and resiliency, enhance customer engagement or monetize distributed assets, whether it’s renewable power generation, energy storage, smart inverters, EVs or home appliances and devices.

The emerging Internet of Energy (IoE)¨ holds out the promise of safer, more efficient, reliable and resilient power plants and grids. The IoT technologies and applications are moving at the grid edge addressing the distributed storage and distributed generation (where smaller power sources and storage can be aggregated to provide power), and in the home, such as smart meters, smart appliances and electric vehicles, which are becoming commonplace and change how the prosumer and consumer interact with our energy supply.

Energy utilities are facing new challenges and need to address the strategic way forward. Some can opt for a conservative approach on staying as a pure commodity just embracing the new technologies and adapting their services to the new demand and other choose to become a added value service providers for multiple kind of energy needs and fully embrace the new digital era fostered by the adoption of IoT. The success on both approaches would certainly rely on a deep transformation over the whole value chain to adapt to the new demand and supply needs, including customer relations, operations, business models and compliance. An efficient implementation of these strategies will translate into solid growth perspectives.

New players are entering the market and introducing their innovations. Those new market entrants range from very technological start-ups to very large companies (including Tesla or Google). As IoT starts to be adopted in the energy sector, new challenges and opportunities arise for market players. These should certainly take into consideration for the strategic way forward.

- Adopt a prosumer centric approach, delivering fully customized and personalized services for end users and also, in the future, smart things enabled by IoT.
- Make use of all the relevant data gathered by IoT devices and develop a data orchestration able to, on the one hand, monetize the information and, on the other hand, be flexible enough to adapt to market changes and consumer behaviours in a real-time dynamic and prescriptive way.

Understand the IoT ecosystem and make use of open platform foundations and automation processes, enabling the creation of most appropriate services quickly, cost-effectively and efficiently tailored to the customer needs.

4.9. Smart Buildings

A well-recognized mega trend is that the world's urban population is growing quickly. By 2050, 66% of the world's people will be living in cities, compared to 54% in 2014. Cities will get bigger, and there will be more of them. In these cities, buildings are currently consuming 33% of the world's energy. Comparatively, that's more than industry or transportation consume.

Buildings consume 53% of the world's electricity, estimated to increase to 80% by 2040 (IEA, 2016). Therefore, the expectation for having smarter and more sustainable buildings will get higher and higher, and the associated regulation will continue to develop, like the new EPBD directive in Europe.

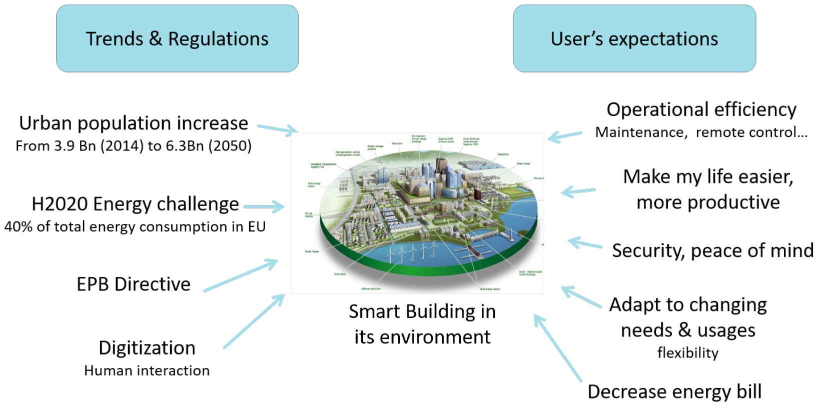
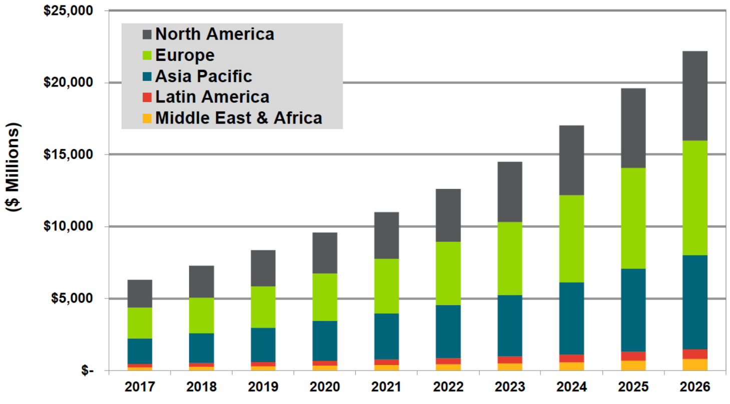

Trends & Regulations
User's expectations
Urban population increase
From 3.9 Bn (2014) to 6.3Bn (2050)
H2020 Energy challenge
40% of total energy consumption in EU
EPB Directive
Digitization
Human interaction
Smart Building in its environment
Operational efficiency
Maintenance, remote control…
Make my life easier, more productive
Security, peace of mind
Adapt to changing needs & usages
flexibility
Decrease energy bill

Figure 11: Smart Buildings - Trends and Regulations vs. User's Expectations (Source: AIOTI - WG013 - May 2016)

IoT is a key enabler for meeting the expectations for buildings. With active controls, up to 50% increase in efficiency can be expected. In terms of operational efficiency, maintenance represents 35% of a building's lifetime costs (IFMA, 2009). By implementing a program of proactive, predictive maintenance and analytics, a building can save up to 20% per year on maintenance and energy costs.

New disruptive technologies are catalysts for huge efficiency gains. The information and control enabled by the IoT are helping create intelligent buildings that:

- Minimize the energy and associated CO_2 needed to run assets and operations
- Optimize the performance, efficiency, and lifespan of physical assets
- Ensure the safety, security, and efficiency of people and processes



Source: Navigant Research

Figure 12: Scale for investment in intelligent building technologies (Source: Navigant Research)

Navigant Research envisions that "2017 is poised to tip the scales for investment in intelligent building technologies". They believe IoT can address energy efficiency and predictive maintenance, while also generating enterprise-wide key performance indicators for the C-suite.

If technology digitization and IoT brings a lot of potential for buildings, we must not forget to put the human in the middle of the picture. We need to include a fundamental (re)thinking of what it means to define and articulate man's environment and its relation to the IoT. After all; architecture is the adaptation of space to human needs. The 2013 EC's Onlife Initiative's (OI) subtitle was 'Being Human in a Hyperconnected World', thus emphasizing the timeless values connected with the fact that having some private sphere is essential to act in public sphere. Increasing technology does not alter this but creates the need for real acceptation and adaptation

As a result, it is fundamental to keep a place in our future work for the following issues:

1. What is the society we want, what values do we consider important, what is our attitude towards topics like privacy, like individuality? Do we need/wish a world dominated by algorithm's, by technologies that can be out-of-control'?
2. The IoT should be considered a concept, not a technology. Paraphrasing the OI: when our worldview - which is based on a concept - is changing due to technological developments we need to rethink the concept. Man is a technological being; the IoT cannot be looked upon as a digital/technological 'threat' only but as a way to incorporate/enhance other more important human values: consciousness, awareness, creativity, democracy.
3. We tend to look upon (home) technology as a comfort issue, neglecting or downplaying the fact that many technologies (can) have a deep impact on our private life. We have no real educated view of what it means to engage with a 'smart' building and/or architecture; with the above in mind much more research is needed to (re)think the consequences of lived/smart space.
4. Changes in the societal framework require another approach in how to create and supply a built environment; i.e. the change in households, elderly people staying at home longer, refugee shelter, etc. This can be matched with need for a better social - urban - environment devoted to contact, less individual and more mutual.
5. The current way of building housing has not fundamentally changed since decades; the future - and in fact today as well - requires another way of building: more flexible, more adaptive; more based on common ground instead of individual housing.
6. This implies, together with the possibilities of industry, a far more industrial approach concerning our built environment, i.e. a change/choice for a separation of structure and infill, facilitating flexibility and a better connectivity for (digital) infrastructure.
7. If we consider our (home) environment the essential element in our life it implies that we need control over it; spatial privacy - given that we accept its traditional built connotation - is easier to create and maintain in an environment of our choice.
8. Regarding sustainability and environmental issues: given e.g. the energy question it will be easier to structure and maintain a more common architecture then a sum of individual ones.

For commercial buildings, the transition to smart buildings is vital to the growth of the organization. It will help the building management save a lot of money because of better efficiency as well as improved overall building operation and structural monitoring and maintenance.

A trend that is expected is the use of predictive maintenance in facility management. Predictive maintenance makes use of IoT sensors and other hardware devices to get a report on the state of a commercial building and all equipment in it.

Measurement and verification using IoT done by commercial facility managers to track information, measure and collect data even in inaccessible areas within commercial buildings.

Commercial facility owners use sensors in various parts of the building to track all information that they never had access to in the past. IoT allows facility managers to have access to all information using the interconnected systems, allowing the ability to collect near real-time data and analyse it with higher spatial resolution. Similar considerations will apply to residential buildings,

Other applications are using IoT technologies for better asset optimization, for energy efficiency, efficient construction management, green buildings and real-time data accessibility.

4.10. Future IoT industrial Developments

Decision-support as a service

IoT-enabled smart farming applications produce enormous amounts of data, its hose processing and analysis are recognized to play a crucial role in solving important challenges of agriculture in the mid- and long-term, such as the pressure for producing food for an increasing global population, with the limited resources available and in a sustainable way. However, in many cases, the analytics needed to extract value from the data collected by the IoT network have to be developed from scratch and deployed to cover specific use cases. Many of these algorithms may be common to different scenarios, therefore having a service that receives a stream (or a batch) of data and provides a stream of results with predefined processing modules can help improve the generalization of IoT solutions and enable the provision of decision-support services on demand.

Interoperability by design

The increase of sensors and connected devices in farms, together with the new storage and analytical capabilities, enables to get better decisions thanks to improve the farm managements. The importance of standards to allow the integration of all data acquired is a key point. However, many solutions are not aware about the need to be interoperable among the other. Many technology providers are not promoting neither applying the interoperability of their products. The adoption of interoperable interfaces thanks to standards and open (or with contracts) API's will bring the opportunity to obtain better wide decisions where multi actor approaches are considered.

Security by design

IoT devices change the ways data is collected, analysed, used, and protected and security needs to be addressed at all IoT architectural layers and be embedded in the design of the IoT devices, applications and services. Security by design principles need to build greater resilience to cyber-attacks, improving detection mechanisms and strengthening IoT ecosystems cooperation through the whole lifecycle of the IoT devices and platforms that make up the IoT applications and services.

Integration of IoT solutions

The demand for IoT-based services in agriculture (i.e. smart farming ones), is constantly increasing: newer generations of farmers are better educated and trained compared to previous ones, so they can better understand the benefits and potential of new technologies for their farms. Currently, there is a high number of IoT-based applications and services for agriculture, focusing on different aspects of the farm and crop management (e.g. fertilisation, irrigation, crop protection and farm management in general). A holistic approach, referring to integrated solutions of modular components that perfectly interoperate with each other, would ensure full exploitation of their potential.

Table 4: Future IoT technological and infrastructure research needs

Topics	2018-2020	2020-2023	Beyond 2023
IoT Identification Technology	Unification of ID methods. (Identification standard for application and profile.	Global identification solutions federating the existing methods.	Seamless identification.
IoT Architecture Technology	Centralized architecture.	Federated architecture.	Distributed architecture.
Sensing Technology	Beginning of "Voice first revolution" "Time of Flight" providing for instance gesture and user detection, Sensor fusion - voice, movement reconstruction, pattern recognition, etc. - with embedded AI.	Expansion of Voice First AI: shift towards voice OS and access to the AI domains they bring Lightweight, ultra-thin, low power and intelligent body-borne sensors leads to novel advances in wireless body area networks (WBANs). Wireless Body Area Network to obtain automated, continuous, real-time measurement of physiological signals allowing detection of behavioural and cognitive conditions.	Voice Analytics Predictive modelling/ Contextual awareness: fall prevention, sentiment analysis, intent and parameter, AI preventive care models.
Processing Architecture	Growing amount of data generated by IoT devices. Need to reduce back and forth communication between sensors and the cloud to maintain	Collaborative edge and real time processing and analytics with embedded AI techniques.	Edge Intelligence maturity (linked with 5G maturity): edge computing with machine learning and advanced networking capabilities. No more user interface.

	performance.		As IoT makes manual data input largely obsolete and ML and AI take over decision-making.
IoT Infrastructure	Cloud based	Edge based	Distributed based.
Connectivity	“Always ready” Short range to access cellular currently dominant.	"Always on” Expansion of LPWA enable a continuous connectivity ⍰ allow remote monitoring of elderly health and wellbeing at a lower cost Short-range: ultra-low-power, adaptive, and robust wireless systems.	5G expansion: every device become ‘smart’ and connected - no latency and greater capacity. Low power, short range networks should still dominate wireless IoT connectivity versus wide area networks in smart living environments.
IoT Communication Technology	Protocols compatibility.	Convergence of protocols and normalised protocols.	Virtualised and software-defined, context-aware protocols.
IoT Network Technology	Ubiquitous network technologies.	Embedded security and intelligence in the network.	Device agnostic network technologies.
IoT Platforms	Common DSS for specific automation of processes.	Multi-domain DSS to accurate decisions.	Autonomous and intelligent systems.
IoT Discovery and Search Engine Technologies	Separate functions.	Integration in the IoT platforms.	Autonomous and intelligent search and discovery engines as part of the IoT applications.
IoT Trust Technologies	Critical Infrastructure Protections for cyber-physical risks.	Risk Management considering cascading effects.	Holistic risk management between critical infrastructures.
IoT Interoperability	Common Semantic Vocabularies (industry adoption).	Common Vocabularies for process and organizational links in water.	Organizational Interoperability.
IoT Standardisation	Standardization of TLS layer. OneM2M vision on East-west communication in IoT platforms.	Trials with OneM2M East-west IoT platforms and finalise standardisation.	Availability of commercial/Open OneM2M East-west IoT platforms.
City public safety network solutions leveraging IoT	IoT becoming pervasive, emergency communications will heavily rely on IoT devices and networks including drones, robots, CCTV cameras, etc.	Safety network solutions embedded in IoT platforms,	Fully integrated safety functions across the platforms

Disaster Traffic Management in Smart Cities	The city infrastructure dynamically controlled to minimize evacuation time and avoid congestion, that will bring great benefits to citizens safety	Federation of functions across different city services	Semi-autonomous coordination systems for traffic management.
Blockchain solutions for IoT	Separate solutions for specific domains	Distributed ledger platforms integrated with IoT platforms	Fully integrated with IoT distributed architectures
Tactile Internet	Edge devices with sensing/actuating capabilities. Hepatic interfaces.	Conversational IoT platforms with new user interfaces to engage with things and humans	New IoT paradigms based on Tactile Internet
IoT Long-Range Communication Technology	Satellite IoT direct access networks	Hybrid IoT Networks mixing satellite and terrestrial LPWAN connectivity.	Low-cost, small-size and low-power Satellite IoT terminals. Full integration satellite-terrestrial LPWA for seamless connectivity.
Sustainable IoT Environments	Improved efficiency for batteries, sensors and microcontrollers Green and efficient cloud farms Systems integrated in the environment.	Energy harvesting field tests with real use in ultra-low power scenarios Cloud farms with self-generated energy sources	Energy harvesting in all self-powered devices (sensors, gateways) and all components of the IoT environment, in general. No need for battery recharges.
Next-Generation IoT Devices	Miniaturisation and integration under current micro-technologies paradigm	High integration and partial adoption of nanotechnologies in IoT devices	Full adoption of nanotechnologies for seamless deployable, low-cost IoT devices, with edge/distributed processing capabilities
IoT Security, Safety, Privacy and Trust	Remote attestation of IoT Collaborative safety Need to define the "European Baseline Requirements for Security and Privacy" that minimizes risk, is neutral in technological terms, and remains open to innovation Standardisation and certification: ensuring minimal security requirements for connected devices.	Scalable attestation of IoT autonomous safety. Industry implementing security features in their products ("security by design"). End user data collected at the edge of the network stored at the edge. Users to control if the data should be used by service providers. Process of authorization, highly private data removed by the things to further protect user privacy.	Fully secure-and-safe-by-design IoT systems and actuators. Efficient tools to protect data privacy and security at the edge of the network

	Baseline requirements for IoT security and privacy that cover the essentials for trust, e.g. rules for authentication / authorization, should set mandatory reference levels for trusted IoT solutions.		
IoT Configuration and Orchestration	Semi-autonomous configuration and orchestration.	Autonomous configuration and orchestration.	Fully dynamic and autonomous configuration and orchestration.
Next Generation IoT autonomous sensing devices	New sensing devices for multiphysics measurements.	Sensor fusion and AI based sensor data processing.	Sensor/actuator fusion and ubiquitous intelligence.
Power Management	Concerns of lifetime, maintenance costs and form factor all linked to battery constraints. Hardware optimization: Ultra-Low power MCUs. Power management ICs designed for energy harvesting. Low-power sensor node application.	Energy storage breakthrough for sensors and other IoT nodes with an extended life time of up to 10 years. Sensor nodes powered by harvested ambient energy. IoT data provided with little or no maintenance. Energy harvesting can help bring intelligent sensing to the edge, for instance in remote or hard-to-access locations	More sensing systems to be self-powered. Low cost of ownership solution, making sensing possible in areas previously considered. impractical, allowing use cases solving challenges that couldn't be solved before.

Table 5: Future IoT economic and market trends

Topic	2018-2020	2020-2023	Beyond 2023
IoT data value	Engage multiple stakeholders of Agri-food in the use of IoT solutions. Ad hoc analysis and prediction systems developed by qualified personnel.	Generic analysis and prediction systems developed by qualified personnel.	Analysis and prediction systems generated and configured by the end-user.
IoT data market places and business models	Focus on data re-use and committed presumption from the supply side.	Define a fair level playing field for data sharing and transactions involving shared data. Mobilise consumer groups and retailers into non-siloed data marketplaces.	Develop assessment techniques and best-practices for communal data-centred governance in a distributed manner Incentivize flexible dis-intermediated communal short supply chains.
Smart Farming Apps Marketplace		Widely usable open frameworks to develop third-party apps.	
IoT as real and handy technology	Promotion of small IoT pilots and living labs at regional level to show IoT capabilities to final users.	Engage multiple training stakeholders of Agri-food in the use of IoT solutions.	Adoption of IoT concepts during technological training agendas, from primary education to university degrees.
Customer-centric Agri-food industry	Increase transparency of food value chain	Customisation of food products	Novel customer-centric interaction with Agri-food brands
IoT technology plug and play	Connectivity plug and play.	Low power solutions. Energy harvesting solutions (solar, thermal, piezo, mechanical,).	Services and functionality plug and play.
IoT continuity of service in case of network breakdown	Local redundancy based on existing systems (FM, Wi-Fi); redundancy through different operators and systems (2G, 3G).	Build-up of further redundancies in existing networks.	Parallel systems based on terrestrial and satellite communication. Network agnostic IoT solutions.
IoT continuity of service – cross-border	IP connectivity with cellular roaming.	Build-up of global services; improvement of seamless roaming.	Global coverage of communication through satellite systems.
IoT data sharing business models	Regulation on data privacy limiting	Fair competition by applying new regulations	Open anonymized GDPR compliant data

	collection of data sets.	and data sharing policies based on win/win models.	sets are a common practice.
IoT for critical applications	Trials with safety critical automated mobility using NGN (5G) – 5G-PPP phase 3.	Availability of specific service (Connectivity and Cloud platforms/MEC) for reliable critical application: ensure given QoS (<100 ms latency – min data rate) 24/7 no interruption > 100ms.	Availability of specific service (Connectivity and Cloud platforms/MEC) for reliable and real time critical application: ensure given QoS (<1 ms latency – min data rate) 24/7 no interruption > 1ms.

Table 6: Future IoT industrial developments

Topic	2018-2020	2020-2023	Beyond 2023
Decision-Support as a Service	Frameworks for facilitating the provision of decision-support services in ad-hoc applications.	Seamless provision of decision-support services in ad-hoc applications.	Seamless provision of decision-support services in universal applications.
Interoperability by design	Promotion of current standards for its usage in farming environments Enhancement of current standards for farming or development of new ones.	Integration of heterogeneous IoT data sources for farming DSS.	Global decisions in the entire food production chain.
Integration of IoT Solutions	Frameworks for facilitating integration of heterogeneous IoT solutions.	Seamless integration of IoT solutions.	Convergence of hybrid solutions and horizontal IoT platforms.

5. References

[1] M. Woolley, Bluetooth 5 - Go Faster. Go Further., online at: https://www.bluetooth.com/~/media/files/marketing/bluetooth_5-final.ashx?la=en

[2] E. Darmois, "High Priority IoT Standardisation Gaps and Relevant SDOs, to be retrieved via (visited in July 2018) https://aioti.eu/wp-content/uploads/2018/05/AIOTI-WG3_High_Priority_Gaps_v1.0_final.pdf, Version 1.0, AIOTI, May 2018

[3] "SmartM2M; IoT LSP use cases and standards gaps", ETSI TR 103 376 (STF 505), 10/2016. https://docbox.etsi.org/SmartM2M/Open/AIOTI/STF505

[4] ResinOS, online at: https://resinos.io

[5] Tata Communications, "India IoT Report – Emergence of a New Civic OS [Operating System]", February 2018, online at: https://www.tatacommunications.com/wp-content/uploads/2018/02/IoT-Report.pdf

[6] Intel, Intel IoT Platform, online at: http://www.intel.com/content/www/us/en/internet-ofthings/infographics/iot-platform-infographic.html

[7] CREATE-IoT D6.1, to be retrieved via (visited in July 2018) https://european-iot-pilots.eu/wp-content/uploads/2017/10/D06_01_WP06_H2020_CREATE-IoT_Final.pdf

[8] Mitsubishi Electric, e-Factory, November 2016, online at: http://app.mitsubishielectric.com/app/fa/download/search.do?kisyu=/sol/efactory&mode=catalog

[9] Infineon – NXP – STMicroelectronics – ENISA Common Position On Cybersecurity, 2016, online at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity

[10] Advancing IoT Platforms Interoperability, River Publishers, Gistrup, 2018, 978-87-7022-005-7 (ebook), IoT European Platforms Initiative (IoT-EPI) White Paper, online at: https://iot-epi.eu/wp-content/uploads/2018/07/Advancing-IoT-Platform-Interoperability-2018-IoT-EPI.pdf

[11] Edge intelligence, IEC White Paper, online at: http://www.iec.ch/whitepaper/pdf/IEC_WP_Edge_Intelligence.pdf

[12] STMicroelectronics intranet

[13] NarrowBand IoT, online at: https://en.wikipedia.org/wiki/NarrowBand_IOT

[14] M. Serrano and J. Soldatos 2015 IoT is More Than Just Connecting Devices: The OpenIoT Stack Explained September 8, 2015. https://iot.ieee.org/newsletter/september-2015/iot-is-more-than-just-connecting-devices-the-openiot-stack-explained.html

[15] LoRa Alliance, online at: https://www.lora-alliance.org/what-is-lora

[16] M. Serrano et al., IoT Semantic Interoperability: Research challenges, best practices, Recommendations and Next Steps. March 2015 http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Semantic_Interoperability_Final.pdf

[17] Open Container Initiative, online at: https://www.opencontainers.org/about

[18] ZigBee technology, online at: https://en.wikipedia.org/wiki/ZigBee

[19] ZWave Technology, online at: https://en.wikipedia.org/wiki/Z-Wave

[20] Organisation for Economic Co-operation and Development (OECD), "The Internet of Things: Seizing the benefits and addressing the challenges", May 2016, online at: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP%282015%293/FINAL&docLanguage=En

[21] B. Schneier, "Security and Function Creep", IEEE Security and Privacy, January/February 2010, https://www.schneier.com/essays/archives/2010/01/security_and_functio.html

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating IoT Innovation in Europe, bringing together small and large companies, start-ups and scale-ups, academia, policy makers and end-users and representatives of society in an end-to-end approach. We work with partners in a global context. We strive to leverage, share and promote best practices in the IoT ecosystems, be a one-stop point of information on all relevant aspects of IoT Innovation to its members while proactively addressing key issues and roadblocks for economic growth, acceptance and adoption of IoT Innovation in society.

AIOTI's contribution goes beyond technology and addresses horizontal elements across application domains, such as matchmaking and stimulating cooperation in IoT ecosystems, creating joint research roadmaps, driving convergence of standards and interoperability and defining policies. We also put them in practice in vertical application domains with societal and economic relevance.

AIOTI is a partner for the European Commission on IoT policies and stimulus programs, helping to identifying and removing obstacles and fast learning, deployment and replication of IoT Innovation in Real Scale Experimentation in Europe from a global perspective.

AIOTI is a member driven organisation with equal rights for all members, striving for a well-balanced representation from all stakeholders in IoT and recognizing the different needs and capabilities. Our members believe that we are the most relevant platform for connecting to the European IoT Innovation ecosystems in general and the best platform to find partners for Real Scale Experimentation.