3

IoT Digital Value Chain Connecting Research, Innovation and Deployment

Ovidiu Vermesan[1], Peter Friess[2], Patrick Guillemin[3], Martin Serrano[4], Mustapha Bouraoui[5], Luis Pérez Freire[6], Thomas Kallstenius[7], Kit Lam[8], Markus Eisenhauer[9], Klaus Moessner[10], Maurizio Spirito[11], Elias Z. Tragos[12], Harald Sundmaeker[13], Pedro Malo[14] and Arthur van der Wees[15]

[1]SINTEF, Norway
[2]European Commission, Belgium
[3]ETSI, France
[4]Digital Enterprise Research Institute, Galway, Ireland
[5]STMicroelectronics, France
[6]GRADIANT, Spain
[7]iMinds vzw, Belgium
[8]SAMSUNG Electronics Research and Development Institute, UK
[9]Fraunhofer FIT, Germany
[10]University of Surrey, UK
[11]ISMB, Italy
[12]FORTH, Greece
[13]ATB Institute for Applied Systems Technology Bremen, Germany
[14]FCT NOVA and UNINOVA, Portugal
[15]Arthur's Legal B.V., The Netherlands

"Productivity isn't about how busy or efficient you are – it's about how much you accomplish." Chris Bailey

3.1 Internet of Things Vision

Internet of Things (IoT) is considered one of the next industrial revolution enablers, which is fuelled by the advancement of digital technologies. IoT is dramatically changing how companies engage in business activities, and

how people will interact with their environment. Its disruptive nature requires the assessment of the requirements for the future deployment across the digital value chain in various industries and in many application areas.

IoT is a concept and a paradigm with different visions, and multidisciplinary activities. IoT considers pervasive presence in the environment of a variety of things, which through wireless and wired connections and unique addressing schemes are able to interact with each other and cooperate with other things to create new applications/services and reach common goals. In the last few years IoT has evolved from being simply a concept built around communication protocols and devices to a multidisciplinary domain where devices, Internet technology, and people (via data and semantics) converge to create a complete ecosystem for business innovation, reusability, interoperability, that includes solving the security, privacy and trust implications.

The IoT is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment. The confluence of efficient wireless protocols, improved sensors, cheaper processors, and a bevy of startups and established companies developing the necessary management and application software, has finally made the concept of the IoT mainstream. The IoT makes use of synergies that are generated by the convergence of Consumer, Business and Industrial Internet customer, Business and Industrial Internet. The convergence creates the open, global network connecting people, data, and things. This convergence leverages the cloud to connect intelligent things that sense

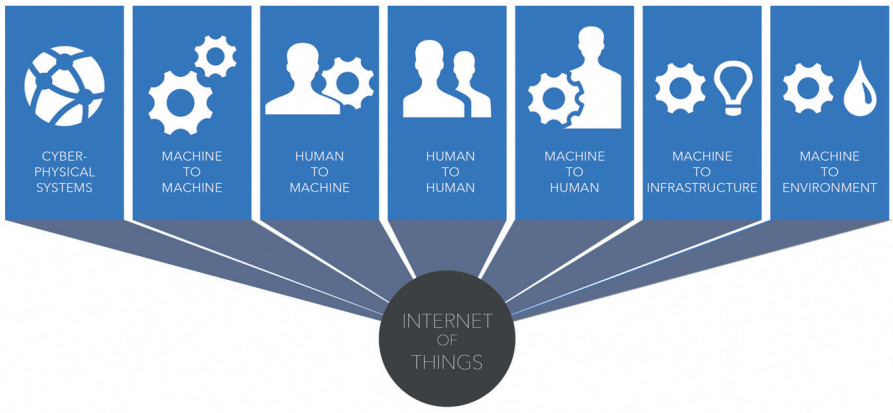

Figure 3.1 IoT integration.

and transmit a broad array of data, helping creating services that would not be obvious without this level of connectivity and analytical intelligence. The dynamics surrounding emerging IoT applications are very complex and issues such as enablement, network connectivity, systems integration, value-added services, and other management functions are all needs that generally must be addressed when the end-users seek to connect intelligent edge devices into complex IoT applications [59].

In this context, the research and development challenges to create a smart world are enormous. IoT ecosystems offer solutions comprising of large heterogeneous systems of systems beyond an IoT platform and solve important technical challenges in the different industrial verticals and across verticals.

IoT's disruptive nature requires the assessment of the requirements for the future deployment across the digital value chain in various industries and in many application areas considering even better exchange of data, the use of standardized interfaces, interoperability, security, privacy, safety, trust that will generate transparency, and more integration in all areas of the Internet (consumer/business/industrial).

IoT will generate even more data that needs to be processed and analysed, and the IoT applications will require new business models and product-service combinations to address and tackle the challenges in the Digital Single Market (DSM).

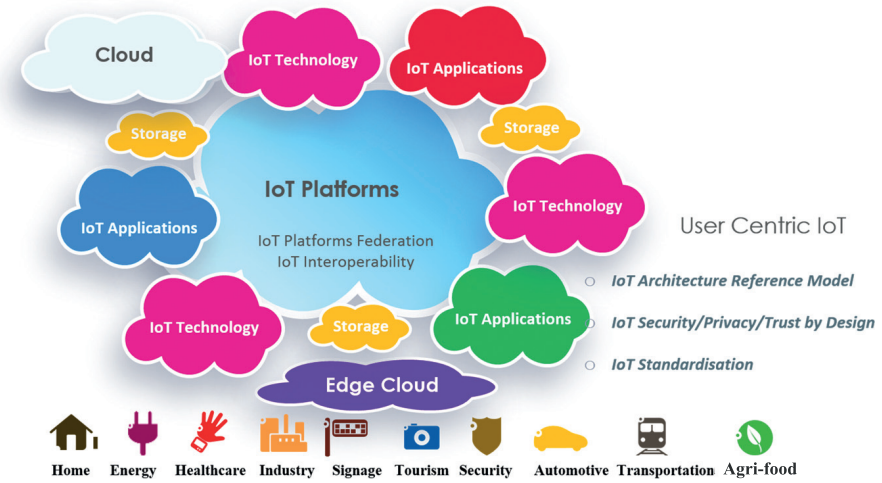

Figure 3.2 IoT platforms interaction and federation.

The use of platforms is being driven by transformative technologies such as cloud, things, and mobile. The IoT and services makes it possible to create networks incorporating the entire manufacturing process that convert factories into a smart environment. The cloud enables a global infrastructure to generate new services, allowing anyone to create content and applications for global users. Networks of things connect things globally and maintain their identity online. Mobile networks allow connection to this global infrastructure anytime, anywhere. The result is a globally accessible network of things, users, and consumers, who are available to create businesses, contribute content, generate and purchase new services.

Platforms also rely on the power of network effects, as they allow more things, they become more valuable to the other things and to users that make use of the services generated. The success of a platform strategy for IoT can be determined by connection, attractiveness and knowledge/information/data flow.

In this context, the Alliance for Internet of Things Innovation (AIOTI), was initiated following the European and global IoT technology and market developments.

The aim of AIOTI is to create and master sustainable innovative European IoT ecosystems in the global context to address the challenges of IoT technology and applications deployment including standardisation, interoperability and policy issues, in order to accelerate sustainable economic development and growth in the new emerging European and global digital markets. The AIOTI is connecting/integrating technologies and applications across the digital value chain and has strong links with the other European initiatives (Private Public Partnerships – PPPs, Joint Technology Initiatives – JTIs, European Innovation Partnerships – EIPs, etc.). The positioning of AIOTI in relation with the other initiatives is presented in Figure 3.3.

The members of AIOTI jointly work on the creation of a dynamic European IoT ecosystem. This ecosystem is building on the work of the IoT Research Cluster (IERC) and spill over innovation across industries and business sectors of IoT transforming ideas to IoT solutions.

The European Commission (EC) considers that IoT will be pivotal in enabling the DSM, through new products and services. The IoT, big data, cloud computing and their related business models will be the three most important drivers of the digital economy, and in this context it is fundamental for a fully functional single market in Europe to address aspects of ownership, access, privacy and data flow – the new production factor.

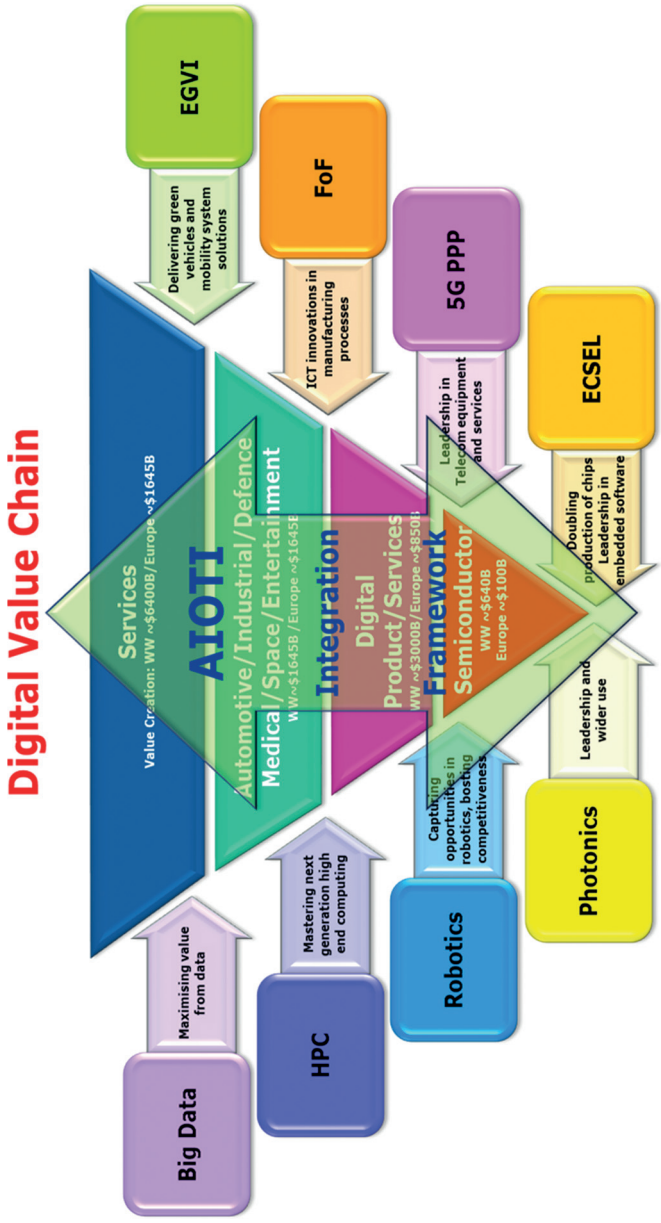

Figure 3.3 AIOTI integration framework.

3.1.1 IoT Common Definition

The IoT is a key enabling technology for digital businesses and one of the main drivers that is contributing to transform the Internet. IoT technologies are deployed in different sectors, from agricultural in rural areas, health and wellness to smart home and smart-X applications in cities.

The IoT is bridging the virtual, digital, physical worlds and mobile networks need to scale to match the demands of billions of things, while the processing capabilities require addressing the information provided by the "digital shadow" of these real things. This need focusing on the developments in the virtual world and the physical world for solving the challenges of IoT applications. In the virtual world, network virtualization, software-defined hardware/networks, device management platforms, edge computing and data processing/analytics are developing fast and urgency to be endeavoured as enabling technologies for IoT. Connecting the virtual, digital, physical worlds generates knowledge through IoT applications and platforms, while addressing security, privacy and trust issues across these dimensions.

Smart IoT applications modify the way people interact with the intelligent spaces (called also cyber-spaces), from how remotely control appliances at home to how the care for patients or elderly persons are performed. The massive deployment of IoT devices represents a tremendous economic impact and at the same time offers multiple opportunities. The IoT's potential is underexploited, the physical and intelligent are largely disconnected, requiring a lot of manual effort to find, integrate, and use information in a meaningful way. IoT and its advances in intelligent spaces advances can be categorised along with the key technologies at the core of the Internet.

Intelligent spaces are created and enriched by IoT and they are environments in which ICTs, sensor and actuator systems become embedded into physical objects, infrastructures, and the places embedded of technology that facilitate physical-human-cyber communication named intelligent surroundings or cyber places in which people live, (e.g. smart cities, industrial/manufacturing plants, homes and buildings, automotive and entertainment). The goal is to enable computers and smart edge devices to take part in activities never previously involved and people to interact with computers and these devices at the edge more naturally i.e. gesture, voice, movement, and context, etc. The IoT developments in the various sectors has created IoT ecosystems that are focusing on Internet of X technologies and applications that address the specific needs of the respective sector with the goal to be interoperable across various other sectors as presented in Figure 3.5.

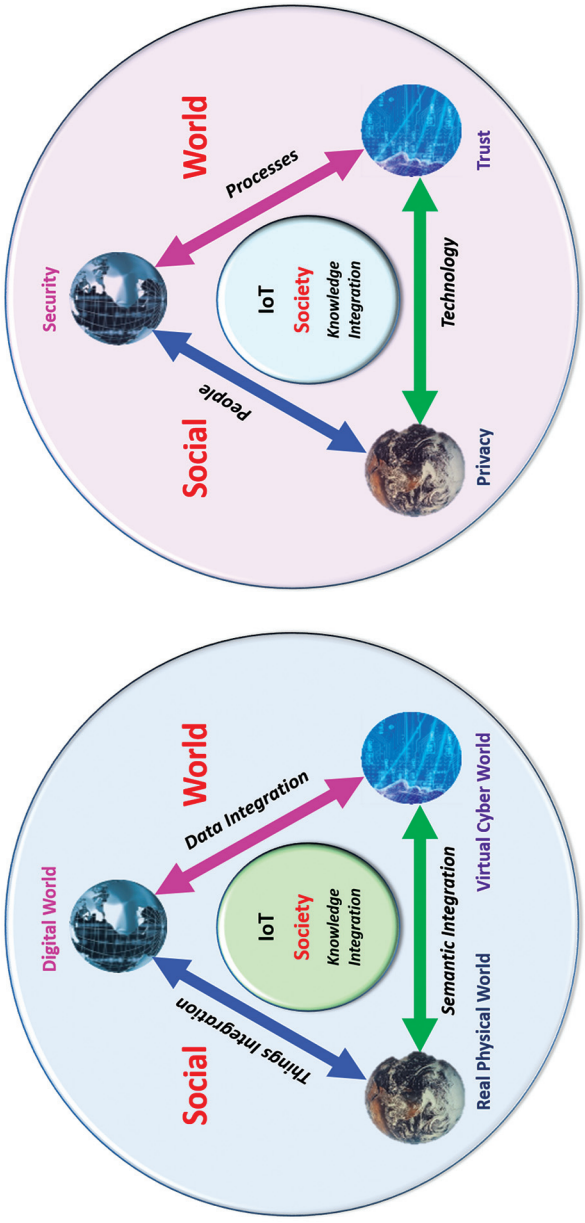

Figure 3.4 Integration.

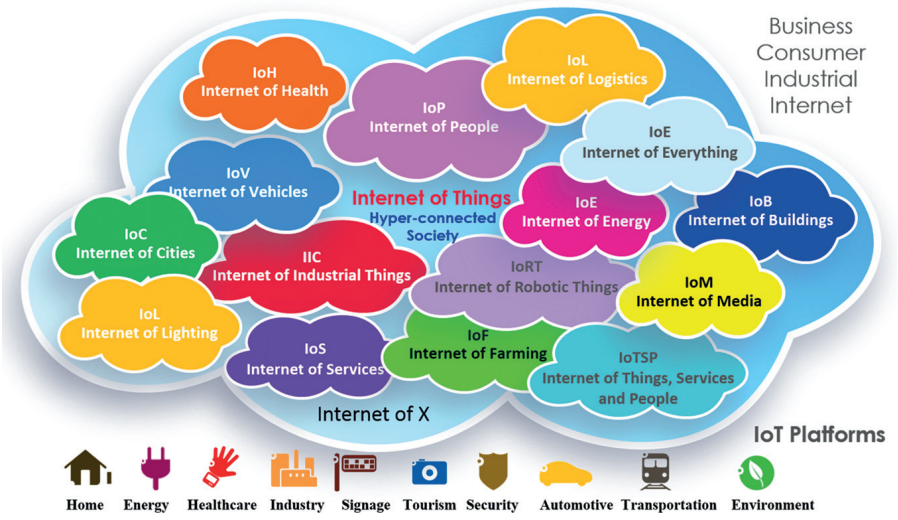

Figure 3.5 Internet of X developments in various industrial sectors.

The traditional distinction between network and device is starting to blur as the functionalities of the two become indistinguishable. Shifting the focus from the IoT network to the devices costs less, scales more gracefully, and leads to immediate revenues.

As a result of this convergence, the IoT applications require that classical industries are adapting and the technology will create opportunities for new industries to emerge and to deliver enriched and new user experiences and services.

In addition, to be able to handle the sheer number of things and objects that will be connected in the IoT, cognitive technologies and contextual intelligence are crucial. This also applies for the development of context aware applications that need to be reaching to the edges of the network through smart devices that are incorporated into our everyday life.

The Internet is not only a network of computers, but it has evolved into a network of devices of all types and sizes, vehicles, smartphones, home appliances, toys, cameras, medical instruments and industrial systems, all connected, all communicating and sharing information all the time.

The IoT has different meanings at different levels of abstractions through the value chain, from lower level semiconductor through the service providers. IoT is a paradigm with different visions, and involving multidisciplinary activities.

The IoT as a "global concept" requires a common high-level definition. Considering the wide background and required technologies, from sensing device, communication subsystem, data aggregation and pre-processing to the object instantiation and finally service provision, generating an unambiguous definition of the "IoT" is non-trivial.

The IERC is actively involved in ITU-T Study Group 13, which leads the work of the International Telecommunications Union (ITU) on standards for next generation networks (NGN) and future networks and has been part of the team which has formulated the following definition [42]: "Internet of things (IoT): A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled. NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

The IERC definition [45] states that IoT is "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 and use intelligent interfaces, and are seamlessly integrated into the information network".

3.1.2 Artificial Intelligence and Cognitive IoT

IoT applications are generating data collected from various domains and industrial sectors. The data generated provides insights from the environments and applications that generated it. Artificial Intelligence (AI) techniques provide the framework and tools to go beyond analytics of real time monitoring and automation use cases for IoT and move to IoT platforms that use concepts from artificial intelligence and apply them to specific IoT use cases to provide smarter decision-making. AI-enabled IoT applications add a new layer of functionality and access, creating the next generation of smart homes/buildings, smart vehicles, and smart manufacturing by providing intelligent automation, predictive analytics and proactive intervention.

In the IoT context, AI will support companies in finding the smart data and analyse the trends and patterns for better decision-making based on defined set of rules.

The AI techniques will enable cognitive systems to be integrated with IoT applications creating optimized solutions for each individual applications. Cognitive IoT technologies will allow embedding intelligence into systems and processes, allowing businesses to increase efficiency, find new business opportunities, and to anticipate risks and threats so they can better address them. The IoT applications will gather and integrate data from many types of sensors and other sources, reason over data, and learn from the interactions, while creating communities of devices that share information. The information collected can be interpreted and managed by people, IoT applications or IoT platforms using cognitive systems in order to generate new and better services and use cases.

The data generated by edge devices combined with the unstructured data available from sources ranging from news Web sites and social networks can be combined using cognitive IoT capabilities at the edge or at the cloud level.

The use on artificial intelligence, swarm intelligence and cognitive technologies together with deep learning techniques for optimising the IoT services provided by IoT applications in smart environments and collaboration spaces will create solutions capable of transforming industries and professions.

3.1.3 IoT of Robotic Things

IoT, artificial intelligence, robotics, machine learning, swarm technologies are the technologies that will provide the next phase of development of IoT applications. Robotics provide the programmed machines designed to be involved in labour intensive and repetitive work, while deep machine learning is the science of allowing/empowering machines to function using learning algorithms instead of programing. The combination of these disciplines opens the developments of autonomous systems combining robotics and machine learning for designing robotic systems to autonomous. Machine learning is part of advance state of intelligence using statistical pattern recognition, parametric/non-parametric algorithms, neural networks, recommender systems, swarm technologies etc. in order to perform autonomous tasks. The industrial IoT is a subset of the IoT, where edge devices, processing units and networks interact with their environments to generate data to improve processes.

The IoT, the technologies, architectures, and services that allow massive numbers of sensor enabled, uniquely addressable "things" to communicate with each other and transfer data over pervasive networks using Internet

protocols, is expected to be the next great technological innovation and business opportunity. Many IoT initiatives are focused on using connected devices with edge devices to manage, monitor and optimize systems and their processes. Advanced and transformational aspects of ubiquitous connectivity and communication include intelligent devices that monitor events, fuse sensor data from a variety of sources, use local and distributed "intelligence" to determine a best course of action, and then act to control or manipulate objects in the physical world, and in some cases while physically moving through that world. The concept called Internet of Robotic Things (IoRT), addresses the many ways IoT technologies and robotic "devices" intersect to provide advanced robotic capabilities, along with novel applications, and by extension, new business, and investment opportunities [17].

The combination of advanced sensing, communication, local and distributed processing, and actuation take the original vision for the IoT to

Figure 3.6 Internet of Robotic Things (IoRT) pervasive technology.

a wholly different level, and one that opens up completely new classes of opportunities for IoT and robotics solution providers, as well as users of their products. The concept allows to:

- Define and describe the characteristics of robotics technologies that distinguish them as a separate, unique class of IoT objects, and one that differs considerably from the common understanding of IoT edge nodes as simple, passive devices.
- Reveal how the key features of robotics technology, namely movement, mobility, manipulation, intelligence and autonomy, are enhanced by the IoT paradigm, and how, in turn, the IoT is augmented by robotic "objects" as "intelligent" edge devices.
- Illustrate how IoT and robotics technologies combine to provide for Ambient Sensing, Ambient Intelligence and Ambient Localization, which can be utilised by new classes of applications to deliver value.

IoT, cognitive computing and artificial intelligence are very important to the strategies for digital value chain integration addressing the implementation of IoT applications in various smart environments.

3.2 IoT Strategic Research and Innovation Directions

The IERC is bringing together EU funded projects with the aim of defining a common vision of IoT technology and addressing European research challenges. The rationale is to target at the large potential for IoT-based capabilities and promote the use of the results from the existing projects to encourage convergence of ongoing work to tackle the most important deployment issues and the transfer of research and knowledge to products and services and apply these in real IoT applications. The vison is illustrated in Figure 3.7 [59].

IoT is a new revolution of the Internet. Things make themselves recognizable and they obtain intelligence thanks to the fact that they can communicate information about themselves and they can access information that has been aggregated by other things.

The technological trend is a move from systems where there are multiple users/people per device, people in control loop of the system, and the system providing the ability for people to interact with people. The IoT brings a new paradigm where there are multiple devices per user; the devices are things that are connected and communicating with other things. The interaction will be with a heterogeneous continuum of users, things and real physical events

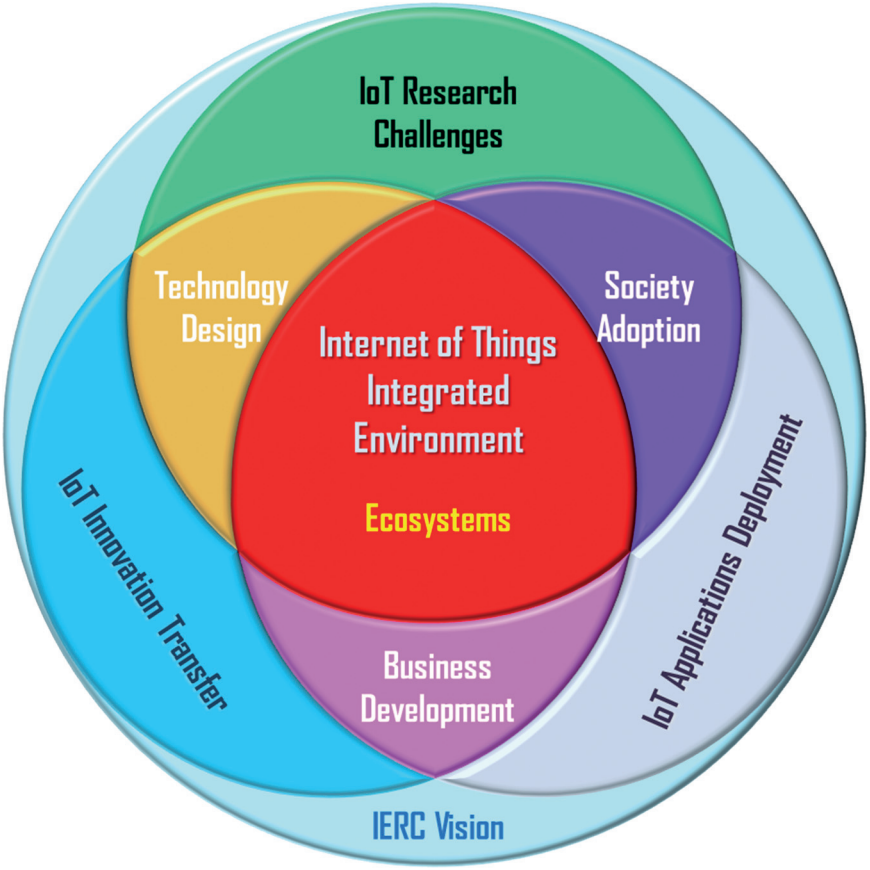

Figure 3.7 IERC Vison for IoT integrated environment and ecosystems.

(e.g., move left/right/up/down, change humidity/temperature/light/sound, etc.) and the Internet is the common convergence connectivity capability, replacing the previous independent systems.

The objectives of IERC is to provide the research and innovation trends, presenting the state of the art in terms of IoT technology and societal analysis in order to apply the develop to the IoT funded projects and further into the market applications and in the EU policies. The final goal is to test and develop innovative and interoperable IoT solutions in areas of industrial and public interest. The IERC objectives are addressed as an IoT continuum of research, innovation, development, deployment and adoption as presented in Figure 3.8 [59].

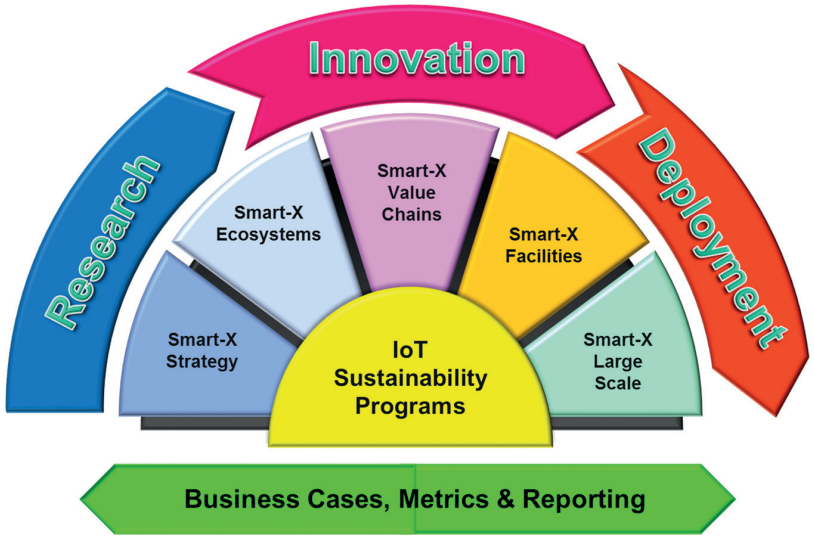

Figure 3.8 IoT continuum: research, innovation, deployment.

The IERC Strategic Research and Innovation Agenda (SRIA) is the result of a discussion involving the projects and stakeholders involved in the IERC activities, which gather the major players of the European ICT landscape addressing IoT technology priorities that are crucial for the competitiveness of European industry.

IERC SRIA covers the important issues and challenges for the IoT technology. It provides the vision and the roadmap for coordinating and rationalizing current and future research and development efforts in this field, by addressing the different enabling technologies covered by the IoT concept and paradigm.

The future IoT developments will address highly distributed IoT applications involving a high degree of distribution, and processing at the edge of the network by using platforms that that provide compute, storage, and networking services between edge devices and computing data centres. These platforms will support emerging IoT applications that demand real-time latency (i.e. mobility/transport, industrial automation, safety critical wireless sensor networks, etc.). These developments will bring new challenges as presented in Figure 3.9 [59].

The IoT value will come from the combination of edge computing and data centre computing considering the optimal business model, the right location, right timing, and efficient use of available network resources and bandwidth.

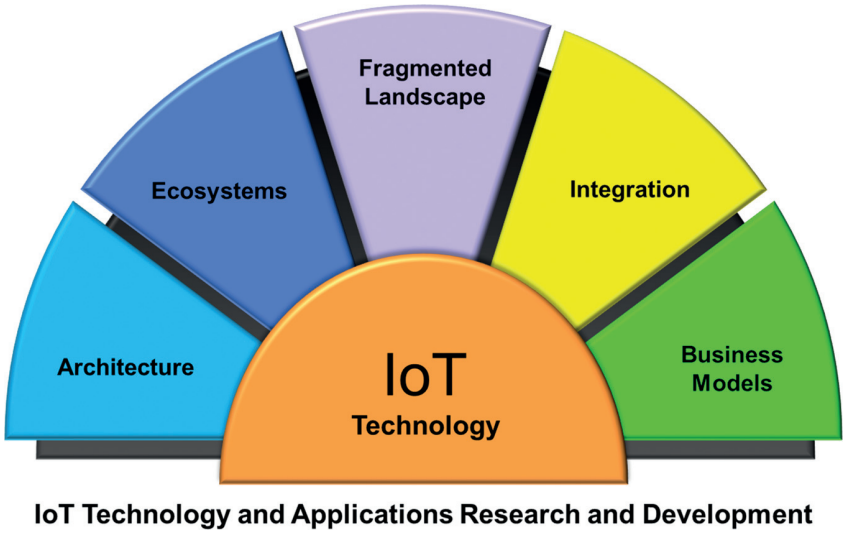

Figure 3.9 IoT future challenges.

The IoT architecture, like the Internet, will grow in evolutionary fashion from a variety of separate contributions and there are many current efforts regarding architecture models under development. The challenges for the IoT architecture are the complexity and cooperative work for developing, adopting and maintaining an effective cross-industry technology reference architecture that will allow for true interoperability and ease of deployment.

The IERC will work for providing the framework for the convergence of the IoT architecture approaches considering the vertical definition of the architectural layers end-to-end security and horizontal interoperability. IoT technology is deployed globally, and supporting the activities for common unified reference architecture would increase the coherence between various IoT platforms. A common architectural approach will require focusing on the reference model, specifications, requirements, features and functionality. In particular, this issue would be important in preparation of the future IoT LSPs, although time schedule might be difficult to synchronize.

The IERC SRIA is developed with the support of a European-led community of interrelated projects and their stakeholders, dedicated to the innovation, creation, development and use of the IoT technology.

Since the release of the first version of the IERC SRIA, we have witnessed active research on several IoT topics. On the one hand this research filled several of the gaps originally identified in the SRIA, whilst on the other it

created new challenges and research questions. Recent advances in areas such as cloud computing, cyber-physical systems, robotics, autonomic computing, and social networks have changed the scope of the Internet of Thing's convergence even more so. The Cluster has a goal to provide an updated document each year that records the relevant changes and illustrates emerging challenges. The updated release of this SRIA builds incrementally on previous versions [45, 46, 73] and highlights the main research topics that are associated with the development of IoT enabling technologies, infrastructures and applications with an outlook towards 2020 [51].

The research activities include the IoT European Platforms Initiatives (IoT-EPI) program that includes the research and innovation consortia that are working together to deliver an IoT extended into a web of platforms for connected devices and objects. The platforms support smart environments, businesses, services and persons with dynamic and adaptive configuration capabilities. The goal is to overcome the fragmentation of vertically-oriented closed systems, architectures and application areas and move towards open systems and platforms that support multiple applications. IoT-EPI is funded by the European Commission (EC) with EUR 50 million over three years.

The projects involved in the programs are listed in the Figure 3.10. The projects are part of the IERC and are cooperating to define the research and innovation mechanisms and identify opportunities for collaboration in IoT ecosystems to maximise the opportunities for common approaches to platform development, interoperability and information sharing. The common activities are organised under six task forces (Figure 3.11) that are conceived and developed under the IoT-EPI program.

The task forces are complementary to the IERC activity chains. The activity chains are created to favour close cooperation between the IoT Cluster projects, the IoT-EPI programme and the AIOTI working groups to form an arena for exchange of ideas and open dialog on important research challenges. The activity chains are defined as work streams that group together partners or specific participants from partners around well-defined technical activities that will result into at least one output or delivery that will be used in addressing the IERC objectives.

The research and innovation items addressed and discussed in the task forces of the IoT-EPI program, the IERC activity chains and the AIOTI working groups for the basis of the IERC SRIA that addresses the roadmap of IoT technologies and applications in line with the major economic and societal challenges underlined in the EU 2020 Digital Agenda [52].

Figure 3.10 IoT-EPI program projects.

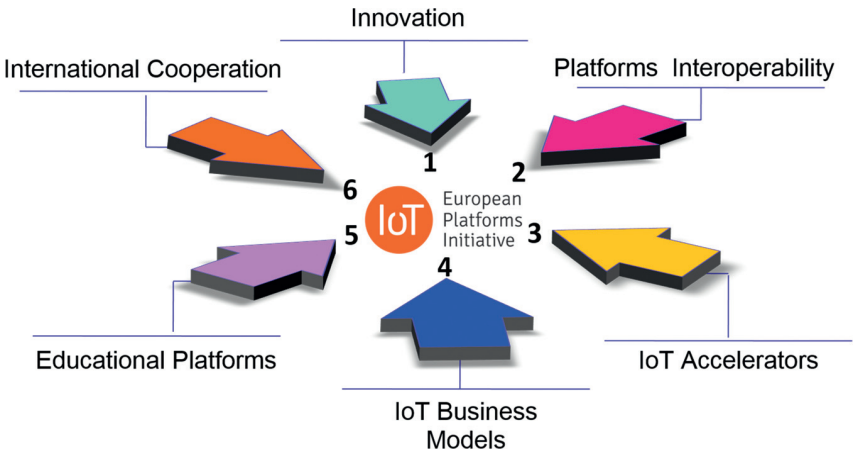

Figure 3.11 IoT-EPI task forces.

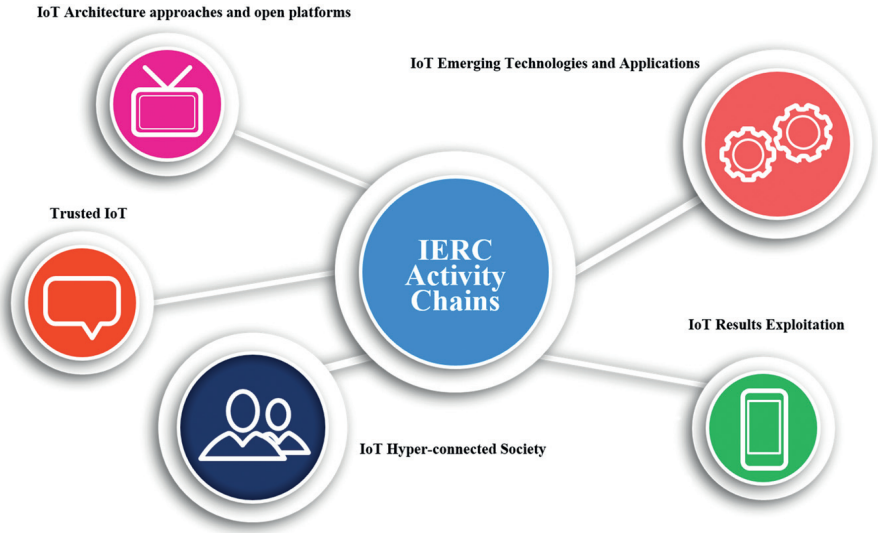

Figure 3.12 IERC activity chains.

The IERC SRIA is developed incrementally based on its previous versions and focus on the new challenges being identified in the last period.

The updated release of the SRIA is highlighting the main research topics that are associated with the development of IoT infrastructures and applications, with an outlook towards 2020 [51].

The timeline of the IERC IoT SRIA covers the current decade with respect to research and the following years with respect to implementation of the research results. As the Internet and its current key applications show, it is anticipated that unexpected trends will emerge leading to unforeseen new development paths.

The IERC has involved experts working in industry, research and academia to provide their vision on IoT research challenges, enabling technologies and the key applications, which are expected to arise from the current vision of the IoT.

The multidisciplinary nature of IoT technologies and applications is reflected in the IoT digital holistic view adapted from [32].

IoT demands an extensive range of new technologies and skills that many organizations have yet to master and creates challenges for organizations exploiting the IoT. The technologies and principles of IoT will have a very broad impact on organizations, affecting business strategy, risk management and a wide range of technical areas such as architecture and network design. The top 10 IoT technologies for 2017 and 2018 as presented by Gartner [21] are:

- IoT Security – due to hardware and software advances IoT security is a fast-evolving area through 2021 and the skills shortage today will only accelerate. Enterprises need to begin investing today in developing this expertise in-house and begin recruitment efforts. Many security problems

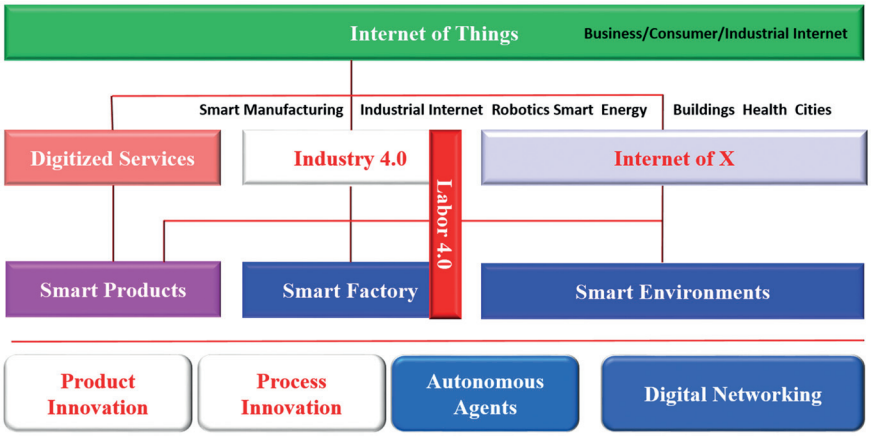

Figure 3.13 IoT digital holistic view across various industrial segments.

today are the result of poor specification, design, implementation and lack of knowledge/training. It is expected that the companies adopting IoT are investing in these areas.

- IoT Analytics – that require new algorithms, architectures, data structures and approaches to machine learning if organizations are going to get the full value of the data captured, and knowledge created. Distributed analytics architectures to capitalize on pervasive, secure IoT network architectures will evolve into become knowledge sharing networks.
- IoT Device Management – Significant innovation will result from the challenges of enabling technologies that are context, location, and state-aware while at the same time consistent with data and knowledge taxonomies. IoT Device Management will probably break the boundaries of traditional data management and create data structures capable of learning and flexing to unique inbound data requirements over time.
- Low-Power, Short-Range IoT Networks – Low-power, short-range networks will dominate wireless IoT connectivity through 2025, far outnumbering connections using wide-area IoT networks.
- Low-Power, Wide-Area Networks – traditional cellular networks cannot deliver a proper combination of technical features and operational cost for those IoT applications that need wide-area coverage combined with relatively low bandwidth, good battery life, low hardware and operating cost, and high connection density. Wide-area IoT networks aim is to deliver data rates from hundreds of bits per second (bps) to tens of kilobits per second (kbps) with nationwide coverage, a battery life of up to 10 years, an endpoint hardware cost of around $5, and support for hundreds of thousands of devices connected to a base station or its equivalent. The first low-power wide-area networks (LPWANs) were based on proprietary technologies, but in the long term, emerging standards such as Narrowband IoT (NB-IoT) will likely dominate this space.
- IoT Processors – low-end 8-bit microcontrollers will dominate the IoT through 2019 and shipments of 32-bit microcontrollers will overtake the 8-bit devices by 2020. The report does not mention the 16-bit processors ever attaining critical mass in IoT applications.
- IoT Operating Systems – a wide range of IoT-specific operating systems with minimal and small footprint will gain momentum in IoT through 2020 as traditional large-scale operating systems including Windows and iOS are too complex and resource-intensive for the majority of IoT applications.

- Event Stream Processing – some IoT applications will generate extremely high data rates that must be analysed in real time. Systems creating tens of thousands of events per second are common, and millions of events per second can occur in some telecom and telemetry situations. To address such requirements, distributed stream computing platforms (DSCPs) have emerged. They typically use parallel architectures to process very high-rate data streams to perform tasks such as real-time analytics and pattern identification.
- IoT Platforms – IoT platforms bundle infrastructure components of an IoT system into a single product. The services provided by such platforms fall into three core categories: (1) low-level device control and operations such as communications, device monitoring and management, security, and firmware updates; (2) IoT data acquisition, transformation and management; and (3) IoT application development, including event-driven logic, application programming, visualization, analytics and adapters to connect to enterprise systems.
- IoT Standards and Ecosystems – ecosystems and standards are not precisely technologies, most eventually materialize as application programming interfaces (APIs). Standards and their associated APIs will be essential because IoT devices will need to interoperate and communicate, and many IoT business models will rely on sharing data between multiple devices and organizations.

Many IoT ecosystems will emerge, and commercial and technical battles between these ecosystems will dominate areas such as the smart home, the Smart City and healthcare. Organizations creating products may have to develop variants to support multiple standards or ecosystems and be prepared to update products during their life span as the standards evolve and new standards and related APIs emerge.

The IERC IoT SRIA addresses these IoT technologies and covers in a logical manner the vision, the technological trends, the applications, the technology enablers, the research agenda, timelines, priorities, and finally summarises in two tables the future technological developments and research needs.

The field of the IoT is based on the paradigm of supporting the IP protocol to all edges of the Internet and on the fact that at the edge of the network many (very) small devices are still unable to support IP protocol stacks. This means that solutions centred on minimum IoT devices are considered as an additional IoT paradigm *without IP to all access edges*, due to their importance for the development of the field.

3.3 IoT Smart Environments and Applications

The IERC vision is that "the major objectives for IoT are the creation of smart environments/spaces and self-aware things (for example: smart transport, products, cities, buildings, rural areas, energy, health, living, etc.) for climate, food, energy, mobility, digital society and health applications" [45].

Today, there is a strong acceleration in the evolution of connected devices, with accelerating scale and scope, as well as higher focus on interoperability. IoT technologies and applications put more and more emphasis on integration of sensors, devices and information systems across industry verticals and organisations to transform operations and enable creation of new business models. IoT technologies focus on gaining new insights from analytics based on data from diverse sources to support decision-making, and improve products, services and experiences for end users. It is envisaged that our environment becomes increasingly "smart" by using this network of connected sensors.

Increasingly complex IoT solutions require more advanced communication platforms and middleware that facilitate seamless integration of devices, networks and applications. In this context, the emergence of IoT platforms with multiple functionalities (i.e. connectivity management, device management, application enablement, etc.) developed for the purpose of supporting and enabling IoT solutions enables rapid development and lower costs by offering standardised components that can be shared across multiple solutions in many industry verticals.

The IoT applications however will gradually move from vertical, single purpose solutions to multi-purpose and collaborative applications interacting across industry verticals, organisations and people, being one of the essential paradigms of the digital economy. Many of those applications still have to be identified and involvement of end-users in this innovation is crucial.

Digital economy enables and conducts the trade of goods and services through electronic commerce on the internet. The digital economy is based on three pillars: supporting infrastructure (hardware, software, telecoms, networks, etc.), e-business (processes that an organisation conducts over computer-mediated networks) and e-commerce (transfer of goods online) [5].

This definition needs to be extended as IoT applications and technologies are more and more embedded in our society. Economic activities classified as "digital economy" are expanding their scale, and are becoming diversified in their transaction forms with many companies in providing product and service hybrids. Intelligent physical goods as part of IoT applications are capable of connecting, capture and producing "smart" data and information

for use in digital services without human interventions. In this context, physical equipment has measuring and communication capabilities, data consciousness and processing capabilities and the digital economy will be driven by IoT "system of systems" interactions where new business models and product-service combinations are aligned with customers that are integrating the concept of product-as-a-service and product-as-an-experience.

IoT is expected to boom in many sectors, such as smart buildings and cities, in the energy sector, in safety and security management, transportation, healthcare, farming and many more, thereby bringing huge business opportunities and jobs in those sectors as well as in the enabling industries (data centres, communications and information technology).

The IoT applications are addressing the societal needs and the advancements to enabling technologies such as nanoelectronics and cyber-physical systems continue to be challenged by a variety of technical (i.e., scientific and engineering), institutional, and economical issues.

IERC is focusing on applications chosen as priorities for the next years and the Cluster provides the research challenges for these applications. While the applications themselves might be different, the research challenges are often the same or similar.

Every industry is being disrupted by IoT, the universe of intelligent devices, processes, services, tools and people communicating with each other as part of a global ecosystem. As technology evolves, products, homes, enterprises and entire cities will be continuously connected as presented Figure 3.14. This represents fundamental change for the insurance industry:

Figure 3.14 The IoT is connecting homes, cars, people, organizations and even entire cities [9].

How are things insured? With what partners? Which services and enabling technologies? The answers to these questions are the first steps toward the development of new and innovative business models. The IoT is driving a connected, as-a-service economy, and traditional insurers must adapt quickly, deciding whether to move up or out. Insurers will need to dramatically reshape their business model, combining insurance with technology, ecosystem services and partners. Insurers are about to become "Insurers of Things" [9].

This new dimension has to be consider for IoT use cases and applications covering various domains and even more when we consider cross-domain applications and implementations.

3.3.1 Wearables

Wearables are integrating key technologies (e.g. nanoelectronics, organic electronics, sensing, actuating, communication, low power computing, visualisation and embedded software) into intelligent systems to bring new functionalities into clothes, fabrics, patches, watches and other body-mounted devices.

These intelligent edge devices are more and more part of integrated IoT solutions and assist humans in monitoring, situational awareness and decision-making. They can provide actuating functions for fully automated closed-loop solutions that are used in healthcare, well-being, safety, security, infotainment applications and connected with smart buildings, energy, lighting, mobility or smart cities IoT applications. Many people already use wearables to monitor their activity level or as a fashion accessory. For example, many of us have a fitbit or a smartwatch.

Creating a seamless user experience is essential for wearable application success. In the future, wearable devices will be more pervasive (e.g. embedded in clothes or pills) and more multifunctional (smartwatches that open doors, start cars and so on) and will become an essential part of people's life.

The IoT applications market in Europe and in the world is moving very fast towards industrial solutions, e.g. smart cities, homes, buildings. The IoT markets have multiple shapes, from simple smart-X devices to complete ecosystems with a full value chain for devices, applications, toolkits and services. Wearables' worldwide market has been identified as the opportunity to materialize what the IoT area has not addressed yet in terms of business creation and commercialization of devices "things", software platforms,

Figure 3.15 Wearables defining priorities for European market.

applications and complete IoT solutions. "Wearables will become the world's best-selling consumer electronics product after smartphones", according to Euromonitor [4]. In the same study the big estimation for sales of wearables are projected to exceed 305 million units in 2020, with a compound annual growth rate (CAGR) of 55 percent during the next five years. Following this big estimation, yet at the Wearables area there is a need for a catalyst that looks for the wider deployment and market uptake of novel/emergent wearables-based IoT applications, technologies and platforms.

The market for wearable computing is expected to grow six-fold, from 46 million units in 2014 to 285 million units in 2018 [36].

Because of wearables are associated to daily life activities and the tendency is to personalise them, following art and design influenced (user-centric) approaches is also crucial. Wearables and its "wear" nature (mobility) will transform diverse sectors such as the healthcare, wellbeing, work safety, public safety and leisure. By involving end users in the creation, the design of

Figure 3.16 Common wearables on the market.

wearables and the identification of services needs, it is expected an exponential growth in the ecosystem for wearables market application.

Wearable technology has been there since early 80's, however the limitation in technology and the high cost on materials and manufacturing generated that wearable ecosystem(s) lost acceptance and stop its grow at that early stage. In todays' technology and economy conditions where technology has evolved and manufacturing cost being reduced Wearable Technology is the best channel for user acceptance and deployments in large user communities. In wearables co-existence with IoT systems and deployed technologies will mark the difference using today's user experience and accelerating tomorrow's user acceptance that is reflected in return on investment by focusing in the most common wearable devices.

Demands in technologies and platforms (supply side) require further work to cope with interoperability, design and arts for user adoption, technology and management and business modelling. In the other hand from users and communities (demand side) it is required to pay attention in reliability of devices, cross-domain operation, and cost reduction and device reusability.

Today's biggest challenges for wearable technology is the reticence to use wearables for privacy or data protection concerns, or the fatigue of using a wearable. In addition, other operational issues also exist such as having the necessary ecosystem in place to support wearable devices, which act as a barrier to deployment, service development or take up. Creating products which meet both end-users need and which create value for the suppliers and users will ensure viable business cases. Wearable devices, which can take or recommend an action based on real time data analysis and perform more than one function (e.g. pain monitoring/treatment that also serves as a security verification that open doors) are more likely to be taken up by different groups of users. They are also more likely to consider them as essential part of their life.

Fitness tracking is the biggest application today and this opens the opportunities for watches that are capable of tracking blood pressure, glucose, temperature, pulse rate and other vital parameters measured every few

seconds for a long period of time to be integrated in new kinds of healthcare applications. Glasses for augmented reality can be another future wearable application.

Healthcare industry is taking huge advantage of smart technology for mobile devices and smart wearables is looking to be a big and profitable market. Smart technology that will be the key to the optimal operating of our future society, especially when it comes to healthcare. Some of the smart wearables, already on the market, or in progress engineered for the healthcare industry have the following features [29]:

- Asthma monitoring and management device with companion app currently in design and production phase, offering real time data and alerts when an asthma situation is experienced, offering journaling, treatment plans, displays and tracking and information on the treating of symptoms
- Device attached to a person's back with a companion app, used to lower back pain and treatment with video game like interactions and interface that give the user exercises to do
- Knee brace with companion app giving stability and pain relief using an electrode placed inside of the brace
- Reusable biosensor embedded in a disposable patch with ECG electrodes and accelerometer monitoring heart rate, breathing, temperature, steps, and body position
- Wearable, wireless ECG monitor under development, strapped around the chest to monitor hearth health and health status, with activity tracking monitoring, a companion app, and connection to a cloud based system allowing a doctor to monitoring a patient in real time
- Pill with ingestible sensor technology to be swallowed, powered by the stomach fluids and sending information of your body's physiologic responses and behaviours to a body-worn and disposable patch which can detect heart rate, activity, and rest, and send information to a mobile device. Information if a patient has taken his prescribed medicines at the correct time and how the patient is responding to the therapies
- Smart device helping people to quit smoking by sensing a person's craving for cigarette/nicotine and then deliver medication to curtail the craving, in addition to giving information about quitting and coaching by a companion app
- Smart contact lenses measuring the glucose levels in the wearer's tears, transmitting this information wirelessly to connected smartphones

- Smart contact lenses under development helping restoring the eye's natural autofocus on near objects for people suffering from vision loss occurring with age
- Smart bra and app under development with sensors embedded to sense the conditions and rhythms in breast tissue to alert of the possibility of cancer
- Diabetes sensors placed on the back of the upper arm for 14 days, reading glucose information and transferring this to a companion app, which also give information about the food people should eat, exercise and proper dieting
- Hospital ulcer monitor put on a patient giving the caregiver an alert if the patient is moving around wrong or if they may need some assistance in moving the proper way to prevent ulcer
- Smart watch with medical grade sensors for kids with certain ailments such as epilepsy with real time data sent to a companion app giving alerts and other goals and health information.

The wearable technology market in Europe remains an emerging market that is expanding across numerous sectors and promises to create new markets and deliver important societal benefits. Research from CCS Insight shows that, based on current trajectories, the Global Wearables market is expected to triple by 2019. AIOTI WG07 [65] saw Europe's natural strengths in privacy, data protection as well as in ubiquitous broadband availability enabling Europe to be a strong global competitor in the wearable technologies and solutions sector. If we add Europe's good brand name and talent in style and fashion then we can claim that Europe can be a leader in the market of wearables.

3.3.2 Smart Health, Wellness and Ageing Well

Healthcare and wellness offer unique opportunities for comprehensive IoT implementation. Health care treatments, cost, and availability affect the society and the citizens striving for longer, healthier lives. IoT is an enabler to achieve improved care for patients and providers. It could drive better asset utilization, new revenues, and reduced costs. In addition, it has the potential to change how health care is delivered.

The emergence of Internet of Health (IoH) applications dedicated to citizens health and wellness that spans care, monitoring, diagnostics, medication administration, fitness, etc. will allow the citizens to be more involved with

their healthcare. The end-users could access medical records, track the vitals signals with wearable devices, get diagnostic lab tests conducted at home or at the office building, and monitor the health-related habits with Web-based applications on smart mobile devices. The application of IoT in healthcare can improve the access of care to people in remote locations or to those who are incapacitated to make frequent visits to the hospital. It can also enable the prompt diagnosis of medical conditions by measuring and analysing a person's parameters. The medical treatment administered to the person under care can be improved by studying the effect of a therapy and the medication on the patients' vitals.

The IoT healthcare applications require a careful balance between data access and sharing of health information vs. security and privacy concerns. Some information could be shared with a physician, while other type of information, will be not accepted to be provided divulge. For these applications, there is a need to have paradigm shift in human behaviour in order for patients to evolve, adapt and ultimately embrace what the IoT technology can provide, a secure Internet domain that can host all health information and push important health data back to the patient and their healthcare providers [59]. The state of health in a population can be best measured by focusing on metabolic syndromes with a set of clear and staged health actions attached to it in order to fight the consequences of such modern lifestyle. If not changed, this lifestyle often results in an early progression of those diseases (as shown in Figure 3.17) [63].

The population of people over 60 is growing at a faster rate than the rest of the population. Unlike previous generations, more seniors will stay at home. In the future IoT technology might allow older people to retain independence with a choice to keep family informed when help is needed. Silver Economy is defined as "an environment in which the over-60 interact and thrive in the workplace, engage in innovative enterprise, help drive the marketplace as consumers and lead healthy, active and productive lives" [71]. There are three groups in the ageing population, depending on their health, i.e. active, fragile and dependent while each of these groups have their own need patterns. At country level differences in needs patterns exist, i.e. depending on the local environment, with the existence of models for care, governmental policy and needs at European geographical levels, i.e. Nordic, Anglo-Saxon, Continental, South-European and Eastern-European. The Silver Economy is related to concepts such as "active and health ageing", "ambient assisted living", "e-health", "age management", "smart care" etc.

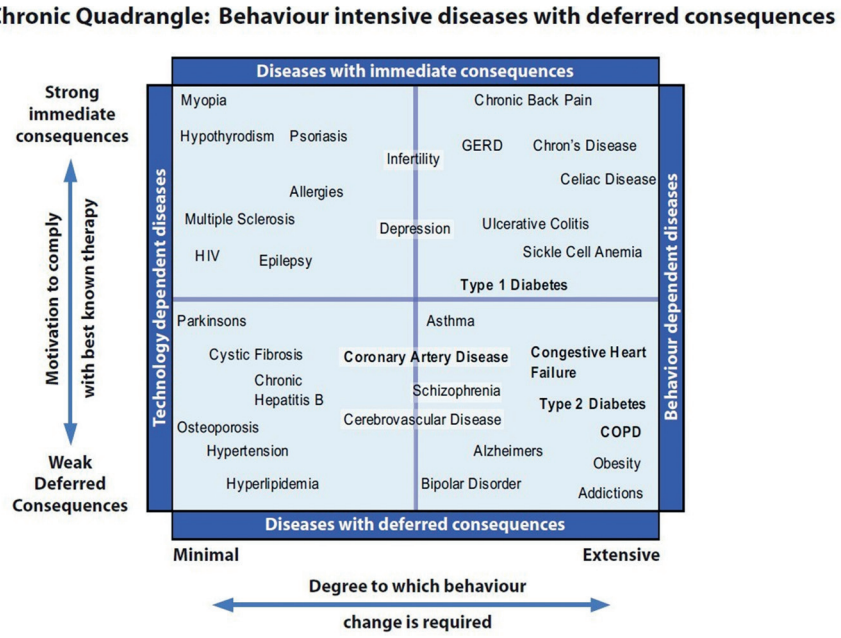

Figure 3.17 Chronic quadrangle.

and depends on the perspective taken or challenge/solution emphasised, using different taxonomies.

Demographic change, the rising incidence of chronic disease, unmet demand for more personalised care, and cost pressure are trends requiring a new, integrated approach to health and social care. Such integration – if brought about in the right manner – has the potential to improve both the quality, security and the efficiency of care service delivery. Potentially this can be to the benefit of all: beginning with elder people in need of care and their family and friends, and including care professionals, service provider organisations, payers and other governance bodies. Within this ongoing change process, the challenge is how to adopt relevant and secure IoT technologies to realise care integration and avoid that telecare, telehealth and other IoT applications in this field remain locked up in segregated silos, mirroring the overall situation of today. In order to capture all the complexity of the ambient assisted living (AAL) market scenario, the previous definition was taken into account as a starting point but have also taken into account a technology view, based on the technology stack supporting the AAL solutions.

IoT applications are pushing the development of platforms for implementing AAL systems that will offer services in the areas of assistance to carry out daily activities, health and activity monitoring, enhancing safety and security, getting access to medical and emergency systems, and facilitating rapid health support.

The main objective is to enhance life quality for people who need permanent support or monitoring, to decrease barriers for monitoring important health parameters, to avoid unnecessary healthcare costs and efforts, and to provide the right medical support at the right time.

The IoT plays an important role in healthcare applications, from managing chronic diseases at one end of the spectrum to preventing disease at the other.

The smart living environments at home, at work, in public spaces should be based upon integrated systems of a range of IoT-based technologies and services with user-friendly configuration and management of connected technologies for indoors and outdoors.

These systems can provide seamless services and handle flexible connectivity while users are switching contexts and moving in their living environments and be integrated with other application domains such as energy, transport, or smart cities. The advanced IoT technologies, using and extending available open service platforms, standardised ontologies and open standardised APIs can offer many of such smart environment developments.

The IoT technology not only overcomes the inconvenience of distance, but also provides people with greater choice and control over the time and the place for monitoring their condition, increasing convenience and making their conditions more manageable. At the same time, it also reduces some of the pressures on clinics and acute hospitals. IoT could make a significant contribution to the management of a number of chronic conditions, heart failure, hypertension, asthma, diabetes and can be integrated with other living environments domains such as mobility, home/buildings, energy, lighting, cities.

Many elderly people are adopting technology more than ever, and in the process, they face unique barriers to usage because they previously had not used them in work situations and commonly have physical limitations that make using computer and the Internet more difficult. The improvement in the IoT technology and user interfaces can lower the barriers and help the elderly people to adopt the technology since many of these people are enthusiastic and express strong openness to learning.

As the population ages, and as the digital health field expands, IoT technologies addressing the unique challenges of aging in place is becoming a reality.

Many elderly people want to age in place and need to be as independent as possible, while the IoT technology provides cognitive aids for independent living. Old people with Alzheimer's, dementia, or memory loss receive help with tasks through cueing, scheduling assistance and finance safety for seniors by on and off switches for caregivers or relatives to help aging people manage their money by blocking purchases, setting spending limits, sending alerts about suspect charges, etc. IoT activity sensors monitor movements in the home and medicine boxes give medication reminders, keep track of steps, and include an emergency button.

The IoT allows building up an archive of patient behaviour in their own home that will enable local analytics to produce probability curves to predict usual and unusual behaviour. Using this, a more accurate prediction of unusual behaviour can be detected that is used to trigger alerts to patients, family and carers, while helping elderly patients stay out of hospital (and thus significantly reduce the cost of hospital admissions).

In this context, there is a need for fundamental shift in the way we think about older people, from dependency and deficit towards independence and well-being. Older people value having choice and control over how they live their lives and interdependence is a central component of older people's well-being. They require comfortable, secure homes, safe neighbourhoods, friendships and opportunities for learning and leisure, the ability to get out and about, an adequate income, good, relevant information and the ability to keep active and healthy. They want to be involved in making decisions about the questions that affect their lives and the communities in which they live. They also want services to be delivered not as isolated elements, but as joined-up provision, which recognises the collective impact of public services on their lives. Public services have a critical role to play in responding to the agenda for older people.

Within this ongoing change process, advanced IoT technologies provide a major opportunity to realise care integration. At the same time, telecare, telehealth and other IoT applications in this field also remain locked up in segregated silos, mirroring the overall situation.

These IoT technologies can propose user-centric multi-disciplinary solutions that take into account the specific requirements for accessibility, usability, cost efficiency, personalisation and adaptation arising from the application requirements.

3.3.3 Smart Clothing

Smart textile, e-fabrics, smart clothing will be produced in all kinds of types and with different features and outlooks and in many cases will embed the features and functionalities of wearable devices of today. The common factor is that smart textiles are made to observe to the wearer, and to react to environmental conditions including chemical, mechanical, electrical, chemical, and magnetic, etc. Intelligent fabrics have digital components, sensors, actuators, circuits, and computers embedded in them to collect process and output data in different ways.

Smart clothing will include many features and different smart solutions are expected on the market in the next years [30, 31]:

- Smart shirt with app, keeping information in 3D showing if too much pressure is put on a certain part of the body, keeping track of your performance, giving information to prevent getting injured while training, with real time feedback
- Health related smart shirt measuring heart rate, breathing rate, sleep monitoring, workout intensity measurements
- Bio sensing silver fibres woven into the shirt
- Clothing to track the amount of calories burned
- Clothing to track movement intensity during workout
- Compression fabric that aids in blood circulation and with muscle recovery
- Body monitor sensors – embedded micro sensors throughout the shirt keeping track of temperature, heart beat and heart rate, and the speed and intensity of your workouts
- Shirt able to keep the measured biometrics information by using a small black box woven into the shirt
- Clothing with moisture control and odour control
- Smart shirts can be used in hospitals for monitoring heart beat and breathing in patients
- Baby monitoring – baby garment telling if the baby is sleeping and monitoring the baby's vital signs
- Baby outfit with sensors and a small monitor on it
- Smart socks for baby, monitoring the baby's breath with alert features
- Eco-friendly solar garments as it harnesses the energy of the sun and enables the wearer to charge the owner's phone, music players, and other powered electronic devices

- Adaptive survival clothing that uses moisture and temperature regulation properties of wool to adapt the human body to normal, non-threatening conditions.

The combination of these "devices" embedded in the clothing with other IoT devices that are monitoring the environment will create new opportunities, new use cases, and business models across various sectors.

3.3.4 Smart Buildings and Architecture

Buildings consume 33% of world energy, this figure grows to 53% of world electricity, and it will continue to grow in the future. As a result, buildings have an important weight in regards to the energy challenge.

Improving life of the occupants implies many aspects including comfort with light, temperature, air quality, having access to services facilitating life inside the building, adapting the behaviour to the needs of the occupants. There is also a direct economic interest to do it as it is recognized that productivity level is connected to the comfort level.

For being energy efficient, the consumption can be optimized locally while taking into account the needs of the occupants and the hosted processes. Buildings can also produce energy from different sources such as Photovoltaic panels and store energy for future usage. This energy can be used internally or given back to the grid. In addition, buildings are not isolated islands but part of larger ecosystem at the district or even city level. The energy price can change over time and have an impact on the energy optimization. It could happen also that the optimization is better driven at a more global level, set of buildings or district for instance. In the smart building implementations, it is necessary to simplify the management, control and maintenance of buildings during the whole life cycle, starting from the design phase. This should lead to much better process efficiency while driving down the operation costs (OPEX).

As a result there is a strong need to leverage on technology and IoT for making buildings smarter, improve life of the occupants (personal or at work), make the buildings more energy efficient, and facilitate the management and maintenance of the building during its whole life cycle. This has to be done not only with the new constructed buildings but also with the existing ones through adequate retrofit solutions. It is important to keep in mind that new construction represents only 2% of the total installed base each year.

The different ingredients of IoT, connectivity, control, cloud computing, data analytics, can all contribute to make smarter buildings (offices, industrial, residential, tertiary, hotels, hospitals, etc.):

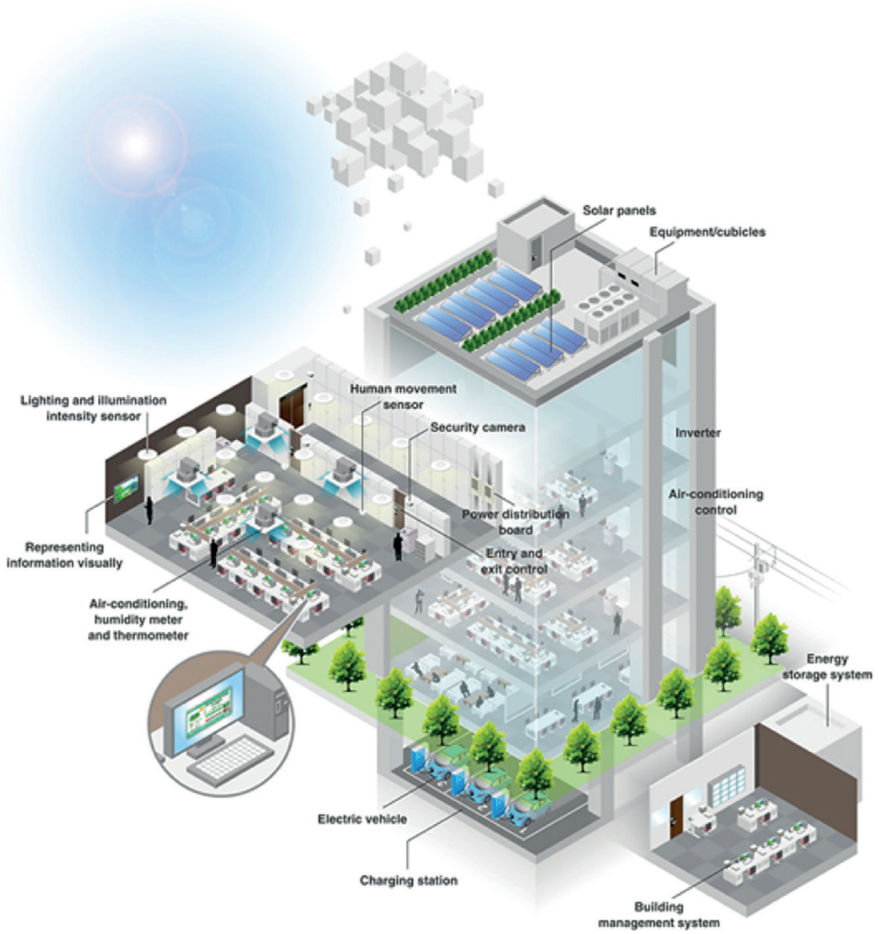

Figure 3.18 Smart building implementation [72].

- Connected to the grid ("smart grid ready")
- Connected to the Smart City
- Energy efficient while taking care of the comfort of the occupants
- Adaptable to the changing needs of the occupants over time
- Providing services for a better life of the occupants
- Easy to maintain during the whole life cycle at minimal cost

The solutions focus primarily on environmental monitoring, energy management, assisted living, comfort, and convenience. The solutions are based on open platforms that employ a network of intelligent sensors to provide information about the state of the home. These sensors monitor systems such

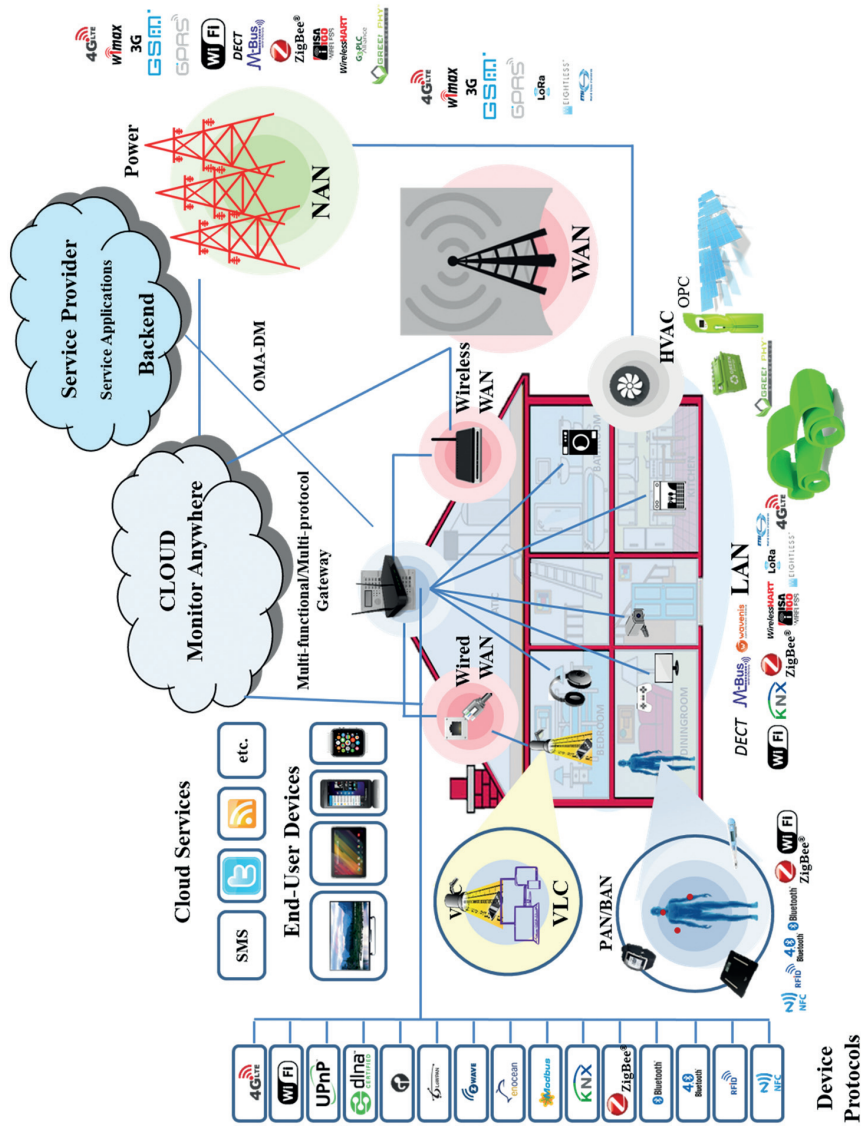

Figure 3.19 Home equipment and appliances [59].

as energy generation and metering; heating, ventilation, and air-conditioning (HVAC); lighting; security; and environmental key performance indicators.

The networking aspects are bringing online streaming services or network playback, while becoming a mean to control of the device functionality over the network.

Integration of cyber-physical systems (CPS) both within the building and with external entities, such as the electrical grid, requires stakeholder cooperation to achieve true interoperability. Maintaining security will be a critical challenge to overcome in smart buildings IoT applications [71].

In the IoT ecosystems, the collaboration among various stakeholders to optimise the smart buildings allow operators of buildings to find ways to conserve energy for both environmental and economic reasons, while architects and builders, are trying to make new buildings as "green" as possible.

IoT technologies are extending today's building automation and transforming the smart buildings and facilities through IoT platforms providing intelligence, security, modularity, and intuitive interfaces that allow autonomous operations. The evolution of building system architectures includes an adaptation level that will dynamically feed the automation level with control logic, i.e. rules, using algorithms and rules as Web resources in a similar way as for sensors and actuators.

The market sizing and opportunities for smart commercial buildings; is increasing and Memoori report "The Internet of Things in Smart Buildings 2014 to 2020" [33] makes an objective assessment of the market for IoT Technologies, Networks and Services in Buildings 2014 to 2020. Market figures indicate that the overall market for systems in buildings will grow from $110.9Bn in 2014 to $181.1Bn in 2020, with Physical Security, Lighting Control and Fire Detection and Safety representing the three largest segments. In order to calculate the technical market potential for the IoT in Buildings.

The report has assessed the additional cost requirement of adding connectivity through sensors to existing or newly installed building systems, as well as projecting the growth in related network hardware and IoT data services that the IoT in Buildings would enable to generate. The report therefore projects that the global market for the IoT in Buildings will rise from $22.93Bn in 2014 to over $85Bn in 2020. In this context, the following estimates are made:

- Overall connectivity penetration rates across all building systems are at only around 16%. This connectivity penetration rate will rise steadily over the coming years, but mainstream penetration, i.e. 50% of all building systems devices connected, is unlikely to be achieved before 2025.

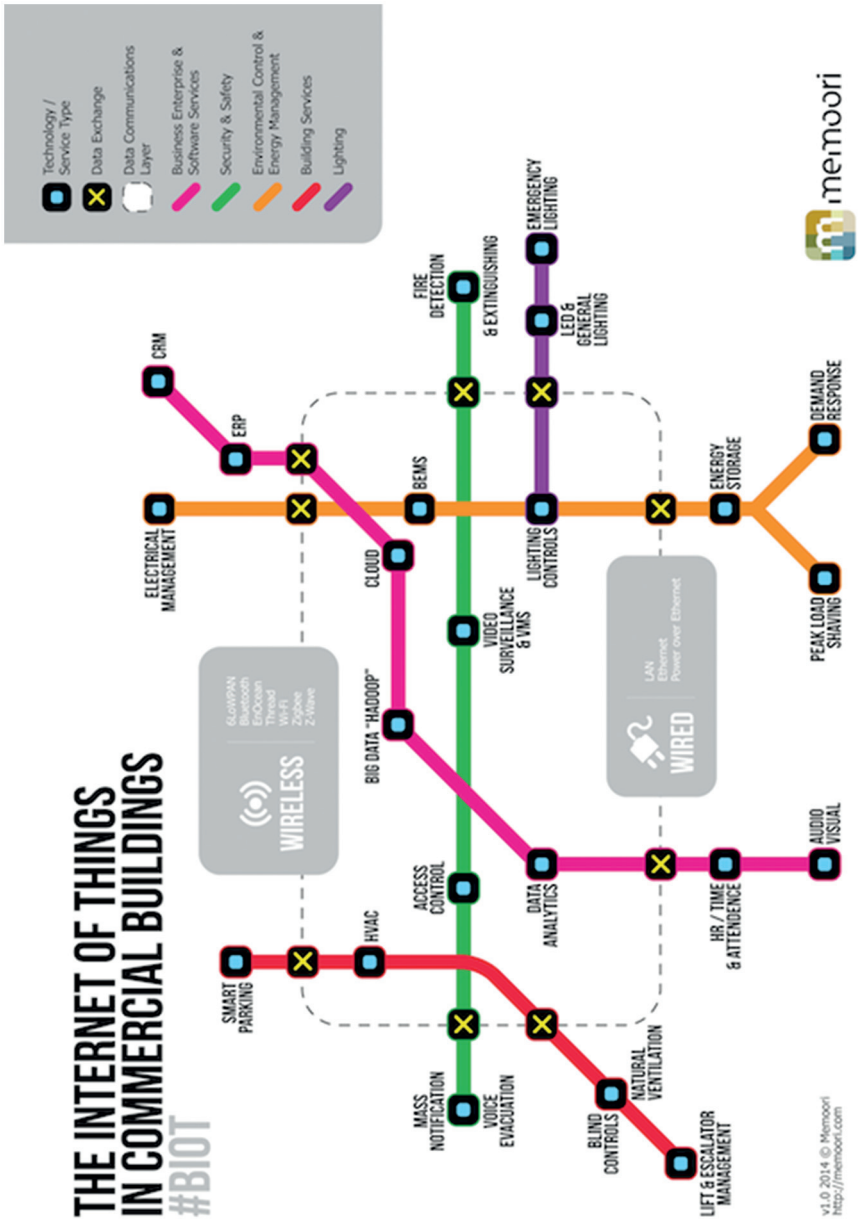

Figure 3.20 IoT in commercial buildings [33].

- The networking and related services segment of the market will show a steady growth of 22.6% CAGR rising from $9.53Bn in 2014 to $32.43Bn in 2020 which represents 37% of overall revenues by 2020. Similar to the market for connectivity hardware, effective network deployment to keep up with the rising bandwidth demands of the IoT in Buildings will be crucial to the effective delivery of services and the management of data flows.

The concept of "Internet of Building" that integrates the information from multiple intelligent building management systems and optimise the behaviour of individual buildings as part of a larger information system. These systems are used by facilities managers in buildings to manage energy use and energy procurement and to maintain buildings. It is based on the infrastructure of the existing Intranets and the Internet, and therefore utilises the same standards as other IT devices. Reductions in the cost and increased reliability of IoT applications using wireless technologies for monitoring and control are transforming building automation, by making the maintenance of energy efficient healthy productive workspaces in buildings increasingly cost effective [50].

IoT technologies and applications used across the buildings and architecture sector need to be integrated with applications in other sectors. The value in "Internet of Buildings" is as much in the edge devices and the data collected, exchanged and processed. Collecting, exchanging and processing data from building services and equipment provides a granular view of how each building is performing, allowing the development of building systems that collect, store and analyse data at the edge and in the cloud, providing better operational efficiency and integration with IoT platforms and applications across various sectors. These efforts will cover the following domains of research.

- IoT architecture and IoT platforms to address smart buildings and architecture monitoring and control strategies and integrate monitors/controls from edge sensors/actuators devices to the data exchange and processing.
- Communication technologies and infrastructures required for IoT buildings applications and their integration with applications and IoT platforms across various consumer and industrial sectors.
- Hardware/software, machine learning and analytics approaches supporting real-time interoperable distributed decision support monitoring and control in heterogeneous environments.
- New developments in the smart buildings addressing business models, applications, IoT technology, interoperability at various levels and frameworks, regulation and law, etc.

3.3.5 Smart Energy

Future energy supply will be largely based on various renewable resources and this source of energy will influence the energy consumption behaviour, demanding an intelligent and flexible electrical grid which is able to react to power fluctuations by controlling electrical energy sources (generation, storage) and sinks (load, storage) and by suitable reconfiguration. The functions are based on networked intelligent devices (appliances, micro-generation equipment, infrastructure, consumer products) and grid infrastructure elements, largely based on IoT concepts.

The energy grid development requires a number of features as listed below in order to implement the vison of the smart grid concept.

- It will integrate traditional and emerging power sources and make the delivery of energy cleaner, safer, and more economical.
- Operators will have the transparency and visibility to monitor and analyse the flow of energy, and two-way communication with consumers' smart meters to analyse consumption patterns.
- Intelligent devices that collect and analyse massive volumes of data will enable operators to plan for contingencies for variable resources.
- Smart IoT devices will manage the distribution of energy based on real-time data and situational awareness, as opposed to historical data patterns.
- Predictive maintenance capabilities will alert operators when a component needs attention or repair, reducing the need for ongoing inspections.
- Adaptive analytics will enable systems to automatically balance energy loads to reduce stress and prevent overheating.

The high number of distributed small and medium sized energy sources and power plants can be combined virtually ad hoc to virtual power plants. Using this concept, areas of the grid can be isolated from the central grid and supplied from within by internal energy sources such as photovoltaics on the roofs, block heat and power plants or energy storages of a residential area.

IoT is expected to facilitate the deployment of new smart energy apps within energy stakeholders ICT (generation and retail companies, Grid and market operators, new load aggregators) bringing new options for real-time control strategies across energy asset portfolios for faster reactions to power fluctuations. These new technologies should combine both centralised and decentralised approaches integrating all energy generation (generation, storage) and load (demand responsive loads in residential, buildings and industries as well as storage and electrical vehicles) through interconnected real-time energy markets. IoT should also improve the management of asset

Figure 3.21 Smart grid concept [49, 79].

performance through more accurate estimations of asset health conditions and deployment of fact based preventive maintenance.

These new smart energy apps will largely be based on the networking of IoT intelligent devices embedded within Distributed Energy Resources (DER) spread across the energy system such as consumer appliances, heating and air conditioning, lighting, distributed generation and associated inverters, grid edge and feeder automation, storage and EV charging infrastructures. While energy systems have historically been controlled through single central dispatch strategies with limited information on grid edge and consumers behaviours, energy systems are now characterized by rapidly growing portfolios of DER structured through several layers of control hierarchies interconnecting the main grid down to microgrids within industries and communities, nanogrids at building level and picogrids at residential scale.

Moreover as most of DER have diffused within end-user premises, new transactive control approaches are required to facilitate their coordination at various scales of the Grid system through real-time pricing strategies. Furthermore aggregators and energy supply companies have started to develop new flexibility offers to facilitate DER coordination virtually through ad hoc virtual power plants raising new connectivity, security and data ownership challenges.

Meanwhile climate change has also recently exposed grids to new extreme weather conditions requiring reconsidering Grid physical and ICT

architectures to allow self-healing during significant disasters while taking advantage of distributed generation and storage to island critical grid areas (hospital, large public campus) and maintain safe city areas during emergency weather conditions.

Integration of cyber-physical systems engineering and technology to the existing electric grid and other utility systems is a challenge. The increased system complexity poses technical challenges that must be considered as the system is operated in ways that were not intended when the infrastructure was originally built. As technologies and systems are incorporated, security remains a paramount concern to lower system vulnerability and protect stakeholder data [71]. These challenges will need to be address as well by the IoT applications that integrate heterogeneous cyber-physical systems.

A new report by Mercom Capital Group indicates that smart grid, battery and storage, as well as energy efficiency companies raised up to US$1.7bn in VC funding in 2015. The report which examines mergers and acquisition activity in the smart grid, battery/storage, and energy efficiency sectors, revealed that the smart grid sector raised US$425 million across 57 deals in 2015, in comparison to US$384 million over 74 deals in the previous year (2014) [79].

The energy grid is expected to be the implementation of a kind of "Internet" in which the energy packet is managed similarly to the data packet – across routers and gateways, which autonomously can decide the best pathway for the packet to reach its destination with the best integrity levels. In this respect, the "Internet of Energy" concept is defined as a network infrastructure based on standard and interoperable communication transceivers, gateways and protocols that will allow a real time balance between the local and the global generation and storage capability with the energy demand.

The Internet of Energy (IoE) concept is defined as a network infrastructure based on standard and interoperable communication nodes that will allow the end-to-end real time balance between the local and the central generation, responsive demand and storage. It will allow units of energy to be transferred when and where it is needed. Power consumption monitoring will be performed on all levels, from local individual devices up to national and international level [78].

Considering the fast diffusion of energy resources on end user premises – becoming prosumers-, the new IoT platform considered will also allow a high level of consumer awareness and involvement through community benchmarking.

Electro mobility requiring the rapid deployment of charging infrastructures adding significant constraints to power grids; EVs will be considered as integral element of future smart energy systems acting as a power load as well as moveable energy storage linked through IoT technologies. EVs will require to transact with the Energy system according to their charge status, usage schedule and energy price which itself will depend on abundance of renewable energy available at a certain time in the energy system. This should ultimately allow monitoring the carbon footprint of all mobility services from wells to wheels.

Latencies are critical when talking about electrical control loops. Even though not being a critical feature, low energy dissipation should be mandatory. In order to facilitate interaction between different vendors' products the technology should be based on a standardized communication protocol stack.

When dealing with a critical part of the public infrastructure, data security is of the highest importance. In order to satisfy the extremely high requirements on reliability of energy grids, the components as well as their interaction must feature the highest reliability performance.

IoT applications in the energy sector go beyond one industrial sector. Energy, mobility and home/buildings sectors will have to share data through energy gateways that will control the transfer of energy and information.

Flexible data filtering, data mining and machine learning procedures as well as new generation IoT platforms are necessary to handle the high amount of raw data provided by billions of data sources while guaranteeing resiliency, security as well as end user data protection. System and data models need to support the design of real-time decision support systems, which guarantee a reliable and secure operation of vital energy infrastructures.

The future research challenges will cover the following areas:

- ICT/IoT architectures and IoT platforms to revisit grid control strategies and integrate hierarchical controls from energy nodes with sensors through ranges of aggregation structures (pico, nano and micro energy systems).
- Novel communication infrastructures required at each level of these grid nodes to meet necessary Service level agreements for each of the energy service considered (energy efficiency, grid ancillary services, grid resiliency, etc. . .).
- New software/smart data and machine learning approaches supporting real-time distributed decision support/transactive controls in highly volatile environments.

- New apps for energy prosumer feedback facilitating smooth real-time energy transactive controls in daily lives leveraging consumer ICT (mobile, TVs, vehicle, IoT, etc. . .).
- IoT end-to-end security framework approach and privacy, trust and safety in order to secure the grid from hackers and acts of cyber-sabotage. Security needs to be built into every device starting at the base of the software stack.
- Providing intelligent solution for connecting and protecting legacy systems (the older, aging parts of the existing energy infrastructure) by building secure Internet gateways that enable cloud-based central control systems to collect local intelligence data from the systems while blocking attacks.
- Embedding intelligence into the energy systems with smart energy devices that deliver manageability, security, and connectivity, while driving down the cost of development and deployment.
- Privacy by design of the energy systems that will assure that the data generated by using the monitoring systems will not expose sensitive customer information. This requires that the same security principals that apply to the energy enterprise will also be applied at the consumer level.

3.3.6 Smart Mobility and Transport

The connection of vehicles to the Internet gives rise to a wealth of new possibilities and applications which bring new functionalities to the individuals and/or the making of transport easier and safer. In this context the concept of Internet of Vehicles (IoV) [78] connected with the concept of Internet of Energy (IoE) represent future trends for smart transportation and mobility applications.

At the same time creating new mobile ecosystems based on trust, security and convenience to mobile/contactless services and transportation applications will ensure security, mobility and convenience to consumer-centric transactions and services.

Representing human behaviour in the design, development, and operation of cyber-physical systems in autonomous vehicles is a challenge. Incorporating human-in-the-loop considerations is critical to safety, dependability, and predictability. There is currently limited understanding of how driver behaviour will be affected by adaptive traffic control cyber-physical systems. In addition, it is difficult to account for the stochastic effects of the human driver in a mixed traffic environment (i.e., human and autonomous vehicle

drivers) such as that found in traffic control cyber-physical systems. Increasing integration calls for security measures that are not physical, but more logical while still ensuring there will be no security compromise. As cyber-physical systems become more complex and interactions between components increases, safety and security will continue to be of paramount importance [71]. All these elements are of the paramount importance for the IoT ecosystems developed based on these enabling technologies.

Self-driving vehicles today are in the prototype phase and the idea is becoming just another technology on the computing industry's parts list. By using automotive vision chips that can be used to help vehicles understand the environment around them by detecting pedestrians, traffic lights, collisions, drowsy drivers, and road lane markings. Those tasks initially are more the sort of thing that would help a driver in unusual circumstances rather than take over full time. But they're a significant step in the gradual shift toward the computer-controlled vehicles that Google, Volvo, and other companies are working on [56].

These scenarios are, not independent from each other and show their full potential when combined and used for different applications.

Technical elements of such systems are smart phones and smart vehicle on-board units, which acquire information from the user (e.g. position, destination and schedule) and from on-board systems (e.g. vehicle status, position, energy usage profile, driving profile). They interact with external systems (e.g. traffic control systems, parking management, vehicle sharing managements, electric vehicle charging infrastructure).

The concept of Internet of Vehicles (IoV) is the next step for future smart transportation and mobility applications and requires creating new mobile ecosystems based on trust, security and convenience to mobile/contactless services and transportation applications in order to ensure security, mobility and convenience to consumer-centric transactions and services.

Smart sensors in the road and traffic control infrastructures need to collect information about road and traffic status, weather conditions, etc. This requires robust sensors (and actuators) which are able to reliably deliver information to the systems mentioned above. Such reliable communication needs to be based on IoT communication, which consider the timing, safety, and security constraints. The integration of the communication gateway into vehicles is presented in Figure 3.23. The expected high amount of data will require sophisticated data mining strategies. Overall optimisation of traffic flow and energy usage may be achieved by collective organisation among the individual vehicles.

Figure 3.22 Home and vehicle IoT solutions [55].

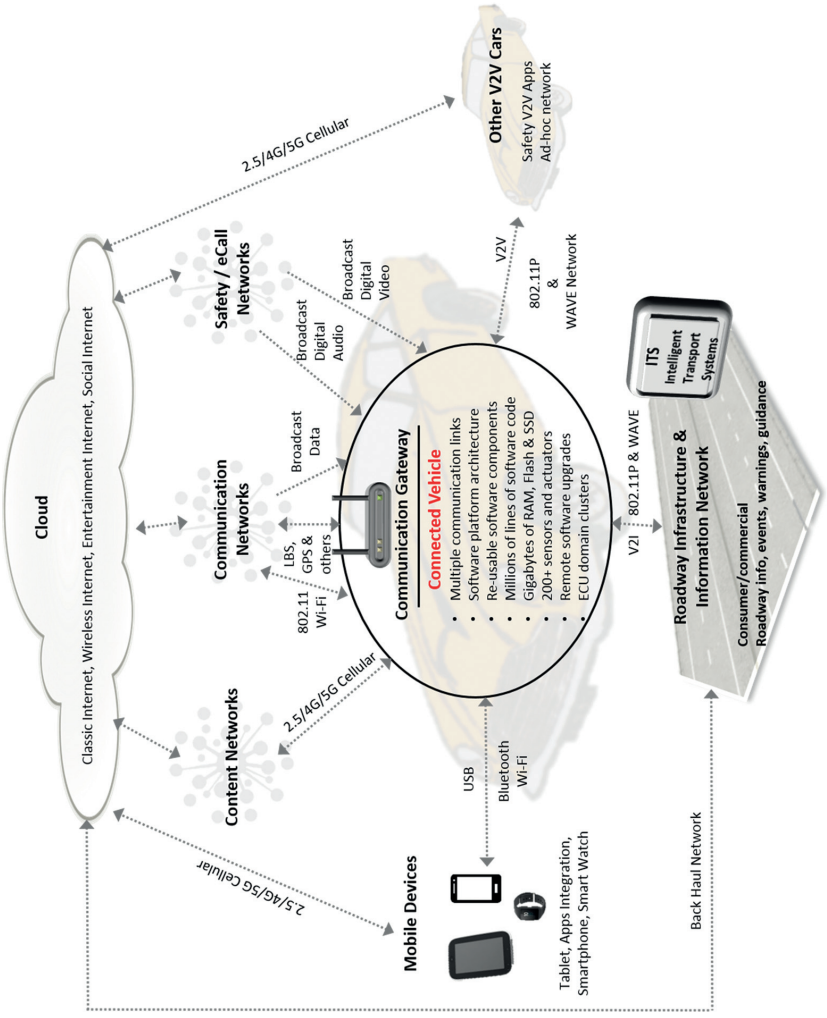

Figure 3.23 Vehicle integrated IoT communication platform.

When dealing with information related to individuals' positions, destinations, schedules, and user habits, privacy concerns gain highest priority. They even might become road blockers for such technologies. Consequently, not only secure communication paths but also procedures which guarantee anonymity and de-personalization of sensible data are of interest.

Connectivity will revolutionize the environment and economics of vehicles in the future: first through connection among vehicles and intelligent infrastructures, second through the emergence of an ecosystem of services around smarter and more autonomous vehicles.

In this context the successful deployment of safe and autonomous vehicles (SAE[1] international level 5, full automation) in different use case scenarios, using local and distributed information and intelligence is an important achievement. This is based on real-time reliable platforms managing mixed mission and safety critical vehicle services, advanced sensors/actuators, navigation and cognitive decision-making technology, interconnectivity between vehicles (V2V) and vehicle to infrastructure (V2I) communication. There is a need to demonstrate in real life environments (i.e. highways, congested urban environment, and/or dedicated lanes), mixing autonomous connected vehicles and legacy vehicles the functionalities in order to evaluate and demonstrate dependability, robustness and resilience of the technology over longer period of time and under a large variety of conditions.

The introduction of the autonomous vehicles enables the development of service ecosystems around vehicles and multi-modal mobility, considering that the vehicle includes multiple embedded information sources around which information services may be constructed. The information may be used for other services (i.e. maintenance, personalised insurance, vehicle behaviour monitoring and diagnostic, security and autonomous cruise, etc.).

The emergence of these services will be supported by open service platforms that communicate and exchange information with the vehicle embedded information sources and to vehicle surrounding information, with the goal of providing personalised services to drivers. Possible barriers to the deployment of autonomous vehicles and ecosystems are the robustness sensing/actuating the environment, overall user acceptance, the economic, ethical, legal and regulatory issues.

The integration of the interconnected and intelligent intra vehicle communication systems and the vehicle to infrastructure into the overall IoT service platforms will offer the possibility to develop new applications and

[1]Society of Automotive Engineers, J3016 standard.

services it is expected that 80% of vehicles in Europe will be two-way connected by 2018. This offer the possibility to combine the vehicle to infrastructure communication and integration with service providers with intermodal vehicle navigation applications and navigation routes based on real-time information. IoT applications for vehicle sharing and the use of transport city fleets (EVs for transport of goods and persons) are part of the deployment of new IoT technologies and related IoT ecosystems. These will open the stepwise rollout of autonomous driving technologies and the linkages of these technologies with shared-use business models and issues relating to the regulatory framework and consumer trust.

For autonomous vehicle applications, computing at the edge of the mobile network will be used for processing the data locally and provide services in real time.

Data transmission costs and the latency limitations of mobile connectivity pose challenges to autonomous vehicle IoT applications that cannot rely only on cloud computing.

Mobile edge computing enables IoT applications to deliver real-time and context-based mobile moments to users of IoT solutions.

In IoT applications involving autonomous vehicles a combination of cloud and mobile edge computing technologies have to be consider by analysing the following:

- Cloud, mobile edge and IoT are increasingly intertwined and used together to improve IoT application experiences. IoT solutions gain functionality through cloud services, which in turn open access to third-party companies and up-to-date information.
- Mobile connectivity for real time autonomous systems create challenges for cloud-enabled IoT solutions since latency limitations affects user experiences in the IoT real time applications context.
- Mobile edge computing assure the real time network connectivity, location and context information. The technology gives access to "near edge" computing capabilities and a cloud like service environment close to the users and edge devices.
- Mobile edge computing is a component of the network infrastructure for blockchain, since the replication of "blocks" via devices can be implemented at the edge.

3.3.7 Industrial IoT and Smart Manufacturing

The role of the IoT is becoming more prominent in enabling access to devices and machines, which in manufacturing systems, were hidden in well-designed

silos. This evolution will allow the IT to penetrate further the digitized manufacturing systems. The IoT will connect the factory to a completely new range of applications, which run around the production. This could range from connecting the factory to the smart grid, sharing the production facility as a service or allowing more agility and flexibility within the production systems themselves. In this sense, the production system could be considered one of the many Internets of Things (IoT), where a new ecosystem for smarter and more efficient production could be defined.

The evolutionary steps towards smart factory require enabling access to external stakeholders in order to interact with an IoT-enabled manufacturing system that is formed of connected industrial systems that communicate and coordinate their data analytics and actions to improve performance and efficiency and reduce or eliminate downtime. These stakeholders could include the suppliers of the productions tools (e.g. machines, robots), as well as the production logistics (e.g. material flow, supply chain management), and maintenance and re-tooling actors. The manufacturing services and applications do not need to be defined in an intertwined and strictly linked manner to the physical system, but rather run as services in a shared physical world. Adopting the industrial IoT requires a change in the way stakeholders design and augment their industrial systems in order that the IoT industrial systems are adaptive and scalable through software or added functionality that integrates with the overall solution.

Industrial IoT applications are using of the data available, business analytics, cloud services, enterprise mobility and many others to improve the industrial processes. These technologies include big data and business analytics software, cloud services, embedded technology, sensor networks/sensing technology, wireless communication, mobility, security and ID recognition technology, wireless network and standardisation. Security is very important in industrial IoT applications that are processing the information from tens of thousands of edge devices nodes. Faulty data injected into the system has the potential to be as damaging as data extracted from the systems via data breach.

The convergence of microelectronics and micromechanical parts within a sensing device, the ubiquity of communications, the rise of micro-robotics, the customization made possible by software will significantly change the world of manufacturing. In addition, broader pervasiveness of telecommunications in many environments is one of the reasons why these environments take the shape of ecosystems.

The future IoT developments integrated into the digital economy will address highly distributed IoT applications involving a high degree of

distribution, and processing at the edge of the network by using platforms that that provide compute, storage, and networking services between edge devices and computing data centres.

IoT applications integrate sensors/actuators and cyber-physical systems offering new opportunities for new combinations of virtual, digital, physical and mechanical work. The IoT and Industrial IoT are currently underlying the far-reaching integration of Information Technology (IT: conventional computers, operating systems, networking components and software platforms.) and Operational Technology (OT: industrial control system and networks, hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise) [12, 13].

Some of the main challenges associated with the implementation of cyber-physical systems in include affordability, network integration, and the interoperability of engineering systems.

Most companies have a difficult time justifying risky, expensive, and uncertain investments for smart manufacturing across the company and factory level. Changes to the structure, organization, and culture of manufacturing occur slowly, which hinders technology integration. Pre-digital age control systems are infrequently replaced because they are still serviceable. Retrofitting these existing plants with cyber-physical systems is difficult

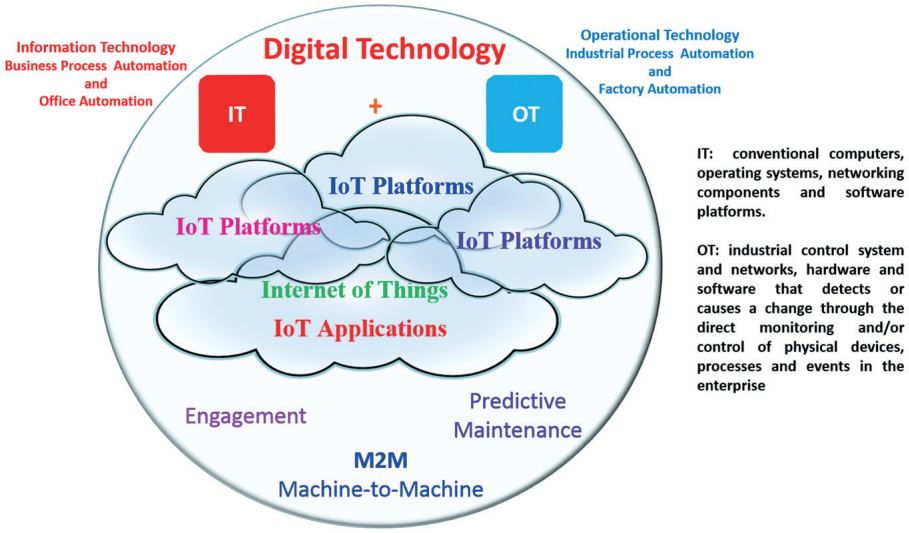

Figure 3.24 IoT providing the core structure for integration of IT and OT.

and expensive. The lack of a standard industry approach to production management results in customized software or use of a manual approach. There is also a need for a unifying theory of non-homogeneous control and communication systems [71].

The industrial IoT is implemented in various forms, one is called Internet of Things, Services and People (IoTSP) [27] were the focus is to develop and enhance process control systems, communications solutions, sensors and software for the IoTSP. These technologies enable the customers in industries, utilities and infrastructure to analyse their data more intelligently, optimize their operations, boost their productivity, and their flexibility. IoTSP is advancing by helping the IoT stakeholders and customers to develop their existing technologies, while keeping sight of our enduring commitment to safety, reliability, cyber security and data privacy. Developing and improving process control system, communication solutions, sensors and software used in IoTSP provide new value for the customers. With these technologies, the customers in industry, utility, transportation and infrastructure can benefit from smart data analysis, optimized operation, and higher productivity and flexibility.

3.3.8 Smart Cities

Cities all over the world, from small regional communities to global mega hubs and from cities with an ancient core to brand new developments, are currently working on 'Smart City' initiatives to make them more efficient, sustainable, and more attractive to citizens and businesses and to encourage economic growth. There are many obstacles to successful implementation of these plans, and translating solutions from one place to another is difficult. While every city on earth is unique and has its own characteristics that will impact why, how and which Smart City solutions may emerge, there are enough similarities for it to be worth investigating how best practices for financing, design, implementation and operation can be shared and how industry can re-use experience gained from earlier projects, for example. Key elements include interoperability of data between devices and subsystems, information flows between project partners, financing, risk management, etc. [57].

A Smart City is defined as a city that monitors and integrates conditions of all of its critical infrastructures, including roads, bridges, tunnels, rail/subways, airports, seaports, communications, water, power, even major buildings, can better optimize its resources, plan its preventive maintenance activities, and monitor security aspects while maximizing services to its

citizens. Emergency response management to both natural as well as man-made challenges to the system can be focused and rapid. With advanced monitoring systems and built-in smart sensors, data can be collected and evaluated in real time, enhancing city management's decision-making [69].

There are a number of key elements needed to form a Smart City, and some of these are smart society, smart buildings, smart energy, smart lighting, smart mobility, smart water management etc. ICT forms the basic infrastructure; varying from sensors, actuators and electronic systems to software, Data, Internet and Cloud, Edge/fog and Mobile Edge computing. ICT is applied to improve these systems of systems building up a Smart City, making them autonomous and interoperable, secure and trusted. The interaction of the systems and the connectivity strongly depend on the communication gateway connecting the edge element data from sensors, actuators, and electronic systems to the Internet, managing- and control systems and decision programs.

An illustrative example of a Smart City model is presented in Figure 3.25 [57]. This model has a mostly technical view, concentrating on how (sub) systems interact with each other supported by telecommunications and information technology. The city is divided into the built environment (including homes, offices and shops and the devices within them), infrastructure-based sectors (e.g. energy and waste) and service-based sectors (e.g. healthcare and education). There is possible interaction between elements within any of these subsystems as well as between subsystems. Smart city infrastructure sectors, such as telecommunications, information technology and electronics, enable and support this interaction. A common theme in the example Smart City models is the use of sensors to collect data from the city, which, through platforms, can be combined, stored, analysed and displayed. This provides decision support for actors in the city who can then act and make changes, the effect of which can in turn be measured [57]. The Smart City is not only the integration and interconnection of intelligent applications, but also a people-centric and sustainable innovation model that is using communication and information technology and takes advantage of the open innovation ecology of the city and the new technologies such as IoT, cloud computing, data analytics, human-human, human-machine, machine-infrastructure, machine-environment interaction.

A Smart City is a developed urban area that creates sustainable economic development and high quality of life by excelling in multiple key areas: economy, mobility, environment, people, living, and government [77].

Identifying or developing sets of Key Performance (KPI) and other indicators to gauge the success of Smart City ICT deployments. KPIs are required

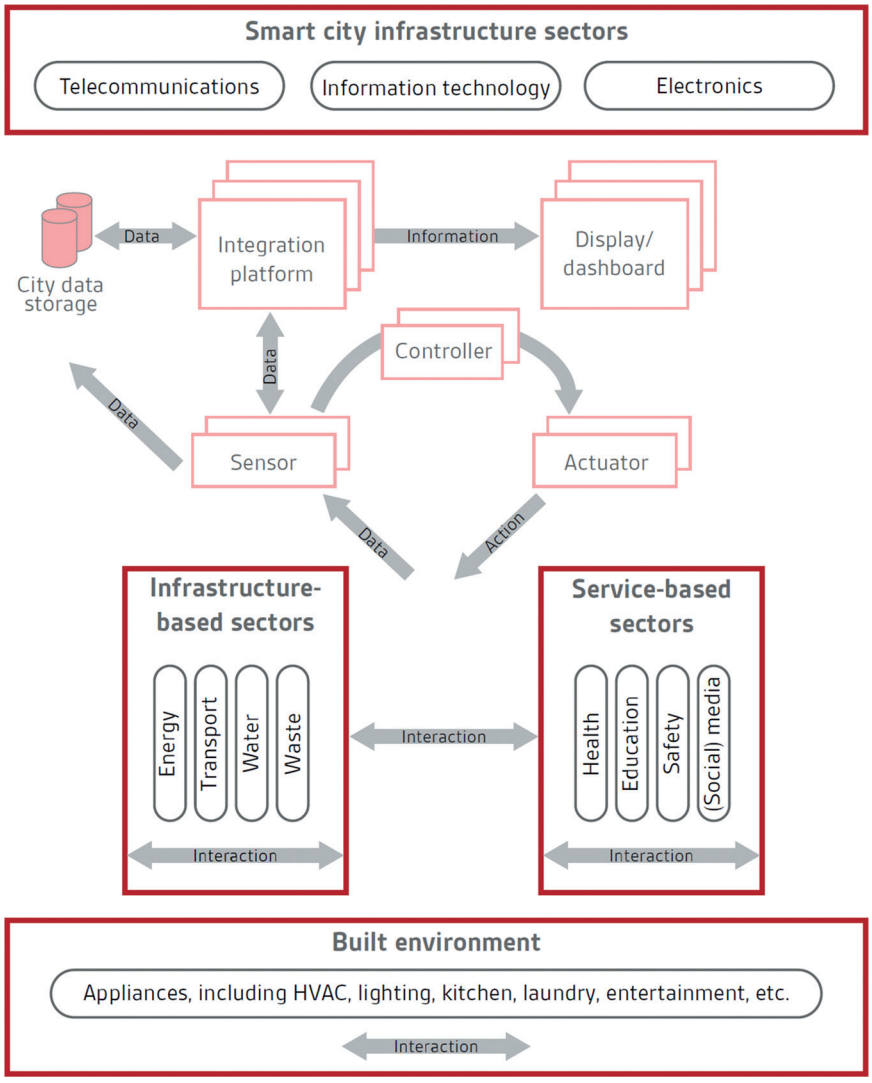

Figure 3.25 Smart City model – technical view [57].

to provide performance as seen from different viewpoints, such as those: of residents/citizens (reliability, availability, quality and safety of services, etc.); of community and city managers (operational efficiency, resilience, scalability, security, etc.); and of the environment (climate change, biodiversity, resource efficiency, pollution, recycling rates/returns). The indicators appropriate for

one city or context may not be the same for others. As such, there should also be standardized guidance for city managers on selecting and using KPIs appropriate to their particular situation. Requirements for standardized risk assessment methodologies for critical infrastructure dependencies across organisations and sectors [58].

3.3.8.1 Open Data and Ecosystem for Smart Cities

As main areas of application, smarter cities plays a relevant role, not only because the impact in re-using and re-purposing technology that is necessary (the number of deployed sensors) but also the increasing demand of new services (by citizens). IoT applications are currently based on multiple architectures, technology standards and seamless software platforms, which have led to a highly fragmented IoT landscape. This fragmentation impacts directly the area of smart cities, which typically comprise several technological silos (i.e. IoT systems that have been developed and deployed independently for smart homes, smart industrial automation, smart transport, and smart buildings etc.).

The operation of IoT applications for Smart Cities will be supported by the introduction of an abstract virtualized digital layer that operate across multiple IoT architectures, platforms (e.g. FI-WARE) and business contexts is required. Smart cities soon will face up the need for an integrated solution(s) (SmartCity-OS) that globally can monitor, visualise and control the uncountable integrated number of operations executed by diverse (and every day increasing) services platforms using the sensor technology deployed in the cities.

The term "Open Data" in the context of Smart Cities generally refers to a public policy that requires public sector agencies and their contractors to release key sets of government data (relating to many public activities of the agency) to the public for any use, or re-use, in an easily accessible manner. In many cases, this policy encourages this data to be freely available and distributable. The value of releasing such data is presumed to lie in the combination of this and other data from various sources. This value can be dramatically increased when the data is discoverable, actionable and available in standard formats for machine readability. The data is then usable by other public agencies, third parties and the general public for new services, and for ever richer insight into the performance of key areas like transport, energy, health and environment. In this context there is a need to ensure that any standards or guidance in this area should not be prescriptive about particular models, but encourage innovation in data re-use [58].

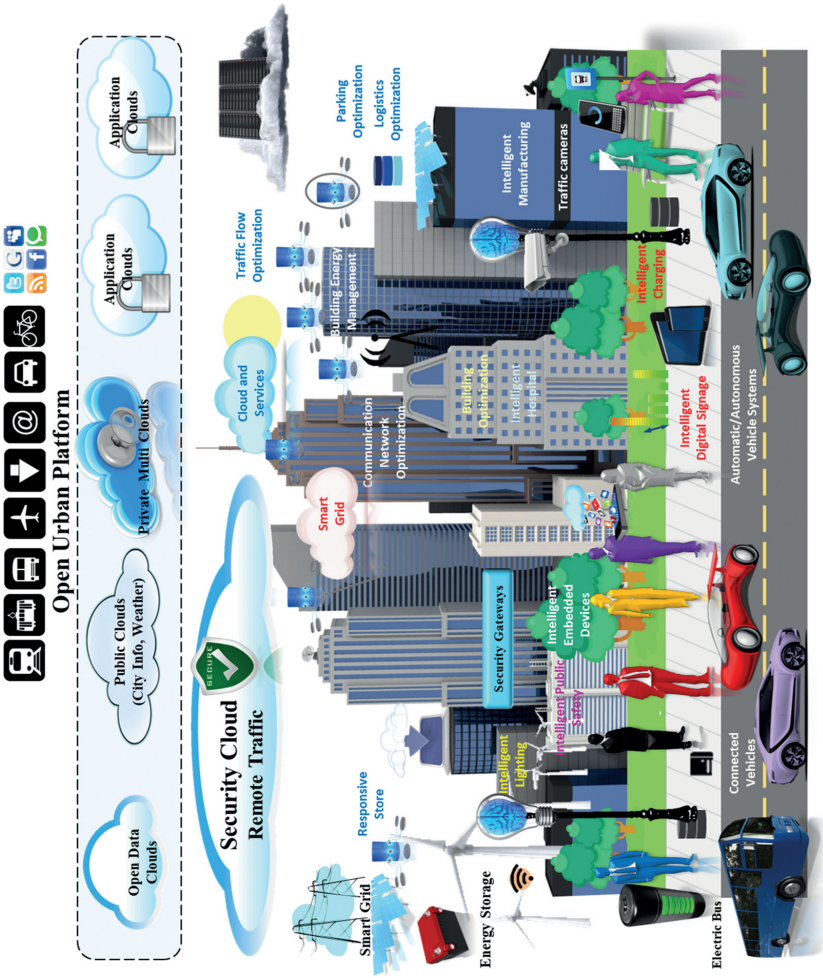

Figure 3.26 Smart City – integration of heterogeneous systems and open data.

The quality of IoT Data and the numerous IoT Data source provisioning are important issues as there is an inherent need to generate semantic-driven business platforms, o address the enabling business-driven IoT ecosystems. These systems have to address functionalities for operating across multiple IoT architectures, platforms and business contexts, to enable a more connected/integrated approach to Smart City applications development.

Smart Cities are becoming one of the biggest fields of application for IoT technologies. Cities are more and more full of devices equipped with sensors, actuators and other appliances providing information that in the past was either impossible or relatively difficult to gather. Their main purpose, among other functionalities, is to gather information about various parameters of importance for management of day-to-day activities in the city as well as for longer term development planning. Examples of such parameters are information about public transport (real-time location, utilization), traffic intensity, environmental data (air quality), occupancy of parking spaces, noise, monitoring of waste bins, energy consumption in public buildings, etc. [66].

Integrated IoT solutions deployed in the cities require addressing interoperability, security, privacy, and trust for all of the suppliers in the

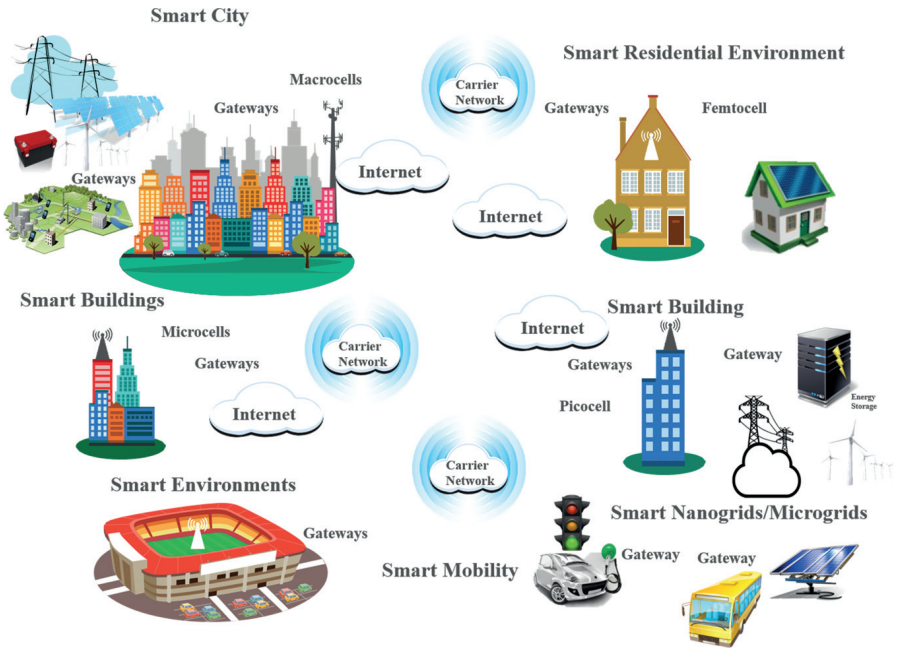

Figure 3.27 Smart City communication technologies landscape.

ecosystem also have policies and safeguards that align to those of the citizens.

The research priorities need to focus on common IoT architecture approaches, IoT data modelling and schema representations, intra-domain and CPS extensions that allows more robustness and extensible IoT platforms with embedded software and applications enabling heterogeneous systems to interact (systems of systems integration) across various verticals in the city.

3.3.8.2 Citizen Centric Smart Cities IoT Applications and Deployments

Public city environments are complex and large. The only possibility to address these largescale, multi-subsystem projects is in a collaborative, open-innovation context, where effort is required to align interests, shape opinions, develop business models and provide a common, interoperable IoT technology ecosystem. Cities are "used" by people, which play different roles on the city (resident citizens, visitors and tourists, businesses, municipal services employees, etc.). The focus on users and citizens can be orchestrated in various dimensions: problems, awareness, participation, culture and digital transformation [66].

In this context, there are numerous important research challenges for smarty city IoT applications:

- Design and implementation of modular architectures enabling easy ways to interface with already existing infrastructures by using standards, protocol wrappers or other innovative means.
- Overcoming traditional silo based organization of the cities, with each utility responsible for their own closed world. Although not technological, this is one of the main barriers.
- Creating algorithms and schemes to describe information created by sensors in different applications to enable useful exchange of information between different city services.
- Mechanisms for cost efficient deployment and even more important maintenance of such installations, including energy scavenging.
- Ensuring reliable readings from a plethora of sensors and efficient calibration of a large number of sensors deployed everywhere from lampposts to waste bins.
- Increasing the intelligence and flexibility on end devices to support them to take autonomous decisions, decreasing resource overloads such as bandwidth and improving their management.

- Provide interoperability solutions that allows that interoperability can be achieved at different levels with the goal of reaching fully interoperability at data level for IoT platforms that operate inside the city and allows the replicability of solutions among cities.
- Design and development of unified APIs for accessing data independently of the protocols, APIs and models supported in the underlying IoT platform in a machine readable way.
- Algorithms for analysis and processing of data acquired in the city and making "sense" out of it.
- IoT large-scale deployment and integration.

3.3.9 Smart Farming and Food Security

Food and fresh water are the most important natural resources in the world. Farming is a major economic activity in Europe [70], with about 12 million farms in the EU-28 in 2010, 40% of the land area and 25 million people dedicated to farming activities. In a European context with its population increasing, achieving higher efficiency in food production is a top priority.

Sustainable farming, producing more with less and with a smaller environmental footprint, is an unstoppable trend that demands new technologies. ICT technologies, and IoT in particular, will be crucial elements for meeting the challenges of tomorrow's sustainable farming, supporting the implementation of smart/precision farming techniques aimed at improving the processes of food production. Indeed, a lot of ICT research and innovation in farming is happening nowadays around precision farming, although the benefits of the application of ICT technologies encompass the whole agri-food value chain as presented in Figure 3.28: food processing, food logistics, wholesale/retail, and finally the consumers.

One crucial aspect that cannot be overlooked, and which is transversal to the whole agri-food value chain, is food safety and traceability: the mechanisms to ensure and monitor those food products are healthy and safe, at their highest possible quality specifications, throughout their whole lifecycle, from farm to fork. Again, food safety can greatly benefit from the application of IoT technologies.

Farming 4.0, or IoT-based innovations applied to farming, has the potential to boost rural areas and EU economy. The AIOTI WG06 Recommendations Report [64], recently published, highlights the benefits that the application of IoT technologies can bring into the agri-food sector, along with the numerous

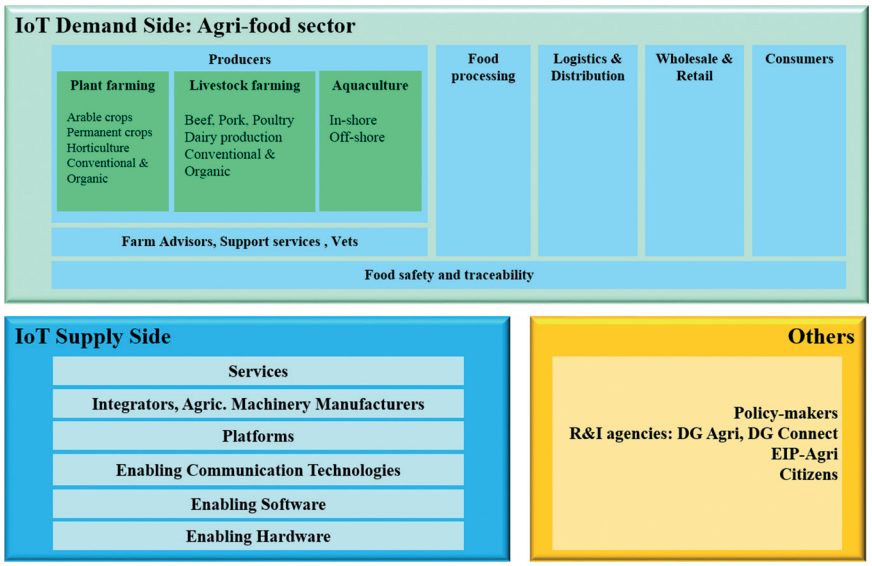

Figure 3.28 Smart farming and food security stakeholders + agri-food value chain.

challenges that must be overcome to unleash their full potential in large scale implementations.

Final IoT-based applications or solutions are enabled by the combination of a number of technology building blocks or layers. Each of those layers faces particular R&I challenges.

IoT applications in the farming sector are dependent on a number of enabling technologies covering hardware (i.e. smart devices that may embed sensors, actuators, communication gateways and other appliances), software (which, embedded in the device, provides it with intelligence, autonomous decision-making, etc.), network/cloud/communication technologies (including the need of reliable, possibly broadband, data coverage in rural or remote areas, and the growing trend of softwarisation/de-hardwarisation and localisation of networks), and services for providing the functionalities needed by the sector. In addition interoperability, standardisation and data management (considering the value and the sensitivity of data generated at farms and other parts of the food chain, but also the added value that comes from data aggregation) are key R&I drivers that are applicable to all technology layers.

A report on smart farming [53] defines seven applications:

- Fleet management – tracking of farm vehicles
- Arable farming, large and small field farming

- Livestock monitoring
- Indoor farming – greenhouses and stables
- Fish farming
- Forestry
- Storage monitoring – water tanks, fuel tanks

Smart farming will allow farmers and growers to improve productivity and reduce waste, ranging from the quantity of fertiliser used to the number of journeys made by farm vehicles. The complexity of smart farming is also reflected into the ecosystem of players. They can be classified in the following way:

- Technology providers – these include providers of wireless connectivity, sensors, M2M solutions, decision support systems at the back office, big data analytical systems, geo-mapping applications, smartphone apps
- Providers of agricultural equipment and machinery (combines, tractors, robots), farm buildings, as well as providers of specialist products (e.g. seeds, feeds) and expertise in crop management and animal husbandry
- Customers: farmers, farming associations and cooperatives
- Influencers – those that set prices, influence the market into which farmers and growers sell their products.

The range of stakeholders in agriculture is broad, ranging from big business, finance, engineering, chemical companies, food retailers to industry associations and groupings through small suppliers of expertise in all the specialist areas of farming.

The end users of precision farming solutions include not only the growers but also farm managers, users of back office IT systems. Not to be forgotten is the role of the veterinary in understanding animal health. Also to be considered are farmers co-operatives, which can help smaller farmers with advice and funding.

The following table provides an overview of the most relevant challenges across the technology layers.

Table 3.1 Technological challenges for IoT applications in the farming sector

Development	2016–2020	Beyond 2020
Enabling hardware	• Improve the ratio computational power-to-energy consumption of devices, possibly combined with energy harvesting or local renewable generation.	• Implementation of more efficient hardware cryptographic primitives embedded in hardware devices

(*Continued*)

Table 3.1 Continued

Development	2016–2020	Beyond 2020
	• Increase hardware robustness: longer lifetime and calibration cycles • Development of cost-effective near-field communication technologies suitable for massive use in food products	
Enabling software	• Development of flexible real-time and embedded micro operating systems • Self-configurable, remotely attestable devices • Large-scale device management and orchestration software and middleware, including SW	• Self-configurable, remotely attestable devices
Enabling network, cloud, communication technologies	• SDN/NFV for telcos targeted to smart agriculture applications • Edge analytics to promote local data circulation • Definition and application of protocols with bounded message delivery times (for real-time applications) • Federated/orchestrated hybrid clouds and transition to communal equipment/infrastructure • Level playing field facilitating competition among service providers • Increase the range of communication and reliability of deployed devices • Adapt communications architecture for supporting low individual device throughput and high aggregated network throughput (i.e. few short messages from each device, but a high amount of individual data sources) • Automatic deployment (no need for configuration of the communications)	• SDN/NFV for telcos targeted to smart agriculture applications • Distributed communication architectures (e.g. Edge Computing) to treat smart farming as critical industries in terms of time latencies
Service layer	• Data analytics and predictive modelling for decision-support systems	• Data analytics and predictive modelling for decision-support systems

	• High accuracy (indoor and outdoor) positioning and mapping solutions cost-effective enough for smaller farms to adopted precision farming • Farm management systems and precision farming solutions easily adaptable to holdings of different sizes • Service providing infrastructure for 3rd parties allowing the integration of external service providers that use internal data (for example, a company that provides irrigation optimization analysis) • Farm management systems satisfying energy efficiency objectives, related to cultivation and farm management processes • User interfaces with high usability and low learning curve • Stimulate innovation in targeting cross-sectorial IoT applications such as smart energy management for farms, smart nutrition management for end-consumers	• Farm management systems satisfying energy efficiency objectives, related to cultivation and farm management processes
Interoperability and standardisation	• Specification and implementation of protocols for agricultural machinery information exchange, including fleet management • Development of open reference vocabularies, formats and protocols for data storage and exchange allowing flexible interaction between arbitrary actors across the food chain • Specification of universal identification standards and technologies inter-linking among different addressing techniques, to make sure those different parts in food traceability scenarios can be properly referred to and logically interrelated.	• Development of open reference vocabularies, formats and protocols for data storage and exchange allowing flexible interaction between arbitrary actors across the food chain
Data management and protection	• Digital Rights Management in the farming domain, including scenarios of data aggregation and data sharing	• Trusted data: integrity and authenticity of the data generated/stored.

(*Continued*)

Table 3.1 Continued

Development	2016–2020	Beyond 2020
	• Trusted data: integrity and authenticity of the data generated/stored. The origin of the product, the processing stages it passed through and other sensitive information must be known. Guarantee the trustworthiness of the source is a crucial requirement. • Low cost authentication mechanisms for devices/machines • Access control policies and access control mechanisms for individual users and individual pieces of information • Develop hybrid cloud storage and interaction models which unite the universal data availability of cloud solutions with the individual, local control of data owners and the resilience against disruptive crisis provided by de-centralized island networks and individualized peer-to-peer communication	The origin of the product, the processing stages it passed through and other sensitive information must be known. Guarantee the trustworthiness of the source is a crucial requirement. • Low cost authentication mechanisms for devices/machines

3.3.9.1 Business Models and Innovation Ecosystems

The deployment and adoption of IoT technologies and applications in the farming sector need to address the different challenges and opportunities created by the new business models introduced. A number of issues that have to be considered are presented below:

- Provide evidence of the sustainability of the IoT-based business, both for the supply (ICT) and demand (agri-food) sides. From the point of view of the users, the quantifiable benefit and profitability must compensate for the cost of the IoT solutions.
- A challenge, and at the same time an opportunity, is the possibility of devising new, disruptive business models. Some traditional companies, for instance, are already shifting their business to data-driven models.
- Stimulate and empower the role of consumers as key element/ beneficiaries of the IoT-enabled food supply chain

- Build trust around the smart farming technology made in the EU (for example through a IoT trust label)
- Analyse the important role of farm advisory services in the context of data-driven farming
- Foster the creation of digital farming innovation hubs, not only in EU, but at regional/national level, to accelerate innovation and adoption, facilitate the early exchange of best practice.

3.3.9.2 Societal Aspects

The complexity of smart farming and the proliferation of IoT technologies provided by various stakeholders or ecosystems requires considering the following social aspects when addressing the implementation and deployments:

- Identify the lack of digital skills preventing the adoption of digital agriculture in some EU regions, and take corrective action involving the necessary stakeholders (cooperatives, regional administrations) in order to prevent a digital divide in EU's agriculture.
- Provide evidence of the positive impact of the digitisation of farming in the EU's rural economy. Analyse new potential relationships between the rural and urban economies.
- Stimulate and empower the role of consumers as key element/beneficiaries of the IoT-enabled food supply chain
- Promote transparency of the food production process and encourage data sharing by farmers along agri-food value chain
- Take action to ensure that the benefits of IoT reach all types of farms, especially smaller and family-owned holdings, which constitute the vast majority in Europe, and thus are of utmost socioeconomic importance

3.3.9.3 Coordination among Different DGs, Programmes and Member States

Although H2020 can help by providing a spearhead or lighthouse in the form of a Large Scale Pilot, a large amount of IoT take-up in the farming sector will be happening in parallel under national or regional initiatives (and thus in a smaller, more fragmented scale). Much of this technology take-up can or will be facilitated by public investments of Structural Funds or other funding sources managed at a national or even regional level, such as EAFRD (European Agricultural Fund for Rural Development, implementing the Common Agricultural Policy 2014–2020, CAP) and ERDF (European

Regional Development Fund), the latter in regions with Smart Specialization Strategies.

The active coordination of the different Administrations involved (EU, national and regional) towards streamlining efforts and generating operational efficiencies can only contribute to maximize the chances of having a vibrant smart farming ecosystem in the EU benefitting users and providers alike, as well as consumers and the European society and economy.

National, regional and cities' Public Administrations can play an important role as either users, infrastructure managers, procurers, initial demand facilitators or subsidizers. In this sense, it is important to consider the aggregation of national and regional initiatives related to IoT for pre-commercial procurement, deployment, coordination of R&I programmes, etc, and the exchange of best-practices among leading Member States/Regions and followers/laggards.

Following the IoT cross-cutting actions implemented in the H2020 Work Programme 2016–17, further collaboration in the design of new work programmes is highly desirable among DG CONNECT, DG AGRI, DG RESEARCH, DG MARE (to include aquaculture in the future actions), as well as DG ENER and DG Health and Food Safety.

3.3.9.4 Policy and Regulations

In the context of the DSM, the barriers blocking widespread deployment of IoT-based innovations in farming (including interoperability, connectivity, and security) must be lowered. The agrifood sector should be no exception in benefitting from the more agile digital economy. In this vein, policy makers could benefit from a sound analysis of major threats: data management and trust (ownership, rules for access, security, and, where applicable, privacy), connectivity and internet access in rural areas, cost of high accuracy positioning services, and digital literacy and skills, among others.

In the context of the EU Common Agricultural Policy (CAP), whose primary objective nowadays is market-oriented sustainable food production, mechanisms could be designed to supporting the adoption of digital technologies in farming uniformly across the EU.

Regulations regarding traceability and labelling should be addressed to facilitate adoption of new IoT solutions for traceability at EU-wide level.

3.4 IoT and Related Future Internet Technologies

3.4.1 Cloud Computing

The Cloud computing definition provided by the National Institute of Standard and Technologies (NIST) covers the main features of the technology. The definition states that the cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [25].

Figure 3.29 summarises the main aspects of cloud, characteristics, the layered architecture and the standard service models. In the following, we describe a few important aspects of Cloud. The architecture of Cloud can be split into several layers: datacentre (hardware), infrastructure, platform, and application. Each of them can be seen as a service for the layer above and as a consumer for the layer below. Cloud services can be grouped in three main categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS refers to the provisioning of applications running on Cloud environments. Applications are typically accessible through a thin client or a web browser. PaaS refers to platform-layer

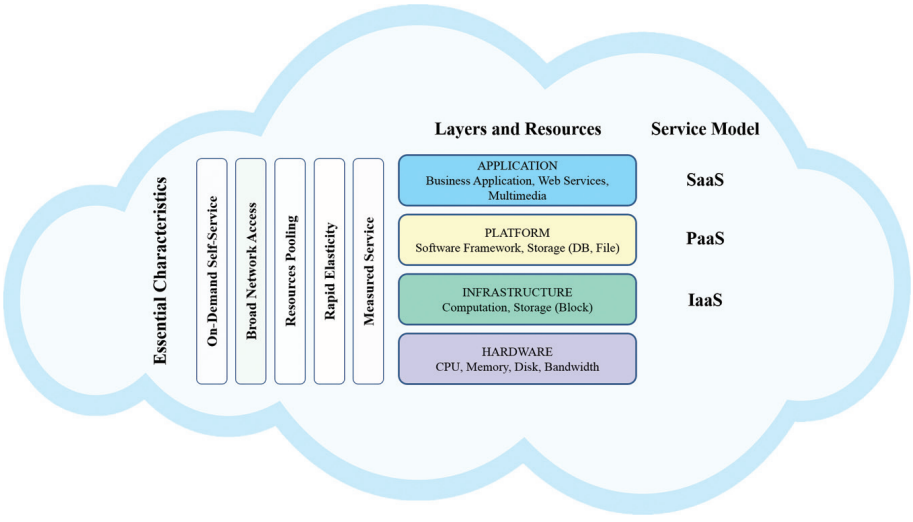

Figure 3.29 Cloud paradigm [24].

resources (e.g., operating system support, software development frameworks, etc.). IaaS refers to providing processing, storage, and network resources, allowing the consumer to control the operating system, storage and applications [24]. IoT can benefit from the capabilities and resources of cloud to compensate its technological constraints (e.g., storage, processing, communication, etc.). Cloud can offer an effective solution for IoT service management and composition as well as for implementing applications and services that exploit the things or the data generated by the things. Cloud can benefit from IoT by extending its usage to deal with real world things in a more distributed and dynamic manner, and for delivering new services in a large number of real life scenarios.

Cloud computing provide a unique opportunity to unify the real, digital and the virtual worlds. IoT enables the building of very large infrastructures that facilitate the information-driven real-time integration of the physical world, sensing/actuating, processing, analytics, with the digital, cyber and virtual worlds on a global scale.

3.4.2 Edge Computing

Virtualisation of objects will push for the convergence of cloud computing and IoT will enable unprecedented opportunities in the IoT services arena [80]. The central idea is that IoT's biggest transformation will be in shifting power in a network from the center to the edge. Rather than devices and users communicating through central hubs – mainframes or cloud based management servers, IoT will allow devices to communicate directly with each other, which is the implementation of the "democratic" vision of a decentralized Internet [82].

The IoT layered architecture include the edge intelligence into the edge computing/processing where all the data capture, processing is done at the device level among all the physical sensor/actuators/devices that include controllers based on microprocessors/microcontrollers to compute/process and wireless modules to communicate. The intelligence at the edge supports devices to use their data sharing and decision-making capabilities to interact and cooperate in order to process the data at the edge, filter it and select/prioritize what is important.

This intelligent processing at the edge select the "smart data" that is transferred to the central data stores for further processing in the cloud. This allows including the Edge Cloud for processing data and addressing the challenges of response-time, reliability and security. For real time fast

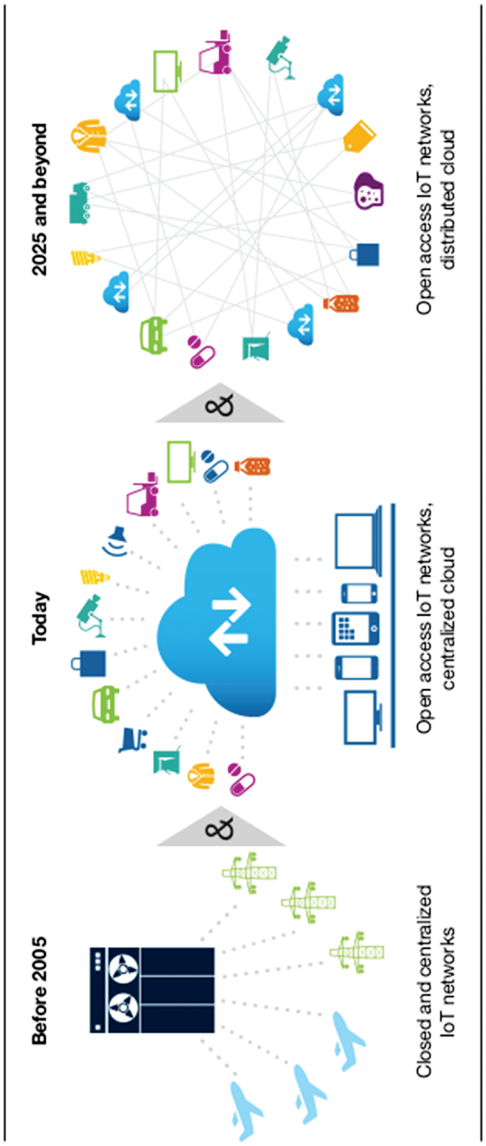

Figure 3.30 Evolution of IoT from centralised networks to distributed cloud [82].

processes, the sensor/actuator edge devices could generate data much faster than the cloud-based apps can process it.

The use of intelligent edge devices require to reduce the amount of data sent to the cloud through quality filtering and aggregation and the integration of more functions into intelligent devices and gateways closer to the edge reduces latency. By moving the intelligence to the edge, the local devices can generate value when there are challenges related to transferring data to the cloud. This will allow as well for protocol consolidation by controlling the various ways devices can communicate with each other.

As part of this convergence, IoT applications (such as sensor-based services) will be delivered on-demand through a cloud environment [81]. This extends beyond the need to virtualize sensor data stores in a scalable fashion. It asks for virtualization of Internet-connected objects and their ability to become orchestrated into on-demand services (such as Sensing-as-a-Service).

Computing at the edge of the mobile network defines the IoT-enabled customer experiences and require a resilient and robust underlying network infrastructures to drive business success. IoT assets and devices are connected via mobile infrastructure, and cloud services are provided to IoT platforms to deliver real-time and context-based services.

Data transmission costs and the latency limitations of mobile connectivity pose challenges to many IoT applications that rely on cloud computing. Mobile edge computing will enable businesses to deliver real-time and context-based mobile moments to users of IoT solutions, while managing the cost base for mobile infrastructure. A number of challenges listed below have to be addressed when considering edge-computing implementation [83]:

- Cloud computing and IoT applications are closely connected and improve IoT experiences. IoT applications gain functionality through cloud services, which in turn open access to third-party expertise and up-to-date information.
- Mobile connectivity can create challenges for cloud-enabled IoT environments. Latency affects user experiences, so poor mobile connectivity can limit cloud-computing deployments in the IoT context.
- Mobile edge computing provides real-time network and context information, including location, while giving application developers and business leaders access to cloud computing capabilities and a cloud service environment that's closer to their actual users.
- Mobile edge computing is an important network infrastructure component for block chain. The continuous replication of "blocks" via devices

on this distributed data centre poses a tremendous technological challenge. Mobile edge computing reveals one opportunity to address this challenge.

Edge computing refers to data processing power at the edge of a network and in industrial IoT applications (i.e. power production, smart traffic lights, manufacturing, etc.) the edge networked devices capture data and process date close to the source of performing "edge analytics" on the data. Edge computing complement cloud computing, since an analytic model or rules are created in the cloud then pushed out to edge devices. Edge computing is closely related to fog computing, that entails data processing from the edge of the network to the cloud.

For the future IoT applications it is expected that more of the network intelligence to reside closer to the source. This will push for the rise of Edge Cloud/Fog, Mobile Edge computing architectures, as most data will be too noisy or latency-sensitive or expensive to be transfer to the cloud.

The previous IERC SRIAs have identified the importance of interoperability semantic technologies towards discovering devices, as well as towards achieving semantic interoperability.

3.5 Networks and Communication

The IERC SRIA intends to lay the foundations for the IoT to be developed by research through to the end of this decade and for subsequent innovations to be realised even after this research period. Within this timeframe, the number of connected devices, their features, their distribution and implied communication requirements will develop, as will the communication infrastructure and it is predicted that low-power short-range networks will dominate wireless IoT connectivity through 2025, far outnumbering connections using wide-area IoT networks [21]. IoT technologies are extending the known business models and leading to the proliferation of different ones as companies push beyond the data, analytics and intelligence boundaries, while everything will change significantly. IoT devices will be contributing to and strongly driving this development.

Changes will first be embedded in given communication standards and networks and subsequently in the communication and network structures defined by these standards.

Further developments of networks and communication technologies are required by the emergence of the Tactile Internet, in which ultra-responsive

and ultra-reliable network connectivity will enable it to deliver physical haptic experiences remotely for different IoT applications. The Tactile Internet will add a new dimension to human-machine interaction through building real-time interactive systems. The combination of Tactile Internet and IoT applications will enable haptic communications at the edge and in the interaction between humans and machines, infrastructure and environment by providing the medium for transporting touch and actuation in real-time i.e., the ability of haptic control through the Internet, in addition to no haptic control and data.

3.5.1 Network Technology

The development in cloud and mobile edge computing requires network strategies for fifth evolution of mobile the 5G, which represents clearly a convergence of network access technologies. The architecture of such network has to integrate the needs for IoT applications and to offer seamless integration and optimise the access to Cloud or mobile edge computing resources. IoT is estimated that will connect 30 billion devices. All these devices are connecting humans, things, information and content, which is changing the performance characteristics of the network. Low latency is becoming crucial (connected vehicles or industrial equipment must react in ms), there is a need to extend network coverage even in non-urban areas, a better indoor coverage is required, ultra-low power as many of the devices will be battery operated is needed and a much higher reliability and robustness is requested.

5G networks will deliver 1,000 to 5,000 times more capacity than 3G and 4G networks today and will be made up of cells that support peak rates of between 10 and 100 Gbps. They need to be ultra-low latency, meaning it will take data 1–10 milliseconds to get from one designated point to another, compared to 40–60 milliseconds today. Another goal is to separate communications infrastructure and allow mobile users to move seamlessly between 5G, 4G, and WiFi, which will be fully integrated with the cellular network. To support the increasing data rates and number of connected devices in urban environments, mobile networks are increasingly dense and heterogeneous in cell-size and radio access technologies (multi-RATs).

Applications making use of cloud computing, and those using edge computing will have to co-exist and will have to securely share data. The right balance needs to be found between cloud/mobile edge computing to

optimize overall network traffic and optimize the latency. Facilitating optimal use of both mobile edge and cloud computing, while bringing the computing processing capabilities to the end user. Local gateways can be involved in this optimization to maximize utility, reliability, and privacy and minimize latency and energy expenditures of the entire networks.

Future networks have to address the interference between the different cells and radiations and develop new management models control roaming, while exploiting the co-existence of the different cells and radio access technologies. New management protocols controlling the user assignment to cells and technology will have to be deployed in the mobile core network for a better efficiency in accessing the network resource. Satellite communications need to be considered as a potential radio access technology, especially in remote areas. With the emerging of safety applications, minimizing the latency and the various protocol translation will benefit to the end-to-end latency. Densification of the mobile network strongly challenges the connection with the core network. Future networks should however implement cloud utilization mechanisms to maximize the efficiency in terms of latency, security, energy efficiency and accessibility.

In this context, there is a need for higher network flexibility combining Cloud technologies with Software Defined Networks (SDN) and Network Functions Virtualisation (NFV), that will enable network flexibility to integrate new applications and to configure network resources adequately (sharing computing resources, split data traffic, security rules, QoS parameters, mobility, etc.).

The evolution and pervasiveness of present communication technologies has the potential to grow to unprecedented levels in the near future by including the world of things into the developing IoT. Network users will be humans, machines, things and groups of them.

3.5.2 Communication Technology

The growth in mobile device market is pushing the deployment of IoT applications where these mobile devices (smart phones, tablets, etc. are seen as gateways for wireless sensors and actuators.

Communications technologies for the Future Internet and the IoT will have to avoid such bottlenecks by construction not only for a given status of development, but also for the whole path to fully developed and still growing nets.

The inherent trend to higher complexity of solutions on all levels will be seriously questioned – at least with regard to minimum energy IoT devices and services.

Their communication with the access edges of the IoT network shall be optimized cross domain with their implementation space and it shall be compatible with the correctness of the construction approach.

These trends require the extension of the spectrum in to the 10–100 GHz and unlicensed band and technologies like WiGig or 802.11ad that are mature enough for massive deployment, can be used for cell backhaul, point-to-point or point-to-multipoint communication. The use of advanced multi-/massive-MIMO technologies have the capability to address both coverage and bandwidth increase, while contributing to optimize the usage of the network resources adequately to real need.

The IoT applications will embed the devices in various forms of communication models that will coexist in heterogeneous environments. The models will range from device to device, device to cloud and device to gateway communications that will bring various requirements to the development of electronic components and systems for IoT applications. The first approach considers the case of devices that directly connect and communicate between each another (i.e. using Bluetooth, Z-Wave, ZigBee, etc.) not necessarily using an intermediary application server to establish direct device-to-device communications. The second approach considers that the IoT device connect (i.e. using wired Ethernet or Wi-Fi connections) directly to Internet cloud/fog service of various service providers to exchange data and control message traffic. The third approach, the IoT devices connect to an application layer gateway running an application software operating on the gateway device, providing the "bridge" between the device and the cloud service while providing security, data protocol translation and other functionalities.

The deployment of billions of devices requires network agnostic solutions that integrate mobile, narrow band IoT (NB IoT), LPWA networks, (LoRA, Sigfox, Weightless, etc), and high speed wireless networks (Wi-Fi), particularly for applications spanning multiple jurisdictions.

LPWA networks have several features that make them particularly attractive for IoT devices and applications that require low mobility and low levels of data transfer:

- Low power consumption that enable devices to last up to 10 years on a single charge
- Optimised data transfer that supports small, intermittent blocks of data

Table 3.2 LPWA network protocols

Name of Standard	Weightless –W	Weightless –N	Weightless –P	SigFox	LoRaWAN	LTE-Cat M	IEEE P802.11ah (LP WiFi)	Dash7 Alliance Protocol 1.0	Ingenu RPMA	nWave
Frequency Band	TV white-space (400–800 MHz)	Sub-GHZ ISM	Sub-GHZ ISM	868 MHz/ 902 MHz ISM	433/868/ 780/915 MHz ISM	Cellular	License-exempt bands below 1 GHz, excluding the TV White Spaces	433, 868, 915 MHz ISM/SRD	2.4 GHz ISM	Sub-GHz ISM
Channel Width	5 MHz	Ultra narrow band (200 Hz)	12.5 kHz	Ultra narrow band	EU: 8×125 kHz, US 64×125 kHz/ 8×125 kHz, Modulation: Chirp Spread Spectrum	1.4 MHz	1/2/4/8/16 MHz	25 KHz or 200 KHz	1 MHz (40 channels available)	Ultra narrow band
Range	5 km (urban)	3 km (urban)	2 km (urban)	30–50 km (rural), 3–10 km (urban), 1000 km LoS	2–5 k (urban), 15 k (rural)	2.5–5 km	Up to 1 km (outdoor)	0–5 km	>500 km LoS	10 km (urban), 20–30 km (rural)

(*Continued*)

Table 3.2 Continued

Name of Standard	Weightless –W	Weightless –N	Weightless –P	SigFox	LoRaWAN	LTE-Cat M	IEEE P802.11ah (LP WiFi)	Dash7 Alliance Protocol 1.0	Ingenu RPMA	nWave
End Node Transmit Power	17 dBm	17 dBm	17 dBm	10 µW to 100 mW	EU: $< +14$ dBm, US: $< +27$ dBm	100 mW	Dependent on Regional Regulations (from 1 mW to 1 W)	Depending on FCC/ETSI regulations	to 20 dBm	25–100 mW
Packet Size	10 byte min.	Up to 20 bytes	10 byte min.	12 bytes	Defined by user	∼100–1000 bytes typical	Up to 7,991 Bytes (w/o aggregation), up to 65,535 Bytes (with aggregation)	256 bytes max/packet	Flexible (6 bytes to 10 kbytes)	12 byte header, 2–20 byte payload

Uplink Data Rate	1 kbps to 10 Mbps	100 bps	200 bps to 100 kbps	100 bps to 140 messages/ day	EU: 300 bps to 50 kbps, US: 900–100 kbps	∼200 kbps	150 Kbps ∼346.666 Mbps	9.6 kb/s, 55.55 kbps or 166.667 kb/s	AP aggregates to 624 kbps per Sector (Assumes 8 channel Access Point)	100 bps
Downlink Data Rate	1 kbps to 10 Mbps	No downlink	200 bps to 100 kbps	Max. 4 messages of 8 bytes/day	EU: 300 bps to 50 kbps, US: 900–100 kbps	∼200 kbps	150 Kbps ∼346.666 Mbps	9.6 kb/s, 55.55 kbps or 166.667 kb/s	AP aggregates to 156 kbps per Sector (Assumes 8 channel Access Point)	–
Devices per Access Point	Unlimited	Unlimited	Unlimited	1 M	Uplink: >1, Downlink: <100 k	20k+	8191	NA (connectionless communication)	Up to 384,000 per sector	1 M

(*Continued*)

Table 3.2 Continued

Name of Standard	Weightless –W	Weightless –N	Weightless –P	SigFox	LoRaWAN	LTE-Cat M	IEEE P802.11ah (LP WiFi)	Dash7 Alliance Protocol 1.0	Ingenu RPMA	nWave
Topology	Star	Star	Star	Star	Star on Star	Star	Star, Tree	Node-to-node, Star, Tree	Typically Star. Tree supported with an RPMA extender	Star
End node roaming allowed	Yes	Yes	Yes	Yes	Yes	Yes	Allowed by IEEE 802.11 amend-ments (e.g., IEEE 802.11r)	Yes	Yes	Yes
Governing Body	Weightless SIG			Sigfox	LoRa Alliance	3GPP	IEEE 802.11 working group	Dash7 Alliance	Ingenu (OnRamp)	Weightless SIG

- Low device unit cost
- Few base stations required to provide coverage
- Easy installation of the network
- Dedicated network authentication
- Optimised for low throughput, long or short distance
- Sufficient indoor penetration and coverage

These different types of networks are needed to address IoT product, services and techniques to improve the Grade of Service (GoS), Quality of Service and Quality of Experience (QoE) for the end users. Customization-based solutions, are addressing industrial IoT while moving to a managed wide-area communications system and, ecosystem collaboration.

Intelligent gateways will be needed at lower cost to simplify the infrastructure complexity for end consumers, enterprises, and industrial environments. Multi-functional, multi-protocol, processing gateways are likely to be deployed for IoT devices and combined with Internet protocols and different communication protocols.

These different approaches show that device interoperability and open standards are key considerations in the design and development of internetworked IoT systems.

Ensuring the security, reliability, resilience, and stability of Internet applications and services is critical to promoting the concept of trusted IoT based on the features and security provided of the devices at various levels of the digital value chain.

3.6 IoT Standardisation

In recent publications mapping emerging technologies to their Hype Cycle, Gartner positions the IoT at the top of the "Peak of Inflated Expectations" [14].

The assessment is widely shared and is reflected by significant IoT related activities in companies of all sizes, in industry standards groups, consortia, alliances and in the press and media. Many observers also remark on the number of technologies, alliances and consortia across the IoT landscape and agree that a consolidation is imminent. These expectations broadly align with the lifecycle phases that Gartner's model predicts for IoT. Gartner's view is that IoT will reach the "Plateau of Productivity" in 5–10 years – somewhere around 2020–2025. On that basis, they anticipate that the period 2015–2019 will see a consolidation phase with a corresponding reduction in hype, a period of intense development of standards, and a transition into a period of real product development.

Table 3.3 Standardisation key challenges addressed by AIOTI

Domain	Activities
Architecture	• Guidelines and recommendations, which contribute to the consolidation of architectural frameworks, reference architectures, and architectural styles in the IoT space.
Semantic Interoperability	• Guidelines and recommendations, which contribute to the consolidation of semantic interoperability approaches in the IoT space.
Privacy	• Guidelines and recommendations regarding personal data and personal data protection to the various categories of stakeholders in the IoT space.

Standardisation will play a key role in the consolidation of IoT landscape; since many of the benefits of IoT will occur based on widespread adoption, the development of global standards is pivotal to ensuring economies of scale and impact.

The standardisation priorities for AIOTI WG03 [61] will be a focus of European engagement and steering in the standardization process. In collaboration with other AIOTI working groups, the focus will be to:

- Maintain a view on the landscape of IoT standards-relevant activities being driven by SDOs, Consortia, Alliances and OSS projects.
- Provide a forum for analysis, discussion and alignment of strategic, cross-domain, technical themes and shared concerns across landscape activities
- Develop recommendations and guidelines addressing those concerns
- Engage the IoT community in disseminating and promoting the results and steering emerging standards

In collaboration with ST505, AIOTI WG03 will build an understanding of SDOs, Alliances, and Consortia; their respective specifications, technologies, and spheres of influence; and the breadth, depth and sustainability of any Open Source Software, which has established a usage profile.

The outputs of the landscape work will drive the WG03 program. Analysis of gaps, divergences, common concerns, and major players will inform the agenda of challenges to be addressed, guidelines and recommendations to be developed and groups to be engaged with.

The following table provides the three key challenges the workgroup is currently responding to.

AIOTI WG03 will support the implementation of the goals set by the EC [16] and promote the use of open standards through actions that: (1) support the entire value chain, (2) apply within IoT domains and cross-IoT domains

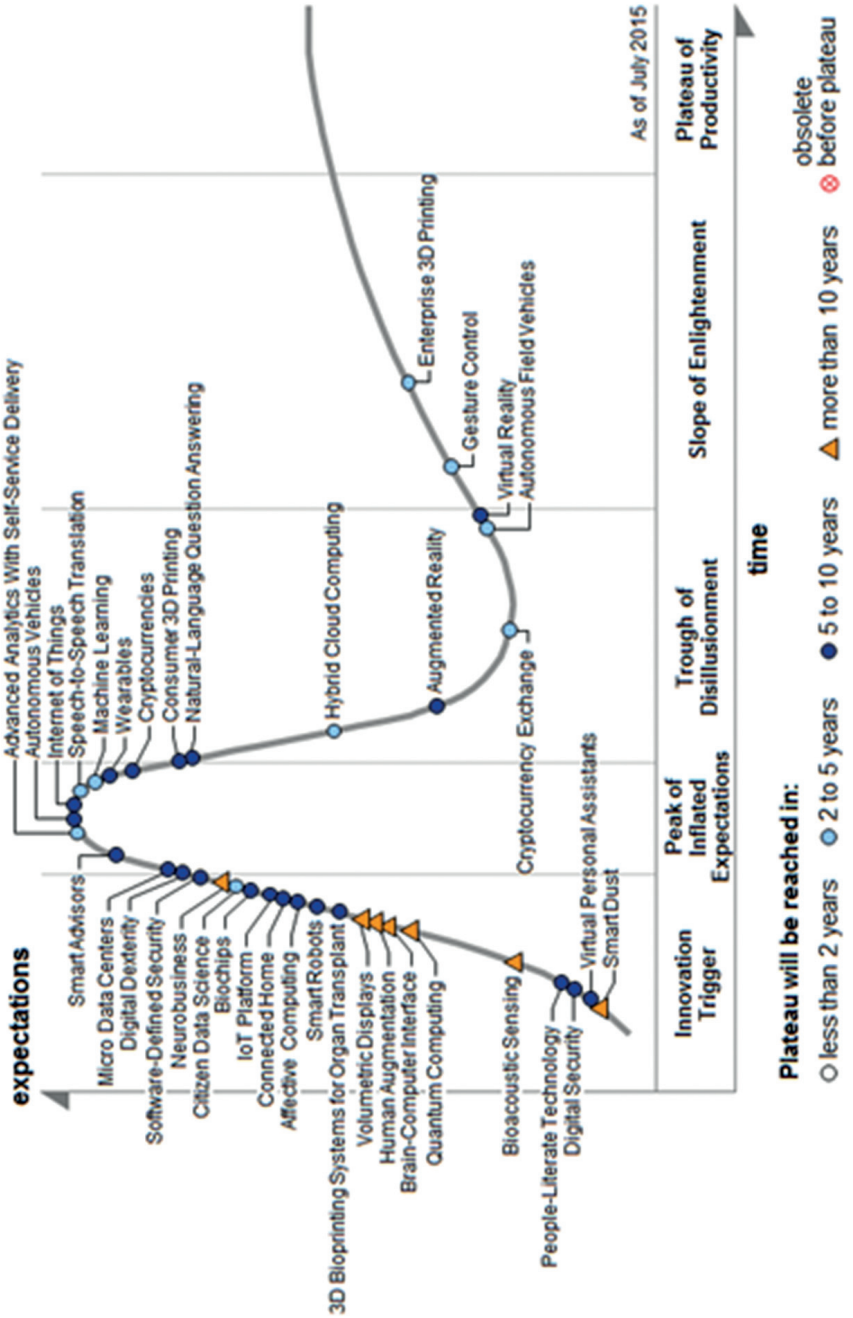

Figure 3.31 Hype Cycle of emerging technologies [14].

Table 3.4 Standardisation challenges for IoT

Specific IoT Standardisation Challenges	
2016–2020	Beyond 2020
• Recommendations of reference architectures, both for experimentation and deployments within IoT domains and cross IoT domains	
• Identification of missing (semantic) interoperability standards and technologies within IoT domains and cross IoT domains and recommendations on solving them	
• Recommendations and guidelines on solving protocol and interface gaps needed to support new IoT features within IoT domains and cross IoT domains. Promote the uptake of IoT standards in public procurement to avoid lock-in	• Further work on recommendations and guidelines on solving protocol and interface gaps needed to support new IoT features within IoT domains and cross IoT domains. Promote the uptake of IoT standards in public procurement to avoid lock-in
• Promoting the use and development of Open Reference Vocabularies and Open Application Programming Interfaces to allow for flexible ad-hoc communication and interaction between different actors within IoT domains and cross IoT domains	• Further development and promotion of the use and development of Open Reference Vocabularies and Open Application Programming Interfaces to allow for flexible ad-hoc communication and interaction between different actors within IoT domains and cross IoT domains
• Provide guidelines on how to translate the Digital Rights Management recommendations within IoT domains and cross IoT domains	
• Recommendation of an interoperable IoT numbering space that transcends geographical limits, and an open system for object identification and authentication, which can be applied within IoT domains and cross IoT domains	
• Explore options and recommend guiding principles, including guidelines for the support of developing standards, for trust, privacy and end-to-end security, e.g. through a 'trusted IoT label' that can be applied within IoT domains and cross IoT domains	• Explore options and recommend guiding principles, including guidelines for the support of developing standards, for trust, privacy and end-to-end security, e.g. through a 'trusted IoT label' that can be applied within IoT domains and cross IoT domains

and (3) are integrating multiple technologies. This is done based on streamlined international cooperation, which enables easy and fair access to standard essential patents (SEPs). In order to accomplish this goal several potential challenges can be foreseen, which are presented in the following table.

3.7 IoT Security

Security needs to be designed into IoT solutions from the concept phase and integrated at the hardware level, the firmware level, the software level and the service level. IoT applications need to embed mechanisms to continuously monitor security and stay ahead of the threats posed by interactions with other IoT applications and environments. Trust is based on the ability to maintain the security of the IoT system and the ability to protect application/customer information, and as well as being able to respond to unintended security or privacy breaches. In the IoT it is important to drive security, privacy, data protection and trust across the whole IoT ecosystem and no company can "do it alone" in the loT space; success will require organizations to partner, value chains to be created and ecosystems to flourish. Yet as loT users start to bring more players, service providers and third party suppliers into their value chain, tech firms and loT solutions providers will face increasing pressure to demonstrate their security capabilities [10].

The worlds of IT and operational technology (OT) are converging, and IT leaders must manage their transition to converging, aligning and integrating IT and OT environments [12]. The benefits that come from managing IT and OT convergence, alignment and integration include optimized business processes, enhanced information for better decisions, reduced costs, lower risks and shortened project timelines. IT and OT are converging in numerous important industries, such as healthcare, transportation, defence, energy, aviation, manufacturing, engineering, mining, oil and gas, natural resources and utilities. IT leaders who are impacted by the convergence of IT and OT platforms should consider the value and risk of pursuing alignment between IT and OT, as well as the potential to integrate people, tools and resources used to manage and support both technology areas. A shared set of standards and platforms across IT and OT will reduce costs in many areas of software management, while the reduction in risks that will come from reducing malware intrusion, internal errors and cybersecurity can be enhanced if IT security teams are shared, seconded or combined with OT staff to plan and implement holistic IT-OT security [12].

The evolution of connected devices as nodes to the IoT brings limitless possibilities. As more and more everyday things are connected to the Internet – medical devices, automobiles, homes, etc. – the long-term forecast for the IoT is staggering: by 2020, there will be 212 billion installed things, 30 billion autonomously connected things and approximately three million petabytes of embedded system data, all of which combined are expected to generate nearly $9 trillion in business value. IoT applications fall into three basic categories [11]:

- Mobile or desktop applications that control IoT devices;
- IoT firmware and embedded applications;
- Applications on open IoT platforms (for example, apps built for Apple Watch).

All of these applications need to be protected or they run the risk of undesirable outcomes such as:

- Improper or unsafe operation of IoT devices;
- Theft of confidential data, private user information or application-related intellectual property;
- Fraud and unauthorized access to payment processing channels;
- Damage to companies brand image and deterioration of customer, prospect and partner trust.

In the case of IoT, applications can be attacked in many ways, often involving apps that first obtain access to the IoT application, then start monitoring, controlling, and tampering with the device.

A holistic approach that involves the device, data, network and application layers is required and the following chart summarizes key IoT security components that must be considered [11]:

The following policy recommendations on net neutrality and IoT, given the current relevance of net neutrality to the European policy debate, following agreement of the Telecoms Single Market legislative package are given in [62] and summarised below:

- Embed "safe and secure software" design and development methodologies across all levels of device/application design and development and implement security into that life cycle at the same time.
- Design, deliver and operate adaptive and dynamic end-to-end security over heterogeneous infrastructures integrating IoT, networks and cloud infrastructures. It is recommended to use underlying standardised OS and hardware security features where architecture permits. The deployment

Information technologies: conventional computers, operating systems, networking components and software platforms.

Operational technologies: industrial control system and networks.

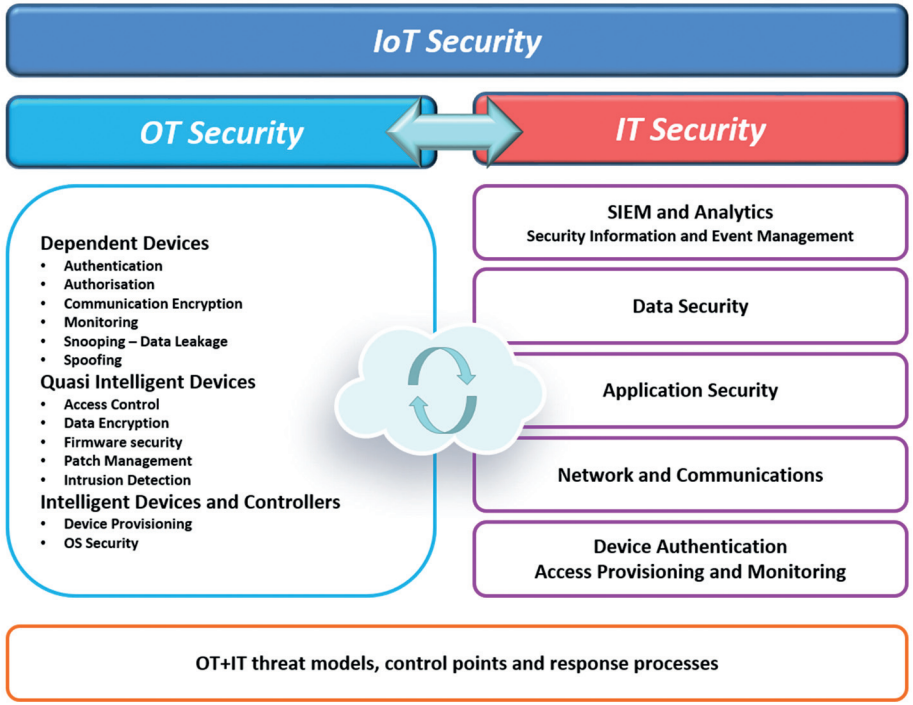

Figure 3.32 IoT security challenges for IT and OT technologies (Adapted from [11]).

should not be specific or propose a modification of existing OS and hardware already integrated by IoT.

- Develop best practices confirming minimum requirements for provision of secure, encrypted and integrity-protected channel, mutual authentication processes between devices and measures securing that only authorised agents can change settings on communication and functionality.
- Develop a "New Identity for Things" – To date, Identity and Access Management (IAM) processes and infrastructures have been primarily focused on managing the identities of people. IAM processes and infrastructure must now be re-envisioned to encompass the amazing variety of the virtualized infrastructure components. For example, authentication and authorization functions will be expanded and enhanced to address people, software and devices as a single converged framework.
- Develop a Common Authentication architecture – by investigation of a Secure Identity and Trusted Authentication mechanism, for example one which takes into account different authentication standards and will provide a single-sign-on solution for IoT applications moving between different systems.
- Certification – the certification framework and self-certification solutions for IoT applications have not been developed yet. The challenge will be to have generic and common framework, while developing business specific provisions. This framework should provide evaluation assurance levels similar to the Common Criteria for Information Technology Security Evaluation (IS0/IEC 15408), which should serve as the reference.

3.7.1 IoT Security Framework based on Artificial Intelligence Concepts

Large-scale applications and services based on the IoT are increasingly vulnerable to disruption from attack or information theft. Vulnerability in general terms is defined as the opportunity for a threat to cause loss. A threat is any potential danger to a resource, originating from anything or anyone that has the potential to cause a threat. Clearly, specific and more intelligent security solutions are required to cope with these issues, which if not addressed may become barriers for the IoT deployment on a broad scale.

Swarm intelligence (SI) is such a technological area, which can inspire the design of new IoT security solutions. A subfield of artificial intelligence,

SI studies the emergent collective intelligence of groups of agents based on social behaviour that can be observed in nature, such as ant colonies, flocks of birds, fish schools and bee hives, where a number of individuals with limited capabilities are able to produce intelligent solutions for complex problems. Vulnerability and reaction to threats seem to be a common thread and IoT can take inspiration from ant colonies, flocks of birds, fish schools and bee hives on how to react to threats.

IoT objects have more capabilities than the above examples; in fact, the trend is towards distributed models, meaning that objects are becoming more intelligent, capable of making their own authentication, authorization and other trust management decisions. Nevertheless, by embracing principles of swarm intelligence, IoT systems can react more effectively to threats. Clearly, a group of IoT objects has more abilities and resources to process large amounts of information in real time in order to prevent, detect and react to perceived or real threats, as well as make decisions based on the acquired information.

The idea is not to make the IoT objects mobile in order to physically group objects when threats occur but to augment the intelligence internalized in each object, with new kind of intelligence that allow the individual resources and intelligence in objects to group. Not all objects need to group at all times. Objects can group around one object identified as a point of attack or around a path of objects.

Clustering is therefore an important area and has been applied in many domains, such as spatial data analysis, image processing, marketing and pattern recognition, etc. For example, ant-based clustering is a type of clustering algorithm that imitates the behaviour of ants, with a perfect social organization where each type of individual specializes in a specific activity within the colony.

In IoT security, the purpose of clustering is to cluster IoT objects into groups according to some predefined rules addressing the issues inherent in detecting and dealing with threats.

The essence of this concept can be best illustrated by the following rules of separation, alignment, cohesion of the first multi-agent algorithm developed by Craig Reynolds in 1986 simulating swarm behaviour.

- Separation: going away from other agents. In the IoT context, this rule would become preserving the distributed nature of the IoT system in the absence of threats, so that individual resources can be focused on the functions to be performed by each object. Unnecessary clustering

would consume resources and would even expose intelligence crowding to attack.
- Cohesion: going to the centre of the surrounding agents. In the IoT context, this rule would become steering resources and intelligence towards one or several points of attack.
- Alignment: heading towards the same direction of other agents. In the IoT context, this rule would become steering along a path of attack.

Complex behaviour can be programmed as rules, based on self-organization. The basic concept is to define rules and constraints and let the IoT system self-organize in the presence of threats. The self-organization properties may help security architects and other professionals to discover new security solutions.

3.7.2 Self-protecting, Self-optimizing and Self-healing IoT Concepts

Self-protecting capability features opens up the possibility for IoT to be used in systems that need to protect themselves from malicious attacks, because security, privacy and data protection are at stake.

IoT may offer other capabilities in addition to self-protection, such as self-optimization and self-healing. With enhanced swarm intelligence, IoT objects are capable of cooperating and sharing resources efficiently. This allows for solving numerous optimization problems, which are otherwise difficult to implement due to the large resources required. Self-optimization capabilities mean that SI can be used in many IoT applications, such as optimal node localization, optimal coverage control, and a wide variety of intelligent routings: shortest transportation path, best available channel at a point in time, minimum energy consumption.

The use of swarm intelligence supported by edge technologies (such as WSN), makes it possible to add more and more cognitive intelligence to the IoT objects, and at the same time add increasing swarm intelligence to the collaborative and connectivity space. Thus, IoT objects strive to improve to a higher level of local intelligence, close to human intelligence, in order to fulfil their function in a distributed manner, while the collective intelligence is centralized in order to solve problems that are more complex.

Swarm intelligence allows IoT to adopt a wide range of solutions already found in AI, data mining and robotics, so that IoT applications become more robust, flexible, adaptable, scalable and self-organized. The self-organization property allows for the formation of swarms of various shapes and sizes.

Each IoT object, which is part of the swarm has an agent with just enough knowledge about its object (such as position, speed) in order to engage the object in collaborative tasks with other objects in the swarm. Thus, IoT objects may be fixed or mobile and the IoT objects may enter and leave the swarm as necessary, without disturbing the meshing architecture of the IoT system. Self-healing systems are another application of IoT. The self-healing property is found in systems that detect and diagnose problems, and thus must embed some form of fault tolerance. Fault-tolerance based on SI implies the generation of alternative transportation paths and the recovery of faulty paths, so that the information is not lost and need not be retransmitted.

3.7.3 IoT Trust Framework

Common IoT threats are presented in [47] together with requirements to make the IoT secure, involving several technological areas. The common thread seems to be the need for end-to-end security.

Trust and usability are very important success factors for IoT, the security and privacy of which need to be addressed across all the IoT architectural layers and across domain applications. Performance, complexity and costs are all factors, which influence adoption in addition to those that engender trust. While important progress has been made and actions have been planned to address usability, there nevertheless remain a number of potential gaps in the overall "trust" framework.

The adoption of fine-grained authorization mechanisms allows for more flexible resource control and enables tolerance when fronting unknown risks. In addition, IP security protocol variants for the IoT with public-key-based cryptographic primitives in their protocol design such as Datagram TLS (DTLS), the HIP Diet EXchange (DEX), and minimal IKEv2, can fulfil the requirements of the IoT regarding scalability and interoperability. End-to-end authentication, integrity confidentiality and privacy are essential.

It is very important for all IoT objects to collaborate with each other and with the environment in order to generate the most appropriate clustering for the task at hand, whether that be optimizing functions, locating and isolating attacked objects, alleviating damage, or healing. Objects' trustworthiness is therefore an important feature, which must involve addressing issues such as security, user access, user credentials/authentication, privacy, disclosure, and transparency. Developing an IoT trust framework addressing security, privacy, and sustainability in IoT products and services, as well as emphasising, "security and privacy by design" as part of IoT product and application

development and deployment, is an important research priority for IoT activities.

It is important to keep in mind that all the technologies must be tailored to the constraints of IoT scenarios and to the characteristics of IoT devices, including limited memory, computing resources, security and backup connectivity.

Block chain technology is useful as a transaction-processing tool that can address trust and security issues and move towards open source and security based on transparency allowing the democratization of trust. This is done by holding a record of every transaction made by every participant and having many participants verify each transaction, providing highly redundant verification and eliminating the need for centralized trust authorities.

3.8 IoT Enabling the Digital Transformation of Industry

IoT refers to an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world. Important IoT application domains span almost all major economic sectors: health, education, agriculture, transportation, manufacturing, electric grids, and many more. Proponents of IoT techniques see a world in which a bridge's structural weaknesses are detected before it collapses, in which intelligent transportation and resilient electrical grids offer pleasant and efficient cities for people to live and work in, and in which IoT-supported e-applications transform medicine, education, and business. The combination of network connectivity, widespread sensor placement, and sophisticated data analysis techniques now enables applications to aggregate and act on large amounts of data generated by IoT devices in homes, public spaces, industry and the natural world. This aggregated data can drive innovation, research, and marketing, as well as optimise the services that generated it. IoT techniques will effect large-scale change in how people live and work. A thing in IoT can be an inanimate object that has been digitised or fitted with digital technology, interconnected machines or even, in the case of health and fitness, people's bodies. Such data can then be used to analyse patterns, to anticipate changes and to alter an object or environment to realise the desired outcome, often autonomously. IoT allows for tailored solutions, both in terms of production and services, in all industry areas. IoT data analytics can enable targeted medical treatment or can determine what the lot-size for certain products should be, effectively enabling the adaptation of production processes as required. In the context

of manufacturing this would enable greater use of customised outcomes rather than trying to predict mass market demand. The IoT can empower people in ways that would otherwise not be possible, for example by enabling independence for people with disabilities and specific needs, in an area such as transport, or helping meet the challenges associated with an ageing society. Those countries that anticipate the challenges while fostering greater use will be best placed to seize the benefits [6].

In order to address the totality of interrelated technologies the IoT technology ecosystem is essential and the enabling technologies will have different roles such as components, products/applications, and support and infrastructure in these ecosystems. The technologies will interact through these roles and impact the IoT technological deployment [35].

IoT ecosystems offer solutions comprising a large system beyond a platform and solve important technical challenges in the different verticals and across verticals. These IoT technology ecosystems are instrumental for the deployment of large pilots and can easily be connected to or build upon the core IoT solutions for different applications in order to expand the system of use and allow new and even unanticipated IoT end uses.

There is a need to adapt research and innovation policies across a broad range of sectors and applications with focus on exchanging the data from and among the things and IoT platforms in an interoperable format. This requires creating systems that cross vertical silos and harvest the data across domains, which unleashes useful IoT applications that are user centric, context aware, and are able to create new services and providing gains from improvements in the base components of IoT, such as optimised wireless communications, data processing, analytics, etc.

Swarm intelligence can inspire the design of new IoT security solutions. In order to render this technology for IoT, it has to be fitted according to the IoT needs and as such more work is needed to understand limitations as well as an effective and interactive way to promote the development of these designs.

In applying the research and innovation, recommendations is important to consider the good practices developed to help policy makers move ahead and promote the positive elements of the IoT while minimising challenges and ensuring broader goals, including the following [6]:

- Evaluate and assess the existing policies and practices to determine that are suitably supportive of the IoT, and do not constitute unintentional barriers to potential IoT benefits.

- Promote the use of global technical standards for the IoT developed by standards setting bodies or industry consortia in order to support the development of an interoperable IoT ecosystem, while stimulating the emergence of new systems, boosting innovation and reinforcing competitiveness.
- As the communication technologies evolve, evaluate spectrum resources to satisfy IoT needs, both current and future, as different elements of the IoT, from machines to edge devices, need a variety of spectrum resources that is fit for purpose.
- Promote skills to maximise opportunities in the labour market and support workers whose tasks become displaced by IoT-enabled and IoT Robotic Things and systems, with adjustment assistance and re-skilling programmes.
- Build trust in the IoT by managing digital security and privacy risks in line with the global and European regulations and practices and by developing a Trust IoT framework based on cross-border and cross-sector interoperability of policy frameworks in the context of DSM.
- Support and further develop open data frameworks that enable the reuse of government data sets and encourage industry to share their non-sensitive data for public benefit.
- Promote and support the development of identity for things to address numbering, discovery, identity and access management. Flexibility is needed for numbering as different services or IoT users may have different requirements.
- Encourage the exploitation of the project results, support the private sector innovation taking advantage of the IoT, and improve the conditions for the creation of start-ups and IoT business models that are built around the opportunities created by the IoT applications and large scale pilots.

Internet of Things Timelines

Table 3.5 Future technological developments

Development	2016–2020	Beyond 2020
Identification Technology	• Identity management • Open framework for the IoT • Soft Identities • Semantics • Privacy awareness	• "Thing/Object DNA" identifier • Context aware identification • Context aware anonymity

IoT Architecture Technology	• Network of networks architectures • IoT reference architecture developments • IoT reference architecture standardization • Adaptive, context based architectures • Self-X properties	• Cognitive architectures • Distributed context, location, and state-aware architectures
IoT Infrastructure	• Cross domain application deployment • Integrated IoT infrastructures • Multi-application infrastructures • Multi provider infrastructures	• Global, general purpose IoT infrastructures • Global discovery mechanism
IoT Applications	• Configurable IoT devices • IoT in farming/water production and tracing • IoT in manufacturing industry • IoT in industrial lifelong service and maintenance • IoT device with strong processing and analytics capabilities • Application capable of handling heterogeneous high capability data collection and processing infrastructures • IoT wearables • IoT in smart cities • IoT and arts	• IoT information open market • Autonomous and Connected Vehicles • Internet of Buildings • Internet of Energy • Internet of Vehicles • Internet of Lighting • Internet of Health • Internet of Robotic Things • Internet of Farming • Internet of Industrial Things • Cognitive Internet • Tactile Internet
Communication Technology	• Wide spectrum and spectrum aware protocols • Ultra-low power chip sets • On chip antennas • Millimetre wave single chips • Ultra-low power single chip radios • Ultra-low power system on chip	• Unified protocol over wide spectrum • Multi-functional reconfigurable chips • Ultra-low power, short range IoT networks

(*Continued*)

Table 3.5 Continued

Development	2016–2020	Beyond 2020
	• Low-power wide-area networks (LPWANs) • Narrowband IoT (NB-IoT)	
Network Technology	• Network context awareness • Self-aware and self-organizing networks • Sensor network location transparency • IPv6-enabled scalability	• Network cognition • Self-learning, self-repairing networks • Ubiquitous IPv6-based IoT deployment
Software and algorithms	• Goal oriented software • Distributed intelligence, problem solving • Things-to-Things collaboration environments • IoT complex data analysis • IoT intelligent data visualization • Hybrid IoT and industrial automation systems • IoT devices over-the-air (OTA) firmware and software updates	• User oriented software • The invisible IoT • Easy-to-deploy IoT SW • Things-to-Humans collaboration • IoT 4 All • User-centric IoT
Hardware	• Smart sensors (bio-chemical) • More sensors and actuators (tiny sensors) • Sensor integration with NFC • Home printable RFID tags	• Nano-technology and new materials
Data and Signal Processing Technology	• Context aware data processing and data responses • Energy, frequency spectrum aware data processing	• Cognitive processing and optimisation
Discovery and Search Engine Technologies	• Automatic route tagging and identification management centres • Semantic discovery of sensors and sensor data	• Cognitive search engines • Autonomous search engines

Power and Energy Storage Technologies	• Energy harvesting (biological, chemical, induction) • Power generation in harsh environments • Energy recycling • Long range wireless power Wireless power • Zero Power Listen-Mode mechanisms	• Biodegradable batteries • Nano-power processing unit
Security, Privacy and Trust Technologies	• User centric context-aware privacy and privacy policies • Privacy aware data processing • Security and privacy profiles selection based on security and privacy needs • Privacy needs automatic evaluation • Context centric security • Homomorphic Encryption • Searchable Encryption • Protection mechanisms for IoT DoS/DdoS attacks	• Self-adaptive security mechanisms and protocols • Self-managed secure IoT • Swarm intelligence • Artificial intelligence • Deep learning security mechanisms
Interoperability	• Optimized and market proof interoperability approaches used • Interoperability under stress as market grows • Cost of interoperability reduced • Several successful certification programmes in place	• Automated self-adaptable and agile interoperability • Plug'n'Play Interoperability
Standardisation	• IoT standardization refinement • M2M standardization as part of IoT standardisation • Standards for cross interoperability with heterogeneous networks • IoT data and information sharing	• Standards for autonomic communication protocols

Table 3.6 Internet of Things research needs

Research Needs	2016–2020	Beyond 2020
Identification Technology	• Convergence of IP and IDs and addressing scheme • Unique ID • Multiple IDs for specific cases • Extend the ID concept (more than ID number) • Electro Magnetic Identification – EMID	• Multi methods – one ID
IoT Architecture	• IoT layered architecture based on use cases from global scale applications, global interoperability, and interconnections of many trillions of things	• New algorithms, architectures, data structures and approaches to machine learning • Pervasive, secure IoT network architectures • Knowledge sharing IoT networks
IoT Infrastructure	• Application domain-independent abstractions and functionality • Cross-domain integration and management • Large-scale deployment of infrastructure • Context-aware adaptation of operation	• Self-management and configuration • Self-healing • Swarm intelligence and adaptation mechanisms
IoT Applications	• IoT information open market • Standardization of APIs • IoT device with strong processing and analytics capabilities • Ad-hoc deployable and configurable networks for industrial use • Mobile IoT applications for IoT industrial operation and service/maintenance • Fully integrated and interacting IoT applications for industrial use	• Building and deployment of public IoT infrastructure with open APIs and underlying business models • Mobile applications with bio-IoT-human interaction • Tactile Internet of Things • Internet of Robotic Things • Virtual reality things • Augmented Things Reality
IoT Platforms and Software Services for IoT	• IoT Platforms • Low-level device control and operations	• Fully autonomous IoT devices

	• IoT data acquisition, transformation and management • IoT application development • IoT Operating Systems • Quality of Information and IoT service reliability • Highly distributed IoT processes • Semi-automatic process analysis and distribution	• Integrated IoT cognitive platforms based on artificial intelligence including device monitoring, management, security, IoT data acquisition, event-driven logic, application programming, visualization, analytics
IoT Architecture Technology	• Code in tags to be executed in the tag or in trusted readers • Global applications • Adaptive coverage • Universal authentication of objects • Graceful recovery of tags following power loss • More memory • Less energy consumption • 3-D real time location/position embedded systems	• Intelligent and collaborative functions • Object intelligence • Context awareness • Cooperative position cyber-physical systems
Communication Technology	• Longer range (higher frequencies – tenths of GHz) • Protocols for interoperability • On chip networks and multi standard RF architectures • Multi-protocol chips • Gateway convergence • Hybrid network technologies convergence • 5G developments • Collision-resistant algorithms • Plug and play tags • Self-repairing tags	• Self-configuring, protocol seamless networks • Wide-area IoT networks
Network Technology	• Grid/Cloud network • Software defined networks • Service based network • Multi authentication • Integrated/universal authentication	• Need based network • Internet of Everything • Robust security based on a combination of ID metrics

(*Continued*)

Table 3.6 Continued

Research Needs	2016–2020	Beyond 2020
	• Brokering of data through market mechanisms • Scalability enablers • IPv6-based networks for smart cities	• Autonomous systems for nonstop information technology service • Global European IPv6-based Internet of Everything

Software and algorithms	• Self-management and control
	• Micro operating systems and IoT operating systems
	• Context aware business event generation
	• Interoperable ontologies of business events
	• Scalable autonomous software
	• Evolving software
	• Self-reusable software
	• Autonomous things:
	  ○ Self-configurable
	  ○ Self-healing
	  ○ Self-management
	• Platform for object intelligence
	• New application programming interfaces
		• Self-generating "molecular" software
		• Context aware software
		• Event stream processing
		• Distributed stream computing platforms (DSCPs)
		• Cognitive application programming interfaces
		• Data structures capable of learning and adapting to unique inbound data requirements over time

Hardware Devices	• Polymer based memory • IoT Processors • Ultra-low power EPROM/FRAM • Molecular sensors • Autonomous circuits • Transparent displays • Interacting tags • Collaborative tags • Zero Power Listen-Mode tags and sensors • Heterogeneous integration • Self-powering sensors • Low cost modular devices • Ultra-low power circuits • Electronic paper • Nano power processing units • Silent Tags • Biodegradable antennae	• Biodegradable circuits • Autonomous "bee" and "ant" type devices • Zero Power tags and sensors

Hardware Systems, Circuits and Architectures	• Multi-protocol front ends • Ultra-low cost chips with security • Collision free air to air protocol • Minimum energy protocols • Multi-band, multi-mode wireless sensor architectures implementations • Adaptive architectures • Reconfigurable wireless systems • Changing and adapting functionalities to the environments • Micro readers with multi standard protocols for reading sensor and actuator data • Distributed memory and processing • Low cost modular devices • Protocols correct by construction • IoT Device Management	• Heterogeneous architectures • "Fluid" systems, continuously changing and adapting
Data and Signal Processing Technology	• Common sensor ontologies (cross domain) • Distributed energy efficient data processing • Autonomous computing • Tera scale computing • Micro servers • Multi-functional gateways	• Cognitive computing Cognitive, software-defined gateways
Discovery and Search Engine Technologies	• Scalable Discovery services for connecting things with services while respecting security, privacy and confidentiality • "Search Engine" for Things • IoT Browser • Multiple identities per object • On demand service discovery/integration • Universal authentication	• Cognitive registries • Global IoT context aware and cognitive registry • Learning algorithms for search and discovery
Power and Energy Storage Technologies	• Paper based batteries • Wireless power everywhere, anytime • Photovoltaic cells everywhere • Energy harvesting • Power generation for harsh environments	• Biodegradable batteries

(*Continued*)

Table 3.6 Continued

Research Needs	2016–2020	Beyond 2020
Interoperability	• Dynamic and adaptable interoperability for technical and semantic areas • Open platform for IoT validation	• Self-adaptable and agile interoperability approaches
Security, Privacy and Trust Technologies	• Low cost, secure and high performance identification/authentication devices • Access control and accounting schemes for IoT • General attack detection and recovery/resilience for IoT • Cyber Security Situation Awareness for IoT • Context based security activation algorithms • Service triggered security • Context-aware devices • Object intelligence • Decentralised self-configuring methods for trust establishment • Novel methods to assess trust in people, devices and data • Location privacy preservation • Personal information protection from inference and observation • Trust Negotiation	• Cognitive security systems • Self-managed secure IoT • Decentralised approaches to privacy by information localisation • Swarm intelligence • Trusted IoT framework
Governance (legal aspects)	• Legal framework for transparency of IoT bodies and organizations • Privacy knowledge base and development privacy standards • Trusted IoT concept and principle • Governance by design	• Adoption of clear European norms/standards regarding Privacy and Security for IoT • Context aware governance
Economic	• Business cases and value chains for IoT • Emergence of IoT in different industrial sectors • Emergence of IoT ecosystems	• Integrated platforms • IoT ecosystems • Emergence of IoT across industrial sectors

Acknowledgments

The IoT European Research Cluster – European Research Cluster on the Internet of Things (IERC) maintains its Strategic Research and Innovation Agenda (SRIA), taking into account its experiences and the results from the on-going exchange among European and international experts.

The present document builds on the 2010, 2011, 2012, 2013, 2014 and 2015 Strategic Research and Innovation Agendas and presents the research fields and an updated roadmap on future R&D from 2016 to 2020 and beyond 2020.

The IoT European Research Cluster SRIA is part of a continuous IoT community dialogue supported by the EC DG Connect – Communications Networks, Content and Technology and international IoT stakeholders. The result is a lively document that is updated every year with expert feedback from on-going and future projects financed by the EC. Many colleagues have assisted over the last few years with their views on the IoT Strategic Research and Innovation agenda document. Their contributions are gratefully acknowledged.

List of Contributors

Abdur Rahim Biswas, IT, CREATE-NET, WAZIUP
Alessandro Bassi, FR, Bassi Consulting, IoT-A, INTER-IoT
Alexander Gluhak, UK, Digital Catapult, UNIFY-IoT
Amados Daffe, SN/KE/US, Coders4Africa, WAZIUP
Antonio Skarmeta, ES, University of Murcia, IoT6
Arkady Zaslavsky, AU, CSIRO, bIoTope
Arne Broering, DE, Siemens, BIG-IoT
Bruno Almeida, PT, UNPARALLEL Innovation, FIESTA-IoT, ARMOUR, WAZIUP
Carlos E. Palau, ES, Universitat Politècnica de Valencia, INTER-IoT
Charalampos Doukas, IT, CREATE-NET, AGILE
Christoph Grimm, DE, University of Kaiserslautern, VICINITY
Claudio Pastrone, IT, ISMB, ebbits, ALMANAC
Congduc Pham, FR, Université de Pau et des Pays de l'Adour, WAZIUP
Elias Tragos, GR, FORTH, RERUM
Eneko Olivares, ES, Universitat Politècnica de Valencia, INTER-IoT
Fabrice Clari, FR, inno TSD, UNIFY-IoT
Franck Le Gall, FR, Easy Global Market, WISE IoT, FIESTA-IoT, FESTIVAL

Frank Boesenberg, DE, Silicon Saxony Management, UNIFY-IoT
François Carrez, UK, University of Surrey, FIESTA-IoT
Friedbert Berens, LU, FB Consulting S.à r.l, BUTLER
Gabriel Marão, BR, Perception, Brazilian IoT Forum
Gert Guri, IT, HIT, UNIFY-IoT
Gianmarco Baldini, IT, EC, JRC
Giovanni Di Orio, PT, UNINOVA, ProaSense, MANTIS
Harald Sundmaeker, DE, ATB GmbH, SmartAgriFood, CuteLoop
Henri Barthel, BE, GS1 Global
Ivana Podnar, HR, University of Zagreb, symbIoTe
JaeSeung Song, KR, Sejong University, WISE IoT
Jan Höller, SE, EAB
Jelena Mitic DE, Siemens, BIG-IoT
Jens-Matthias Bohli, DE, NEC
John Soldatos, GR, Athens Information Technology, FIESTA-IoT
José Amazonas, BR, Universidade de São Paulo, Brazilian IoT Forum
Jose-Antonio, Jimenez Holgado, ES, TID
Jun Li, CN, China Academy of Information and Communications Technology, EU-China Expert Group
Kary Främling, FI, Aalto University, bIoTope
Klaus Moessner, UK, UNIS, IoT.est, iKaaS
Kostas Kalaboukas, GR, SingularLogic, EURIDICE
Latif Ladid, LU, UL, IPv6 Forum
Levent Gürgen, FR, CEA-Leti, FESTIVAL, ClouT
Luis Muñoz, ES, Universidad De Cantabria
Manfred Hauswirth, IE, DERI, OpenIoT, VITAL
Marco Carugi, IT, ITU-T, ZTE
Marilyn Arndt, FR, Orange
Markus Eisenhauer, DE, Fraunhofer-FIT, HYDRA, ebbits
Martin Bauer, DE, NEC, IoT-A
Martin Serrano, IE, DERI, OpenIoT, VITAL, FIESTA-IoT
Martino Maggio, IT, Engineering - Ingegneria Informatica Spa, FESTIVAL, ClouT
Maurizio Spirito, IT, Istituto Superiore Mario Boella, ebbits, ALMANAC, UNIFY-IoT
Maarten Botterman, NL, GNKS, SMART-ACTION
Ousmane Thiare, SN, Université Gaston Berger, WAZIUP
Payam Barnaghi, UK, UNIS, IoT.est

Philippe Cousin, FR, FR, Easy Global Market, WISE IoT, FIESTA-IoT, EU-China Expert Group
Philippe Moretto, FR, ENCADRE, UNIFY-IoT, ESPRESSO, Sat4m2m
Raffaele Giaffreda, IT, CNET, iCore
Roy Bahr, NO, SINTEF, UNIFY-IoT
Sébastien Ziegler, CH, Mandat International, IoT6
Sergio Gusmeroli, IT, Engineering, POLIMI, OSMOSE, BeInCPPS
Sergio Kofuji, BR, Universidade de São Paulo, Brazilian IoT Forum
Sergios Soursos, GR, Intracom SA Telecom Solutions, symbIoTe
Sophie Vallet Chevillard, FR, inno TSD, UNIFY-IoT
Srdjan Krco, RS, DunavNET, IoT-I, SOCIOTAL, TagItSmart
Steffen Lohmann, DE, Fraunhofer IAIS, Be-IoT
Sylvain Kubler, LU, University of Luxembourg, bIoTope
Takuro Yonezawa, JP, Keio University, ClouT
Toyokazu Akiyama, JP, Kyoto Sangyo University, FESTIVAL
Veronica Barchetti, IT, HIT, UNIFY-IoT
Veronica Gutierrez Polidura, ES, Universidad De Cantabria
Xiaohui Yu, CN, China Academy of Information and Communications Technology, EU-China Expert Group

Contributing Projects and Initiatives

IoT6, iCore, EURIDICE, IoT.est, OpenIoT, CuteLoop, BUTLER, IoT-A, SmartAgriFood, EAR-IT, ALMANAC, CITYPULSE, COSMOS, CLOUT, RERUM, SMARTIE, SMART-ACTION, SOCIOTAL, VITAL, WAZIUP, FESTIVAL, BeInCPPS, ESPRESSO, WISE IoT, FIESTA-IoT, iKaaS, ProaSense, MANTIS, ARMOUR, BIG IoT, VICINITY, INTER-IoT, symbIoTe, TAGITSMART, bIoTope, AGILE, Be- IoT, UNIFY-IoT.

List of Abbreviations and Acronyms

Acronym	**Meaning**
3GPP	3rd Generation Partnership Project
AAL	Ambient Assisted Living
AMR	Automatic Meter Reading Technology
API	Application Programming Interface
ARM	Architecture Reference Model
AWARENESS	EU FP7 coordination action Self-Awareness in Autonomic Systems

BACnet	Communications protocol for building automation and control networks
BAN	Body Area Network
BDI	Belief-Desire-Intention architecture or approach
Bluetooth	Proprietary short range open wireless technology standard
BUTLER	EU FP7 research project uBiquitous, secUre inTernet of things with Location and contExt-awaReness
CAGR	Compound annual growth rate
CE	Council of Europe
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Électrotechnique
CEP	Complex Event Processing
DNS	Domain Name System
DoS/DDOS	Denial of service attack Distributed denial of service attack
EC	European Commission
eCall	eCall – eSafety Support A European Commission funded project, coordinated by ERTICO-ITS Europe
EDA	Event Driven Architecture
EH	Energy harvesting
EMF	Electromagnetic Field
ERTICO-ITS	Multi-sector, public/private partnership for intelligent transport systems and services for Europe
ESOs	European Standards Organisations
ESP	Event Stream Processing
ETSI	European Telecommunications Standards Institute
EU	European Union
Exabytes	10^{18} bytes
FI	Future Internet
FI PPP	Future Internet Public Private Partnership programme
FIA	Future Internet Assembly
FIS 2008	Future Internet Symposium 2008

F-ONS	Federated Object Naming Service
FP7	Framework Programme 7
FTP	File Transfer Protocol
GS1	Global Standards Organization
Hadoop	Project developing open-source software for reliable, scalable, distributed computing
HC	Haptic Control
IAB	Internet Architecture Board
IBM	International Business Machines Corporation
ICANN	Internet Corporation for Assigned Name and Numbers
ICT	Information and Communication Technologies
iCore	EU research project Empowering IoT through cognitive technologies
IERC	European Research Cluster for the Internet of Things
IETF	Internet Engineering Task Force
INSPIRE	Infrastructure for Spatial Information in the European Community
IIoT	Industrial Internet of Things
IoB	Internet of Buildings
IoC	Internet of Cities
IoE	Internet of Energy
IoE	Internet of Everything
IoL	Internet of Lighting
IoM	Internet of Media
IoP	Internet of Persons, Internet of People
IoRT	Internet of Robotic Things
IoS	Internet of Services
IoT	Internet of Things
IoT6	EU FP7 research project Universal integration of the Internet of Things through an IPv6-based service oriented architecture enabling heterogeneous components interoperability
IoT-A	Internet of Things Architecture
IoT-est	EU ICT FP7 research project Internet of Things environment for service creation and testing
IoT-I	Internet of Things Initiative
IoV	Internet of Vehicles
IP	Internet Protocol

IPSO Alliance	Organization promoting the Internet Protocol (IP) for Smart Object communications
IPv6	Internet Protocol version 6
ITS	Intelligent Transportation System
KNX	Standardized, OSI-based network communications protocol for intelligent buildings
LOD	Linked Open Data Cloud
LTE	Long Term Evolution
M2M	Machine to Machine
MAC	Media Access Control data communication protocol sub-layer
makeSense	EU FP7 research project on Easy Programming of Integrated Wireless Sensors
MB	Megabyte
MIT	Massachusetts Institute of Technology
MPP	Massively parallel processing
NIEHS	National Institute of Environmental Health Sciences
NFC	Near Field Communication
NoSQL	not only SQL – a broad class of database management systems
OASIS	Organisation for the Advancement of Structured Information Standards
OEM	Original equipment manufacturer
OGC	Open Geospatial Consortium
OMG	Object Management Group
OpenIoT	EU FP7 research project Part of the Future Internet public private partnership Open source blueprint for large scale self-organizing cloud environments for IoT applications
Outsmart	EU project Provisioning of urban/regional smart services and business models enabled by the Future Internet
PAN	Personal Area Network
PET	Privacy Enhancing Technologies
Petabytes	10^{15} byte
PHY	Physical layer of the OSI model
PKI	Public key infrastructure

PPP	Public-private partnership
Probe-IT	EU ICT-FP7 research project Pursuing roadmaps and benchmarks for the Internet of Things
PSI	Public Sector Information
PV	Photo Voltaic
QoI	Quality of Information
RFID	Radio-frequency identification
SASO	IEEE international conferences on Self-Adaptive and Self-Organizing Systems
SDO	Standard Developing Organization
SEAMS	International Symposium on Software Engineering for Adaptive and Self-Managing Systems
SENSEI	EU FP7 research project Integrating the physical with the digital world of the network of the future
SIG	Special Interest Group
SLA	Service-level agreement/Software license agreement
SmartAgriFood	EU ICT FP7 research project Smart Food and Agribusiness: Future Internet for safe and healthy food from farm to fork
SmartSantander	EU ICT FP7 research project Future Internet research and experimentation
SOA	Service Oriented Approach
SON	Self-Organising Networks
SRIA	Strategic Research and Innovation Agenda
SI	Swarm Intelligence
SWE	Sensor Web Enablement
TC	Technical Committee
TI	Tactile Internet
USDL	Unified Service Description Language
UWB	Ultra-wideband
VR	Virtual Reality
W3C	World Wide Web Consortium
WSN	Wireless sensor network
Zettabytes	10^{21} byte
ZigBee	Low-cost, low-power wireless mesh network standard based on IEEE 802.15.4
Z-Wave	Wireless, RF-based communications technology protocol

Bibliography

[1] ISO/IEC JTC 1 – Information technology, Internet of Things (IoT) – Preliminary Report 2014, online at http://www.iso.org/iso/internet_of_things_report-jtc1.pdf
[2] Bluetooth, online at http://www.bluetooth.com
[3] ANT+, online at http://www.thisisant.com/
[4] It's confirmed: Wearables are the "next big thing", online at http://www.cnbc.com/2015/09/22/after-smartphones-wearable-tech-poised-to-be-next-big-thing.html
[5] Digital Economy Collaboration Group (ODEC), online at http://archive.oii.ox.ac.uk/odec/
[6] OECD Digital Economy Paper No 252, June 2016 – The Internet of Things – Seizing the Benefits and Addressing the Challenges, online at http://www.oecd-ilibrary.org/docserver/download/5jlwvzz8td0n.pdf?expires=1466330492&id=id&accname=guest&checksum=266AECBA35AAD3AC3F1BF7CAE3D8C409
[7] Wi-Fi Alliance, online at http://www.wi-fi.org/
[8] Z-Wave alliance, online at http://www.z-wavealliance.org
[9] Accenture. Are you ready to be an Insurer of Things?, online at https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Strategy_7/Accenture-Strategy-Connected-Insurer-of-Things.pdf#zoom=50
[10] KPMG – security and the IoT ecosystem, online at https://www.kpmg.com /BE/en/IssuesAndInsights/ArticlesPublications/Documents/security-and-the-iot-ecosystem.pdf
[11] Is the Internet of Things Too Big to Protect? Not if IoT Applications Are Protected!, online at https://securityintelligence.com/is-the-internet-of-things-too-big-to-protect-not-if-iot-applications-are-protected/
[12] Gartner Says the Worlds of IT and Operational Technology Are Converging, online at http://www.gartner.com/newsroom/id/1590814
[13] Gartner IT Glossary: Operational Technology (OT) http://www.gartner.com/it-glossary/operational-technology-ot
[14] Gartner Inc. 2015. Gartner Hype Cycle, online at http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp
[15] Gartner Inc. 2015. Newsroom. Gartner's 2015 Hype Cycle for Emerging Technologies, online at http://www.gartner.com/newsroom/id/3114217
[16] European Commission, ICT Standardisation Priorities for the Digital Single Market, Communication from the Commission to the European

Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European Commission, 19-4-2016
[17] The Internet of Robotic Things, ABIresearch, AN-1818, online at https://www.abiresearch.com/market-research/product/1019712-the-internet-of-robotic-things/
[18] HART Communication Foundation, online at http://www.hartcomm.org
[19] IETF, online at https://www.ietf.org
[20] EnOcean Wireless Standard, online at http://www.enocean.com
[21] Gartner Identifies the Top 10 Internet of Things Technologies for 2017 and 2018, online at http://www.gartner.com/newsroom/id/3221818
[22] DASH7 Alliance, online at http://www.dash7.org
[23] RuBee, online at http://www.rubee.com/
[24] Botta, A., de Donato, W., Persico, V. and Pescapé, A., "Integration of Cloud computing and Internet of Things: A survey", Future Generation Computer Systems, Volume 56, March 2016, pp. 684–700.
[25] Mell, P. and Grance, T., "The NIST definition of Cloud computing", Natl. Inst. Stand. Technol., 53 (6), 2009, p. 50.
[26] Home Gateway Initiative (HGI), online at www.homegatewayinitiative.org
[27] Internet of Things, Services and People – IoTSP, ABB, online at http://new.abb.com/about/technology/iotsp
[28] Artemis IoE project, online at www.artemis-ioe.eu
[29] Wearables in healthcare, online at http://www.wearable-technologies.com/2015/04/wearables-in-healthcare/
[30] A Look at Smart Clothing for 2015, online at http://www.wearable-technologies.com/2015/03/a-look-at-smartclothing-for-2015/
[31] Best Smart Clothing – A Look at Smart Fabrics 2016, online at http://www.appcessories.co.uk/best-smart-clothing-a-look-at-smart-fabrics/
[32] Brunkhorst C., "Connected cars, autonomous driving, next generation manufacturing – Challenges for Trade Unions", Presentation at IndustriAll auto meeting Toronto Oct. 14^{th} 2015, online at http://www.industriall-union.org/worlds-auto-unions-meet-in-toronto
[33] The Internet of Things in Smart Buildings 2014 to 2020, Memoori report, online at http://www.memoori.com/portfolio/internet-things-smart-buildings-2014-2020/
[34] W. Arden, M. Brillouët, P. Cogez, M. Graef, et al., "More than Moore" White Paper, online at http://www.itrs.net/Links/2010ITRS/IRC-ITRS-MtM-v2%203.pdf

[35] O. Vermesan. The IoT: a concept, a paradigm, and an open global network. *Telit2market International*, Issue 10, February 2015, pp. 120–122, online at http://www.telit2market.com/wp-content/uploads/2015/02/telit 2market_10_15_anniversary_edition.pdf

[36] Market research group Canalys, online at http://www.canalys.com/

[37] Platform INDUSTRIE 4.0 – Recommendations for implementing the strategic initiative INDUSTRIE 4.0, Final report of the Industrie 4.0 Working Group, online at, http://www.acatech.de/fileadmin/user_upload/ Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseite n/Industrie_4.0/Final_report__Industrie_4.0_accessible.pdf, 2013

[38] P. C. Evans and M. Annunziata, Industrial Internet: Pushing the Boundaries of Minds and Machines, General Electric Co., online at http://files.gereports.com/wp-content/uploads/2012/11/ge-industrial-internet-vision-paper.pdf

[39] Cisco, "Securely Integrating the Cyber and Physical Worlds", online at http://www.cisco.com/web/solutions/trends/tech-radar/securing-the-iot.html

[40] H. Bauer, F. Grawert, and S. Schink, Semiconductors for wireless communications: Growth engine of the industry, online at www.mckinsey.com/

[41] ITU-T, Internet of Things Global Standards Initiative, http://www.itu.int/ en/ITU-T/gsi/iot/Pages/default.aspx

[42] International Telecommunication Union – ITU-T Y.2060 - (06/2012) – Next Generation Networks – Frameworks and functional architecture models – Overview of the Internet of things

[43] IEEE-SA – Enabling Consumer Connectivity Through Consensus Building, online at http://standardsinsight.com/ieee_company_detail/consensus-building

[44] Mobile-Edge Computing – Introductory Technical White Paper, 2014, online at https://portal.etsi.org/Portals/0/TBpages/MEC/Docs/Mobile-edge_Computing_-_Introductory_Technical_White_Paper_V1%2018-09-14.pdf

[45] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, et al., "Internet of Things Strategic Research Agenda", Chapter 2 in Internet of Things – Global Technological and Societal Trends, River Publishers, 2011, ISBN 978-87-92329-67-7

[46] O. Vermesan, P. Friess, P. Guillemin, H. Sundmaeker, et al., "Internet of Things Strategic Research and Innovation Agenda", Chapter 2

in Internet of Things – Converging Technologies for Smart Environments and Integrated Ecosystems, River Publishers, 2013, ISBN 978-87-92982-73-5

[47] O. Vermesan, P. Friess, P. Guillemin, H. Sundmaeker, et al. Internet of Things Strategic Research and Innovation Agenda. O. Vermesan and P. Friess, Eds. *Internet of Things Applications – From Research and Innovation to Market Deployment*. Alborg, Denmark: The River Publishers, ISBN: 978-87-93102-94-1, 2014, pp. 7–142.

[48] SmartSantander, EU FP7 project, Future Internet Research and Experimentation, online at http://www.smartsantander.eu/

[49] Introducing Fujisawa SST – A town sustainably evolving through living ideas, Panasonic, online at http://panasonic.net/es/fujisawasst/

[50] H. Grindvoll, O. Vermesan, T. Crosbie, R. Bahr, et al., "A wireless sensor network for intelligent building energy management based on multi communication standards – a case study", ITcon Vol. 17, pg. 43–62, http://www.itcon.org/2012/3

[51] EU Research & Innovation, "Horizon 2020", The Framework Programme for Research and Innovation, online at http://ec.europa.eu/research/horizon2020/index_en.cfm

[52] Digital Agenda for Europe, European Commission, Digital Agenda 2010–2020 for Europe, online at http://ec.europa.eu/information_society/digital-agenda/index_en.htm

[53] Beecham Research Limited. Towards Smart Farming: Agriculture Embracing the IoT Vision, online at http://www.beechamresearch.com/download.aspx?id=40

[54] E. Guizzo. How Google's Self-Driving Car Works. IEEE Spectrum, online at http://spectrum.ieee.org/automaton/robotics/artificial-intelligence/how-google-self-driving-car-works

[55] Smartphone owners are ready for home and car IoT solutions, online at http://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/internet-of-things-global-mobile-consumer-survey-infographic.html

[56] Freescale vision chip makes self-driving cars a bit more ordinary, online at http://www.cnet.com/news/freescale-vision-chip-makes-self-driving-cars-a-bit-more-ordinary/

[57] Mapping Smart City Standards – Based on a data flow model, online at http://www.bsigroup.com/LocalFiles/en-GB/smart-cities/resources/BSI-smart-cities-report-Mapping-Smart-City-Standards-UK-EN.pdf

[58] ISO/IEC JTC 1 – Information technology, Smart cities – Preliminary Report 2014, online at http://www.iso.org/iso/smart_cities_report-jtc1.pdf

[59] Report on Internet of Things Applications, AIOTI WG01, September 2015, online at https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020

[60] Report on Innovation Ecosystems, AIOTI WG02, September 2015, online at https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020

[61] Report on IoT LSP Standard Framework Concepts, AIOTI WG03, September 2015, online at https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020

[62] Report on Policy Issues, AIOTI WG04, September 2015, online at https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020

[63] Report on Smart Living Environment for Ageing Well, AIOTI WG05, September 2015, online at https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020

[64] Report on Smart Farming and Food Safety Internet of Things Applications, AIOTI WG06, September 2015, online at https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020

[65] Report on Wearables, AIOTI WG07, September 2015, online at https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020

[66] Report on Analysis and Recommendations for Smart City Large Scale Pilots, AIOTI WG08, September 2015, online at https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020

[67] Report on Smart Mobility, AIOTI WG09, September 2015, online at https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020

[68] Report on Smart Manufacturing, AIOTI WG11, September 2015, online at https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020

[69] R. E. Hall, "The Vision of A Smart City" presented at the 2nd International Life Extension Technology Workshop Paris, France September 28, 2000, online at http://www.crisismanagement.com.cn/templates/blue/down_list/llzt_zhcs/The%20Vision%20of%20A%20Smart%20City.pdf

[70] Eurostat, Agriculture, forestry and fishery statistics, ISSN 1977-2262, 2013 edition, online at http://ec.europa.eu/eurostat/documents/3930297/5968754/KS-FK-13-001-EN.PDF/ef39caf7-60b9-4ab3-b9dc-3175b15feaa6

[71] The Silver Economy as a Pathway for Growth Insights from the OECD-GCOA Expert Consultation, online at http://www.oecd.org/sti/the-silver-economy-as-a-pathway-to-growth.pdf

[72] Are You Implementing Internet of Things with the Right Database?, online at http://www.datastax.com/2014/06/implementinternet-of-things-with-the-right-database

[73] O. Vermesan, P. Friess, G. Woysch, P. Guillemin, S. Gusmeroli, et al., "Europe's IoT Stategic Research Agenda 2012", Chapter 2 in The Internet of Things 2012 New Horizons, Halifax, UK, 2012, ISBN 978-0-9553707-9-3

[74] Libelium, "50 Sensor Applications for a Smarter World", online at http://www.libelium.com/top_50_iot_sensor_applications_ranking#

[75] BUTLER, FP7 EU project, online at http://www.iot-butler.eu/

[76] Building smart communities, online at http://www.holyroodconnect.com/tag/smart-cities/

[77] Using Big Data to Create Smart Cities, online at http://informationstrategyrsm.wordpress.com/2013/10/12/using-big-data-to-create-smart-cities/

[78] O. Vermesan, et al., "Internet of Energy – Connecting Energy Anywhere Anytime" in Advanced Microsystems for Automotive Applications 2011: Smart Systems for Electric, Safe and Networked Mobility, Springer, Berlin, 2011, ISBN 978-36-42213-80-9

[79] US$1.7bn raised in smart grid, battery and storage and efficiency sectors, online at http://www.metering.com/news/us1-7bn-raised-in-smart-grid-battery-and-storage-and-efficiency-sectors/

[80] M. M. Hassan, B. Song, and E. Huh, "A framework of sensor-cloud integration opportunities and challenges", in *Proceedings of the 3rd International Conference on Ubiquitous Information Management*

and Communication, ICUIMC 2009, Suwon, Korea, January 15–16, pp. 618–626, 2009.
[81] M. Yuriyama and T. Kushida, "Sensor-Cloud Infrastructure – Physical Sensor Management with Virtualized Sensors on Cloud Computing", NBiS 2010: 1–8.
[82] IBM and Samsung bet on Bitcoin Tech to save the Internet of Things, online at https://securityledger.com/2015/01/ibm-and-samsung-bet-on-bitcoin-to-save-iot/
[83] Mobile Edge Computing Will Be Critical For Internet-Of-Things And Distributed Computing, online at http://blogs.forrester.com/dan_bieler/16-06-07-mobile_edge_computing_will_be_critical_for_internet_of_things_and_distributed_computing
[84] Y. Bengio, Y. LeCun, "Scaling learning algorithms towards AI", *Large Scale Kernel Machines*, MIT Press, 2007
[85] Open Geospatial Consortium, Geospatial and location standards, online at http://www.opengeospatial.org.
[86] W3C Semantic Web, online at http://www.w3.org/
[87] European Commission, "Smart Grid Mandate, Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployments", M/490 EN, Brussels, 2011
[88] Global Certification Forum, online at http://www.globalcertificationforum.org
[89] SENSEI, EU FP7 project, online at http://www.sensei-project.eu
[90] IoT-A, EU FP7 project, online at http://www.iot-a.eu
[91] IoT6, EU FP7 project, online at http://www.iot6.eu
[92] IoT@Work, EU FP7 project, online at https://www.iot-at-work.eu/
[93] Federated Object Naming Service, GS1, online at http://www.gs1.org/gsmp/community/working_groups/gsmp#FONS
[94] Ambient Assisted Living Roadmap, AALIANCE