H2020 Work Programme 2016-2017
H202-IoT-02-2016
Duration: 36 months

CROSS FERTILISATION THROUGH ALIGNMENT, SYNCHRONISATION AND EXCHANGES FOR IoT

H2020 – CREATE-IoT Project

Deliverable 01.02

Evolution of IoT FA

Revision: 1.00
Due date: 30-09-2017 (m09)
Actual submission date: 16-10-2017
Lead partner: SINTEF

Dissemination level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Summary					
No and name	**D01.02 Evolution of IoT FA**				
Status	Released	**Due**	m09	**Date**	30-09-2017
Author(s)	O. Vermesan (SINTEF), R. Bahr (SINTEF), J. Valiño Llamazares (ATOS), G. Micheletti (IDC), B. Copigneaux (IDATE), S. Ropert (IDATE), H. Yi (IDATE), T. Suárez (BLU), Eleni Karamichali (NUIG), Mythili Menon (MI), Lucio Scudiero (AS)				
Editor	O. Vermesan (SINTEF)				
DoW	This deliverable summarizes part of the work carried out in task T01.01 (IoT Focus Area coordination and road mapping), and includes roadmap of IoT in Europe presenting next stages of IoT deployment and the evolution of IoT FA. Result of sharing ideas and concepts at European level, and alignment with activities at the national level and similar activities in countries and regions outside Europe. Landscape analysis of IoT large-scale pilots in member States, PPPs, Cluster Book contribution.				
Comments					

Document history			
Rev.	**Date**	**Author**	**Description**
0.00	15-01-2017	SINTEF	Template/Initial version.
0.01	23-01-2017	SINTEF	General information and overall structure.
0.02	08-08-2017	SINTEF	Contents and structure.
0.03	30-08-2017	SINTEF	Work allocation.
0.04	05-09-2017	ATOS, IDATE	Input different Sections.
0.05	14-09-2017	SINTEF, MI, AS, IDC, IDATE	Inputs to Sections 3.2, 3.3, 5 and 6.
0.06	18-09-2017	SINTEF, ATOS, BLU, AS, MI	Inputs to Sections5, 6 and 7.
0.07	26-09-2017	SINTEF	Input Sections 5 6, incl. references.
0.08	27-09-2017	IDATE, SINTEF	Updates/inputs Section 3.1
0.09	12-10-2017	SINTEF	Inputs Section 5.
0.10	16-10-2017	SINTEF	Review comments considered.
1.00	16-10-2017	SINTEF	Final version released.

Disclaimer
The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

The document reflects only the author's views and the EC is not liable for any use that may be made of the information contained therein.

Table of contents

1. EXECUTIVE SUMMARY

Publishable summary

This document is presenting the framework for providing a roadmap of IoT in Europe presenting next stages of IoT deployment and the evolution of IoT FA. The document is the result of sharing ideas and concepts at European level, and alignment with activities at the national level and similar activities in countries and regions outside Europe.

Technology road mapping is a strategic planning approach to identify the actions and funding decisions needed to boost IoT technological development and innovation in different technological sectors across Europe. It is a tool for IoT stakeholders, and governmental policy makers to support and the future IoT technological developments.

The IoT roadmap conveys the main purpose to chart the European IoT overall direction for technology development or usage. The IoT road map aims at supporting the development of new IoT technologies by establishing causal or temporal relations between the technological possibilities and choices and the business objectives thereby highlighting the necessary steps to reach the market with the right IoT research programs and IoT FA strategies at the right time.

The IoT roadmap is an extended look at the future of IoT field composed from the collective knowledge and imagination of the IoT drivers of change in the field. This emphasizes the importance that knowledge and expertise plays in the process, the forward-looking nature of the approach, and its flexibility.

The process of developing the framework for providing a roadmap of development and evolution of IoT FA brings together the various IoT key stakeholders and perspectives from the IERC, IoT-EPI and IoT European Large-Scale Pilots Programme, which have identified the societal and technological challenges that are affecting the overall development of IoT technologies and applications, and the IoT activities in different countries in Europe. The roadmap is acting as reference point for ongoing dialogue and action for the IoT FA and will be an integrated part of the delivery D01.05 IoT landscape and alignment with European IoT Strategic Research and Innovation Agenda (SRIA) planned for m21. The IoT roadmap is designed as a multi-layered time-based representation, bringing together various perspectives into a common high-level landscape that enables both ‘demand’ and ‘supply’ side views to be represented, balancing "market pull" and "technology push".

Non-publishable information

None. This document is public.

2. INTRODUCTION

2.1 Purpose and target group

The aim of IoT FA strategy and coordination plan is to harmonize and correlate the IoT activities of IoT European funded projects and related IoT activities through mapping corresponding developments and consolidate them together with the pilots at IoT-FA level, and include where appropriate results from other relevant activities in various industrial domains.

The document provides the roadmap of IoT in Europe presenting next stages of IoT deployment and the evolution of IoT FA and is the result of sharing ideas and concepts at European level, and alignment with activities at the national level and similar activities in countries and regions outside Europe.

2.2 Contributions of partners

This delivery is one of six deliveries from task T01.01 (IoT Focus Area coordination and road mapping). The description below explains the partner contributions in task T01.01.

SINTEF is the task leader (T01.01) and the deliverable responsible. The work ensured that the IoT roadmap in deliverable D01.02, helps reach a consensus about a set of IoT FA stakeholders' needs and the technologies, policy issues required to satisfy those needs, provides a mechanism to help forecast IoT technology, deployments and policy trends developments, and provides a framework to help plan and coordinate IoT technologies/applications, policy developments in Europe, with a global perspective. Worked for the alignment and synchronisation of the activities with the work of the AIOTI, IoT-EPI and IoT LSPs for developing a sound coherent strategy for open exchanges and collaboration between the various activities of the FA. The activities included the promotion for sharing of conclusions and road mapping with similar activities in countries and regions outside Europe.

ATOS worked on the analysis of relevant activities and stakeholders involved in the IoT, linking their area of work to the business models they are adopting. This information is processed to identify best practices based on research done and ATOS experiences in ongoing and past projects in the IoT domain.

PHILIPS contributed using a broader market assessment, stakeholders interviewing and organizing workshops to come to a validated road mapping in the deliverable D01.02. This are aligned on national, European and regions outside Europe. Both technical and business experts have participated and the work is in full alignment with their AIOTI work.

IDC worked on the creation of a conceptual framework for the collection of pertinent data on IoT activities and additional use cases currently ongoing in those European countries not covered by the present consortium members. A similar activity has been directed at additional IoT initiatives in other mature and emerging markets outside Europe.

IDATE involved in the production of the roadmap in the deliverable D01.02, bringing together the technical and non-technical inputs and directing the edition process, contribute to the roadmap by analysis of the market forces (demand-pull), the technology readiness (technology push), and the future needs in term of scientific research, public policies, and industry activities.

BLU focused on analysing planned start-up, developer and SME involvement, procedures, including publication channel for calls to ensure that the broader IoT community is aware of them and able to participate, selection criteria and process; monitoring mechanisms.

GRAD provided a liaison with the AIOTI vertical WGs, coordinated their contributions to the roadmap (deliverable D01.02) for the wide adoption of IoT in the corresponding sectors, at a European level. GRAD also provided links with the task T02.02 for integrating the methodologies, best practices and business models aspects learnt from the LSPs in the roadmap.

NUIG worked the IoT road mapping in deliverable D01.02. The main contribution is to guide in the direction of semantic interoperability vision and the definition and uptake of semantic methodologies for the IoT, helped on bridging current IoT-EPI projects activity with the LSP, and in general continued building community through the contribution to support IoT focus activities.

MI supported the global road mapping, in the deliverable D01.02, with a focus on international cooperation and standardization. In addition to operating and maintaining a major, federated, IoT testbed in Europe (IoT Lab), it compiled and edited the U4IoT chapter for the Cluster Book and continues to be the primary means of direct communication with the other H2020 CSA, U4IoT.

AS supported the global road mapping activities with a focus on IoT and privacy, hence form the basis of the deliverable D01.02.

2.3 Relations to other activities in the project

The content of this document is providing an overview of societal and technological challenges that are affecting the overall development of IoT technologies and applications. The IoT activities in different countries in Europe, and forming the framework road mapping the evolution of IoT FA in order to foster the take up of IoT in Europe and to enable the emergence of IoT ecosystems supported by open technologies and platforms. This is ensuring an efficient interplay of the various elements of the IoT FA and liaise with relevant initiatives at EU (JTIs, PPPs, FAs, EPIs), Member States and at the international level to create societal and market acceptance of IoT applications. The work behind this document is linked with the work in WP02 for sharing common approaches where corresponding activities are developed and consolidated together with the pilots at IoT FA level, and include results from other relevant activities in the factory of the future, smart city, and intelligent vehicle domains. The sharing ideas and concepts supports the activities in WP03 that focus on developing develop a methodology for exploitation of the combination of ICT and art for stimulating innovation and societal and ethical acceptance.

The overview of the IoT activities at the national level are linked with the work in WP04 for setting up a European IoT Value Chain integration framework as part of the Digital Single Market that fosters links between communities of IoT users and providers, as well as with Member States' initiatives and other related initiatives.

The future societal and technological challenges and the trends addressing security, privacy, trust and engagement are directly connected with the work in WP05 on the development of IoT by providing comprehensive technical and non-technical solutions regarding privacy, security and trust issues to the projects across the IoT FA. This is the base for further development and exploitation of security and privacy mechanisms towards good practices and a potential label (“Trusted IoT”).

The identification of technological challenges sustains the work in WP06, for building pre-normative and standardized IoT ecosystems solutions that provide increased interoperability across different domains ecosystems.

3. SOCIETAL AND TECHNOLOGICAL CHALLENGES

Today the economic and social progress remains uneven and the accelerating environmental degradation and climate change requires new investments and rethinking the strategy of global industrialisation. A number of economic, social, technological, demographic and environmental changes and challenges including deeper globalization, persistent inequalities, demographic diversity and environmental degradation need to be addressed in order to have a balanced sustainable development in the new digital economy. These challenges influence and reinforce each other in different ways and pose enormous pressure to find solutions to tackle them. To meet these challenges, research and innovation is a global strategic priority to meet the growing human and society challenges, with new business models, products and services that make support the economic grow and wellbeing of the citizens. In this context, IoT need to address the societal, technological and business challenges in order to provide solutions for future sustainable development.

3.1 Societal challenges

The purpose of this section is to present the societal challenges at the global level from the perspective of IoT technologies and applications that can support solving many of these challenges in the future.

Figure 1: Societal challenges

Its analysis of 15 global societal challenges provides insights into what is at stake and how these challenges are interdependent and can in a way or another be solved with support from IoT technologies. The overview of societal challenges is presented in Figure 1.

3.1.1 Climate change

The Earth's forest area is being reduced Deforestation is destroying wildlife habitats and decreasing the carbon stocks in the world's forests every year.

Regional trends in air pollution differ. NOx, SO_2, and O_3 emissions are declining in OECD countries, for instance, but are stable or increasing in other parts of the world. POPs are compounds absorbed by microorganisms and plants that then accumulate in wildlife and are associated with a range of adverse human health effects. Ocean waste and the associated mix of chemicals and non-biodegradable components are broadly acknowledged as a serious and increasing threat to the marine environment.

Climate change will worsen the outlook for the availability of critical resources such as food, water and energy. Climate change analysis shows that the severity of existing weather patterns intensifies, with wet areas getting wetter and dry and arid areas becoming more so.

3.1.2 Scarcity of resources and circular economy

Population growth and new consumption patterns associated with growing prosperity will place ever more pressure on natural resources. Coal, gas, and oil will account for more than 80% of global energy output in the next years.

The production of many raw materials of critical importance to a range of industries is highly concentrated geographically. Raw materials classified as critical such as Indium, Magnesium, Niobium, Platinum, Tantalum, Tungsten, Antimony, Beryllium, Cobalt, Fluorspar, Gallium, Germanium, Graphite are concentrated within a single country and can influence the global production of Rare Earth Elements. Global water demand will increase, with the largest demand increases coming from manufacturing, electricity, and domestic use. By 2025, 1.8 billion people will be living in countries or regions with absolute water scarcity, and fully two-thirds of the world population could be facing water stress conditions. Rivalry over access to energy and ever-scarcer natural resources will be a major determinant of geo-political shifts in the world in the coming decade and beyond.

Over the past few years, disruptive technological change and system wide innovation have made it possible to set the premises of an economy that is restorative and regenerative by design – the circular economy. This type of economy looks beyond the current "take, make and dispose" extractive industrial model and aims to redefine products and services to design waste out, while minimising negative impacts. Underpinned by a transition to renewable energy sources, the circular model builds economic, natural and social capital.

IoT is allowing the Circular Economy to develop at a much faster pace than ever. Indeed, the implementation of internet of things (IoT) technologies, with reuse and repurpose in mind, in the design and manufacturing of today's products is key to meet new and unknown challenges such as the scarcity of resources. While the IoT is already present in industries such as transportation, where buses, metros, railways, and aviation are taking advantage of billions of sensors to schedule maintenance, and reduce waste, many other markets are still behind, especially consumer products, and they are ripe for transformation. In fact, the IoT is allowing "anonymous assets" to become "intelligent assets", which can sense, communicate, and store information about themselves. These intelligent assets are already bringing about a first wave of fusion of manufacturing and digital technologies, creating products that can signal any problem, determine when need to be repaired, and schedule their own maintenance. In this respect, relatively inexpensive sensors could be fitted

in everything from dishwashers to coffee makers, and from drills to lawn mowers, and help keeping them in perfect working condition for longer.

A new generation of IoT enabled products could help eliminate waste if those are manufactured to be shared. Apps like Uber and AirBnb could be used to share rarely used equipment and charge a small price per use. For example, a lawn mower could be reserved, located, and rented as needed. That could also be a new business for manufacturers. If a company such as Black & Decker could produce a durable drill, equipped with sensors to charge people per minute of use, as well as indicate when a component needs be replaced. Instead of making millions of drills every year, it could make thousands and collect usage fees. One example of pay per use is electric-cars' batteries. Most manufacturers, including Nissan, Renault, and Tesla, are starting to use a lease per km model. The electric vehicle owner leases the battery from the manufacturer, who charges a rental price per distance travelled or hours used, and the replaces the battery when its performance falls below 80%. Those batteries are then being repurposed to store electricity produced by renewable energy sources, where they can have a much longer operating life. At the end of their life cycle, batteries will be disassembled, and their still good components will be used to make new ones.

Unfortunately, the consumer electronics market is one of the biggest culprits and does not seem to lean towards the circular economy's concept, at least for the time being. Smartphone vendors, for example, are making their products more difficult to repair all the time, and impossible to upgrade. They have moved from removable batteries to fixed ones, and they do not allow memory upgrades on many of their flagship models. They just want power users to replace their smartphones every two years. Still, the trend is set and is very likely to pursue over the next few years with the IoT helping to push for an economy that is restorative and regenerative by design.

3.1.3 Demographic and social changes

Increasing by more than 80 million a year, the global population could grow from 7.4 billion in 2016, reaching 8 billion by 2025. Medium-variant projections by the United Nations Population Division (UNPD) assume that most of this population growth will occur in today's developing countries, particularly in Africa and Asia (excluding Japan) and Latin America.

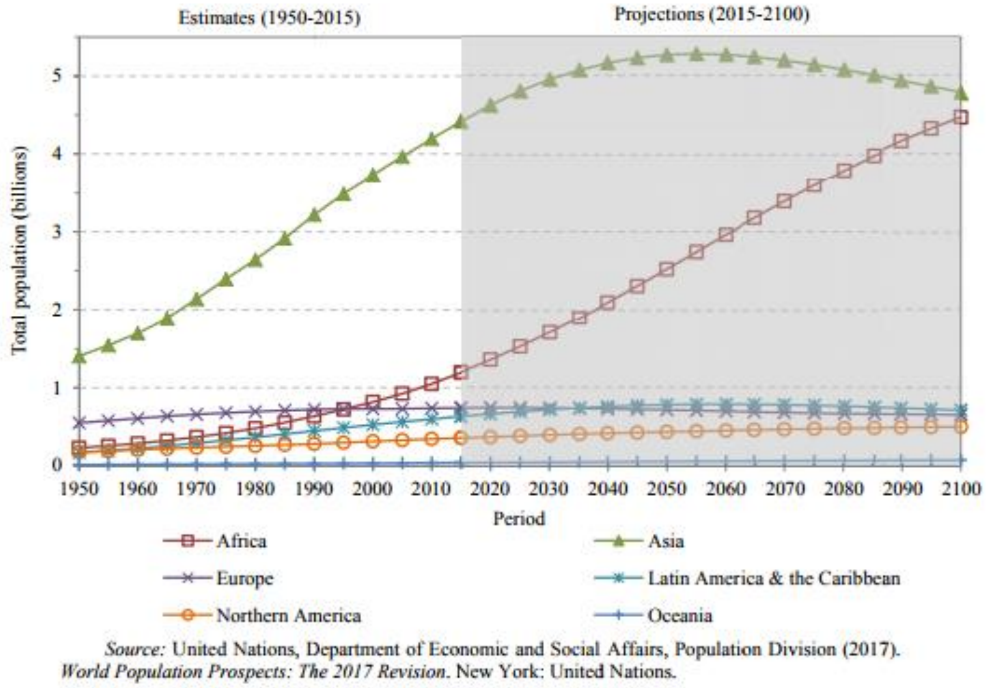

Figure 2: Population by region: estimates, 1950-2015; and medium-variant projection, 2015-2100

Stable growing population imposes significant pressure on natural resources and infrastructure, including energy, food productivity and supplies, and transportation systems. Meanwhile, persistent economic and demographic asymmetries between countries are likely to remain drivers of international migration. Facing this trend, the IoT technologies tend to facilitate cooperation between developed and developing economies, and optimise the resources consumption globally.

Along with the population growth is the changing population age structure. Technology and economic growth enable people to live longer – senior population (> 65) will double during the period of 2015 ~ 2050. Rapid population aging arises many concerns such as workforce shortage, fiscal stress, financial collapse of pension and medical-social systems.

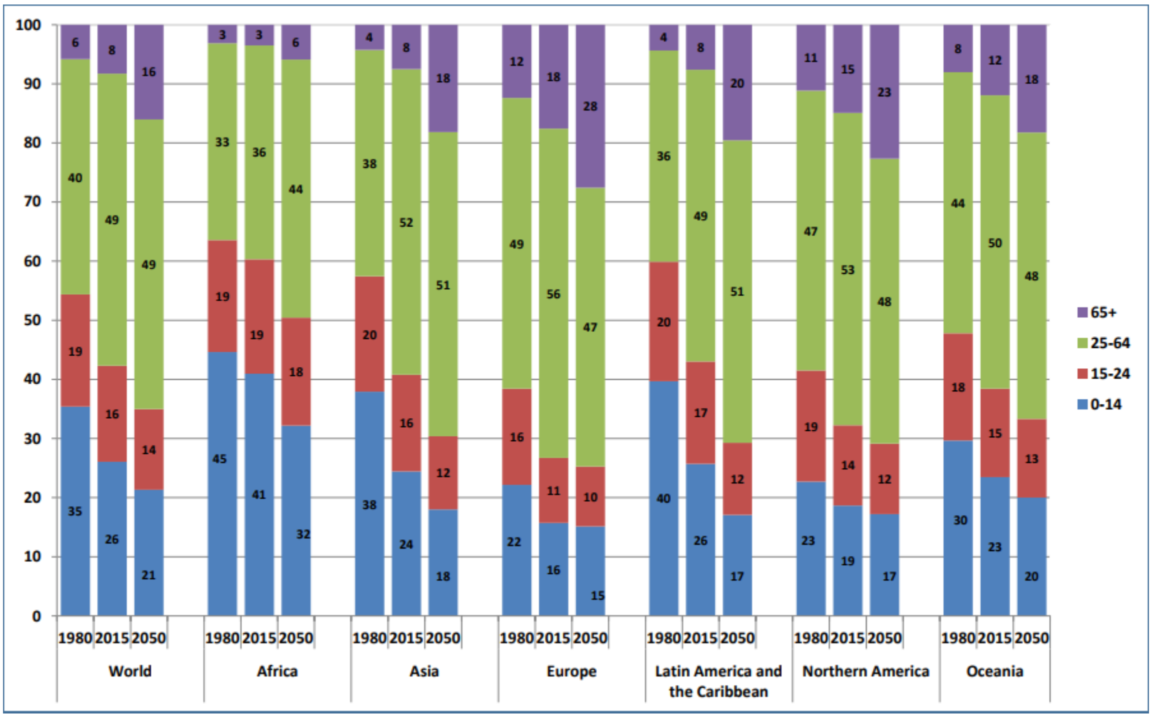

Figure 3: Percentage distribution of the populations of major world regions by broad age group, 1980 -2100

In the meantime, the global working-age population (WAP) is estimated to stay stagnant. The WAP of Europe and North America start declining, contrast to a strong growing of WAP in Africa and Latin America and the Caribbean for the next decades.

The deployment of IoT solutions will play an important role to adapt to aging population, particularly in the healthcare industries. In addition, high level of automation and data intelligence, which is taking place in a wide range of industries (manufacturing, automobile, energy, etc.), tends to be in synergy with labour structure reform, to adapt to labour decline in a foreseeable future.

Urbanisation will continue for the coming decades in every geographic region. By 2030 it is expected that 5 billion people are living in cities, up from, which means that six out of every ten people will be city dwellers.

Urban areas in developing regions will account for most of this growth. Africa is the least urbanized region today, with 40% of its people living in urban area - half the proportion of Latin America and the Caribbean, which is the most urbanized developing region. 50% of Asia's population is projected to be living in urban areas in the next few years.

What accompany urbanisation are not only economic benefits, but also the pressure placed on city resources and infrastructure. In addition to dense use of land, water and electricity, the sheer volume of urban dwellers also put critical requirement on the urban transportation capacity and vehicle exhaust.

The applications like connected cars and intelligent transport system (ITS) will provide many opportunities to coordinate the urban mobility resource in an efficient manner.

Beyond the challenges that demographic changes impose to society, the evolution of social structure creates, nevertheless, amount of opportunities, particularly in developing countries.

It is expected a rise of middle class in developing countries – Brookings estimated that two thirds of middle class will be in Asia. For instance, China has already overtaken the US in 2014 to become the largest economy in purchasing power parity (PPP2) terms.

Figure 4: Estimated middle class population in 2030

In addition, reverse brain drain and women's empowerment are also likely to evoke different opportunities, reflected in the rise of customized applications and innovative technologies. In this context, global socialization, supported by social platforms will change the patterns in networking, digital marketing, and innovative socializing.

3.1.4 Governance gap

The trends show that power becomes more diffuse with a number of various state and non-state actors, as well as subnational actors, such as cities, that play important governance roles.

With the increasing number of players, with different goals and agendas involved to solve major transnational challenges will complicate decision-making.

Discussions forming the international policy agenda have previously been primarily led by national governmental authorities. This is changing as city, state, and provincial governments are forming strategic partnerships with other actors, increasing their ability to influence the international policy debate.

The lack of consensus between and among established and emerging international actors suggests that multilateral governance will be limited and could pave the way toward fragmentation.

The governance gap is expected at the domestic level being driven by dynamic political and social changes. The advances in health, education, and income will drive new governance structures.

3.1.5 Diffusion of power among countries

More than 70% of the global population resides in countries with increasing inequality. This trend is set to continue, and will heighten the potential for social and political instability in many developed countries.

Income inequalities are also expected to persist between rural and urban areas, and between women and men. The accumulated global net public debt is expected to approach or surpass global GDP by 2035. This will put severe constraints on policy options, and affect the capacity of governments to respond to major social, economic, and environmental challenges.

Emerging economies are experiencing economic growth, lifting millions out of poverty while also exerting more influence in the global economy. The rebalancing of global power might lead to the rise of new international system, increasingly shaped by the grouping of nations that are developing more rapidly than others. The emerging markets are expected to be the future economic engines of growth – signalling a potential shift in economic power in the future.

3.1.6 Economical paradigm shift

New disruptive, successful, business organizations emerge as companies bringing together a cluster of people, focused on goals, ideas, innovation and strategy, decide to enter a new market, engineer a new product, or transform a concept into a radical new business model.

These new types of organisations aim for providing the right skills at the right time, for the right purpose, at the most optimal cost and respond to the hierarchical multinational organizational structure that was built over the last 50 years.

Networked organisations evolve to deliver solutions in partnership rather than do everything alone. The model is spread to start-ups, small firm cooperatives, freelance communities and independent workers - adopting new management approaches and business models.

Disruptive innovation and technological change lies at the very core of this new type of organizations and contribute to the emergence of ta new economical paradigm shift – the shift to an IoT-based economy driven by the rise of the digitized internet for communications, new forms of smart energy, and an automated transport and logistics, to mention just three areas where IoT and Connected Objects are producing the most visible impacts.

To be a real paradigm shift, and in order to produce effects on the economy, IoT cannot be seen through the usual lenses of data only. Indeed, the paradigm shift will not occur because of the sheer, huge amount of data generated but because a similarly huge number of sensors will connect an ever-greater number of devices that will be able to “talk to each other” – every machine will be able to interact with every other machine. In other words, at the heart of the IoT is not just the connection of devices or the use of digital technologies but the generation and analysis of data that can be used to derive meaningful intelligence across the business. Connected sensors and devices now provide the potential to generate and access data that businesses could not previously obtain with ease and the cost of these technologies has fallen radically in recent years, allowing for increased connectivity between physical and digital objects in an unprecedented way. Consequently, businesses are now able to respond to changing market conditions with speed and agility and to engage the business and its customers with real-time information that can be turned into actionable insights, thus formulating new delivery models and significantly transforming the way businesses function. The IoT is driving momentum to link digital technologies with product development, operations, organizational processes, and business models, allowing businesses to operate more efficiently and innovatively while reducing costs and increasing customer satisfaction. Through connecting previously unconnected objects and devices, information from across the entire supply chain can be collected and analysed to gain new insights across the business, creating value by combining IoT-generated data with environmental, social, and enterprise data from existing information systems and assets.

Employment of digitization across the economy, and the use of IoT in particular, is likely to drive down many costs of doing business. According to some scholars [5] "By constantly using

analytics, algorithms, and apps, we can dramatically increase our productivity every day" and "reduce our marginal costs to create a very streamlined economy".

Ultimately, the shift is toward empowered consumers, who are increasingly adopting the tools and technologies to guide their own economic destinies. "Now we have three billion people now out on the Internet of Things, and every one of them now are 'prosumers,'" says Rifkin. "That is, everyone at one time or another as has shared video, posted blogs, or have taken massive online college courses. That's all zero marginal costs."

3.1.7 Globalisation, trade, finances and future markets

The global flows of goods, services, finance, and people are rising rapidly - representing over a large percent of global GDP and creating new degrees of connectedness among economies. The degree of interconnection for a city or nation is seen as an important indicator of current and potential prosperity.

The introduction of mobile and online payments that transform mobile devices into credit cards, the trend towards the decline of the use of cash will only accelerate. The development is seen as the drop of payment technology into the vehicles, bicycles, clothing and everything as part of the trend involving IoT and introduction of electronic currencies such as Bitcoin, Litecoin.

These electronic currencies are decentralised, controlled by users rather than the government and transactions are anonymous. Today's credit cards block payments from some countries, while currencies like Bitcoin enable instant payment to anyone from anywhere in the world. By 2025, the electronic transactions will dominate and the cash will remain a backup way of payment.

3.1.8 Global hyperconnected knowledge society

Global hyperconnected knowledge society redefines how individuals, enterprises and governments interconnect, relate and provides new models for innovation, new opportunities for growth and new risks that will have to be managed and mitigated.

The Human Centred Computing (HCC) approach has emerged as novel ICT technologies (from eCommerce, to extended use of Cloud services, Big Data based profiling, Cyber Physical Systems and "Internet of Things") and their use in commercial relationships (from advertising to retail). As a result, these new relationships impact several human fundamental notions: **identity, privacy, relationships, culture, reputation, motivations, responsibility, attention, safety and fairness.**

Regarding the development of the Internet of Things, some of these notions are specifically important to consider:

- **Responsibility:** The rising complexity of IoT systems, the multiple roles of stakeholders and layered approach of hardware / software result in near to impossible attribution of responsibilities in case of failure, error, or denegation of IoT services. This will have stronger and stronger consequences as IoT systems get more complex and more intertwined with Physical devices and even in a far-reaching vision with actual human beings. Difficulty to attribute responsibility raises the double risk of either putting too much constraint on IoT technology producers, and therefore impeding innovation capacity, or to the contrary that the risk entirely reposes on end users.
- **Fairness:** The existing risk of "Digital divide" can be foreseen to be in a near future significantly increased in both scale and impact. The differences in access to ICT technologies, is being reinforced in a knowledge divide, which create the risk of a 2-speed society with a strong divide between those who master and understand ICT technologies and their impact on society and life and those who don't. Additionally, questions of fairness, linked with responsibility, on fairness of automated decisions and algorithms will have to be raised. The intentions, and views of the world of the designer are embedded in every creation, therefore

the fairness of the decisions can always be questioned even for supposedly neutral and machine automated choices

- **Control:** The development of the Internet of Things enables constant monitoring not only of Things but of human beings. This potential constant oversight is having serious impacts on human behaviours, pushing human beings to enforce a self-control of their behaviour. It participate to the transition from "disciplinary societies" (Foucault) to "societies of control" (Deleuze): a new system of domination that can degenerate into a totalitarian system at least as easily as before.

This impacts not only citizen directly but also businesses, large and small, online and offline and the trend is set to increase strongly in the coming years as ICT reach closer and further in the "real" world (IoT), as they gain the ability to generate and handle more knowledge (Data) and to act more and more autonomously.

- **Citizens** are worried about **deterioration of human relationships** (risks of scams, loss of human contacts, privacy concerns…) and of the disruption to several fundamental values (notion of self, reputation, culture, attention and motivation).
- **Businesses** are mostly treating ethical concerns as **business threats** and taking actions mostly to protect themselves but **without concern for the global perspective**.

Policy makers are facing **increased complexity** as **real-time interactions** and rapid technological evolution make policy definition and enforcement difficult. The development and enforcement of **top-down regulation seems insufficient** and indeed inadequate to ensure trust and responsibility in digital life interaction. At the same time, and at least in part due to the new interactions made possible by the digital age, **the expectations in term of inclusiveness, sustainability and respect of human fundamental notions are increasing**.

3.1.9 Shared economy and global shared responsibility

The sharing economy capitalises on the social trend that people no longer want to own an asset and are more interested in its use. The concept of sharing economy is based on organisations that use online platforms to connect distributed groups of individuals and enterprises and enable them to share access to their assets, resources, time and skills on a scale that was not possible before. In this context, the platforms underpinning this new collaborative economy paradigm include all online platforms at the base of the sharing economy, where people can share their goods or find available vehicles/seats/rooms/etc. The most successful examples can be found in the transport sphere such as BlaBlaCar, Uber, Lyft, BlackLane, Drivy, and Koolicar, but also in the accommodation sector (AirBnB), on-demand household services (Deliveroo), on-demand professional services (Upwork, for administrative services) or collaborative financing (SyndicateRoom for equity crowdfunding).

Indeed, according to a recent study by PwC [6], the five-key sector are at the forefront of the sharing economy development in Europe today:

- Peer-to-peer accommodation: households sharing access to unused space in their home or renting out a holiday home to travellers
- Peer-to-peer transportation: individuals sharing a ride, car or parking space with others
- On-demand household services: freelancer marketplaces enabling households to access on-demand support with household tasks such as food delivery and DIY
- On demand professional services: freelancer marketplaces enabling businesses to access on-demand support with skills such as administration, consultancy and accountancy
- Collaborative finance: individuals and businesses who invest, lend and borrow directly between each other, such as crowd-funding and peer-to-peer lending

The study estimates these five key sectors of the collaborative economy to have generated revenues of nearly €4bn and facilitated €28bn of transactions within Europe in 2015 alone and that in the same year an impressive number of 237 collaborative platforms had been founded in Europe.

Today, sharing economy platforms use smartphone and web applications to communicate between the service provider, the platform, and the customer. With the advent of IoT and its further development and deployment, smartphones could communicate directly with devices that help provide the services—without the direct involvement of the device's owners. This kind of automation could make the sharing economy even more efficient and user-friendly.

In the United States this is already becoming a working concept. Companies like GigaOM created a concept for an IoT smart locking device, called "Lock-Bot" which would allow guests to access the key to the unit securely, and return it at the end of their stay—with notifications to the property owner that the transaction had been completed. While the locking device failed to reach its Kickstarter funding goal, it is an indication of the direction the sharing economy is heading in the US but also in Europe.

3.1.10 Dynamic technology and innovation

The technology is entering the cognitive era with process power and data storage almost free, networks and the platforms providing global access and pervasive services, while IoT and cybersecurity creating opportunities in new markets.

The transition to new technologies is a complex process triggered by the interactions among socio-technical landscape, socio-technical regimes, and disruptive innovations. The interactions are accelerated by the learning processes, price/performance increase, and ecosystem support. The new capabilities offered by IoT ecosystems where multiple applications communicate with each other as a network are increasing. By plugging into these IoT ecosystems, stakeholders can get access to entire networks. In this context, in the future there will be a transition from the value chains to value networks.

Digital technology is beginning to catalyse areas in the physical world, i.e. genomics, nanotechnology and robotics, that have an impact on high potential sectors as renewable technology, medical research and logistics. The technology developments are moving from circuits to systems and systems of systems, from applications to architectures and from products and services to platforms.

3.1.11 Production paradigm shift, automatization, robotization

The landscape of the manufacturing is changing dramatically. Manufacturing facilities are measured by their ability to produce with most flexibility. The competitive advantages of real-time data acquisition and the ability to respond in timely and adaptive ways to market demands are driving businesses to adopt more pervasive Internet and Internet of Things-based technologies, and leverage the Internet to drive the Industrial Internet applications.

Information technology-based solutions to maximize citizens' economic productivity and quality of life while minimizing resource consumption and environmental degradation will be critical to ensuring the viability of large cities.

New manufacturing and automation technologies and robotics are changing the work patterns in the developing and developed countries. In developed countries, these technologies are improving productivity, address labour constraints, and reduce the need for outsourcing.

The new technologies could have a similar effect as outsourcing with low- and semi-skilled manufacturing workers in developed economies becoming redundant and increasing domestic inequalities.

For developing economies, the new technologies could stimulate new manufacturing capabilities and further increase the competitiveness of the manufacturers and suppliers from these countries.

3.1.12 Digital transformation

IoT technologies and applications are driving digital transformation through gathering large amount of data, rapid deployment of decisions, predictive maintenance and advanced diagnostics, AI and robotic things used in different applications and domains. The IoT applications are expanding from addressing one industrial sector to develop solutions across sectors.

The industry is undergoing significant digital transformation. Data and artificial intelligence (AI)-based algorithms become important competitive differentiators. Data offers visibility into each prosumer's electricity exports and imports, providing the fundamental basis of the transitive energy market. This data also allows the newly formed distribution service orchestrators to actively manage the dynamic and volatile distribution networks, either through pricing signals or by actively interrupting the power supply.

According to IDC [7], in 2017–2020 digital transformation will emerge at a macroeconomic scale — the dawn of the digital economy —where enterprises will be measured by their ability to achieve and exceed a whole new set of demanding performance benchmarks enabled by cloud, mobility, cognitive/artificial intelligence (AI), the Internet of Things (IoT), augmented reality/virtual reality (AR/VR), and the digital transformations fuelled by these technologies.

With around 85% of FT 500 companies' chief executive officers (CEOs) already putting Digital Transformation at the core of their corporate strategies, it is no surprise that a growing number of CEOs are placing greater interest in what the latest technologies can do for the business, and how they can implement a Digital Transformation strategy that can help them on the path to compete efficiently. Announcements, such as Mars' recent decision to replace the chief information officer (CIO) with a former technology business executive to act as chief digital officer (CDO), only add to the increasing relevance of technology as a key enabler in the transformation journey.

According to IDC's latest Western Europe Digital Transformation Survey (March 2017), 64% of Western European organizations are currently undergoing a formal digital business transformation effort and an additional 25% are about to embark on a transformation journey.

IDC's Digital Transformation model revolves around five key dimensions: Information, Leadership, Omni-Experience, Operating Model, and WorkSource. All these dimensions require careful consideration when undertaking a digital journey, and in all these dimensions, IoT plays a role within and across companies and organizations throughout their digital transformation process. However, the Operating Model dimension, is where IoT's role has been more impactful as of today. This dimension encompasses the ability to make business operations more responsive and effective by leveraging digitally connected products/services, assets, people, and trading partners. This is precisely where IoT initiatives, initial demonstration and practical application can release more value and allow companies and organizations to spend more time and energy on developing new products and services by integrating the business' external digital connections to its markets and suppliers with the internal digital processes and projects that are directly impacted by customer requirements.

3.1.13 Food security

The global demand for food is escalating rapidly. This is driven by population growth, increased wealth, and the resource intensity of food supply. If current food consumption and food waste management practices continue, agricultural output will need to increase by 60% by weight by 2050 relative to 2005.

Climate change's impact on global food security will relate not just to food supply, but also to food quality, food access and utilization, and the stability of food security. Climate change may affect the nutritional properties of some crops. Research has found that under conditions of elevated levels of carbon dioxide, the concentrations of minerals in some crops (e.g. wheat, rice and soybeans) can be up to 8 percent lower than normal. Protein concentrations may also be lower, while carbohydrates are higher. Climate change is also expected to increase the incidence of diseases, particularly water–borne diseases, such as diarrhoea, that contribute to undermining the body's ability to utilize the nutrition in food. Higher temperatures and less rainfall will make clean water less available in many areas, compromising hygiene, and facilitating spread of water-borne pathogens [14].

To safeguard food security, measures for climate change adaptation need to be applied not only to food production, but also to all other stages of the food supply chain. However, as of yet, there has not been sufficient research into the impacts of climate change on food processing, packaging, transport, storage and trade. Adaptation initiatives need to engage multiple sectors and consider a broad range of systemic and transformational options [15].

3.1.14 Health, wellness and wellbeing

The health sector is of course one sector that will be the most heavily affected by these changing demographics. As presented in 3.1.3, senior citizens are estimated to reach 16% of the global population by 2050 – and 28% of the European population – according to United Nations. According to another report by WTO, by 2025 more than 20% of Europeans will be 65 or over, with a particularly rapid increase in numbers of over 80s.

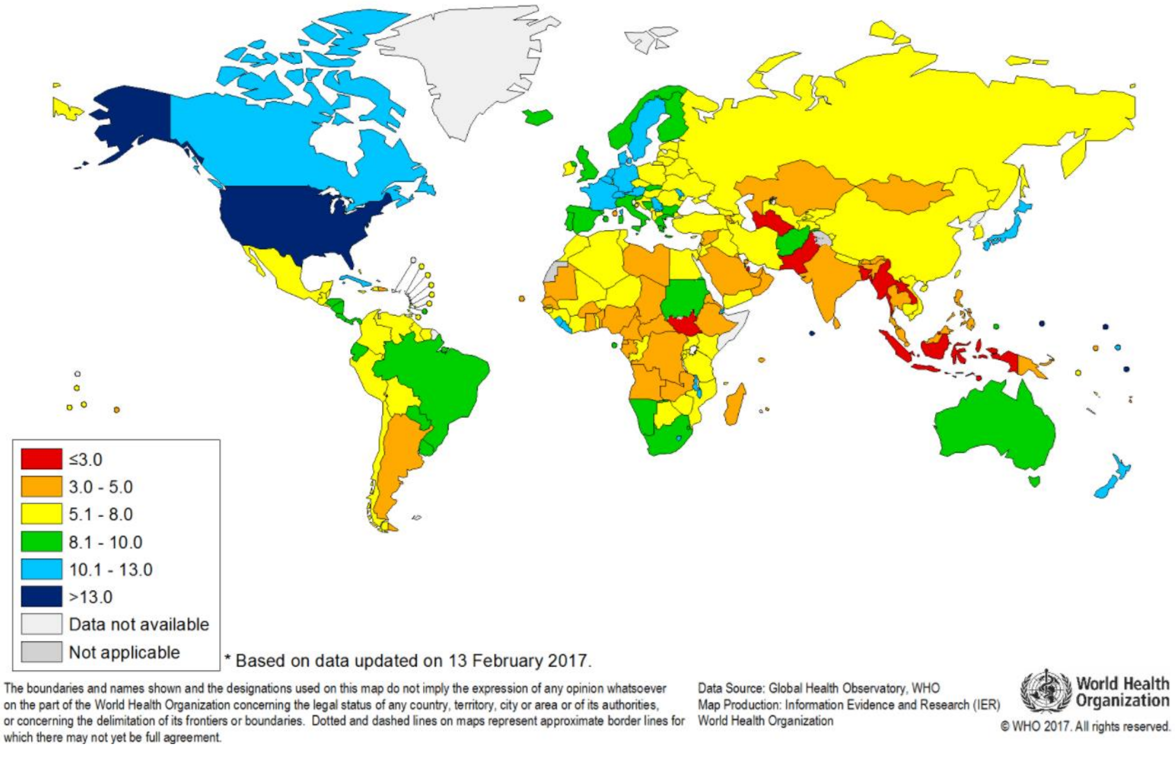

Figure 5: Total expenditure on health as a percentage of the gross domestic product (GDP), WTO, 2014

In addition, there is also a rising incidence of chronic conditions. WHO reported that 300 million people in the North America and Europe have at least one chronic disease. Chronic diseases such as heart disease, stroke, cancer, chronic respiratory diseases and diabetes are by far the leading cause of mortality in Europe, representing 77% of the total disease burden and 86% of all deaths.

The health spending are rising as well. It is generally compromised of health goods and services (i.e. current health expenditure) including personal health care (curative care, rehabilitative care, long-term care, ancillary services and medical goods), and collective services (prevention and public health services as well as health administration).

The global expenditure on health as a percentage of GDP has increased from 8.5% to 9.9% from 1996 to 2014.

The fraction of global GDP spent on healthcare will continue to increase in the coming decades, mainly driven by rising healthcare costs in developed countries, linked to ageing populations, increased patient expectations, a growing burden of disease, sub-optimal allocation of resources, and rising unit costs of care.

Wellness and wellbeing with applications for body, mind and soul offering smarter drugs, virtual hospitals, and cyber documents, the healthcare industry is moving in the direction of disruptive change with knowledge-based and IoT technology embedded in research, development, diagnostics, and monitoring.

IoT-enabled health products and services have a significant economic value, which means potential savings for governments that cover the care costs. Largely represented by informal caregiving and powered by connected sensors, wellness and health monitoring is often conducted by patients themselves. It is expected to reduce overall caregiving costs, with fewer physical visits to hospitals and lower readmission rates.

- The value of informal caregiving in the United States is estimated at 552 billion USD13 for 2014.
- In the UK, the amount of money that informal caregiving saves the government totals close to 2.5 billion GBP a week, according to CarersUK.

Improved care quality and health conditions are another objective in a mid-to-long run, particularly for the fragile and senior population. The connected diagnostic devices, as well as the monitoring services give them the ability to overcome certain deficiencies in daily life (disorientation, hearing loss or diminished eyesight, among other things), while providing a greater sense of safety and security. In addition, the application of AI and analytics to personal health & wellness data paves the way of personalized medicine in a predictive and preventive approach, thus reducing diseases' attack rates.

3.1.15 Security, safety, privacy, trust

Sensors, mobile phones, wearable objects, RFID tags, cameras, middleware components, have a common feature: they are all points of entrance of data, often personal data. As the players of the IoT landscape heavily leverage on personal data to deliver services and increase consumers' welfare, personal data protection and security are key elements in the "value creation chain" of IoT.

In this regard, IoT does not necessarily pose new challenges; it – however – makes traditional challenges escalate and multiply. For example, data subject's control on personal data becomes more difficult due to the dispersed number of data sources and entities processing personal data; as the chain of providers of IoT services stretches, allocation of responsibilities and enforcement of data protection law become more complex than before; and the same can be said with regards to compliance to the principles of purpose limitation and data minimisation. Plus, it is not easy to identify in each case what the viable legal ground for personal data processing is.

The data subject's consent is not always a reliable one; in some cases – especially in the Smart Cities domain – Union or Member State law may constitute the legal basis for personal data processing through IoT deployments.

There is therefore an underlying relation between the need of privacy and the consequential need of trust in the IoT architectures handling our personal data, which renders necessary to make the IoT trustworthy and the data processing operations taking place therein transparent.

The need for privacy can thus be categorized around the following subcategories:

- **Identity Privacy**: The need of privacy for information that can identify a person.
- **Location Privacy**: The need of privacy for information that can identify a person's
- location, since the location is in itself a personal data which can reveal further personal data, e.g. points of interest
- **Footprint Privacy**: The need of privacy for all personal data leaked unintentionally, e.g. preferred language [2]. To these subcategories a further one should be added:
- **Dynamic Privacy**: The need to keep control on the processes of profiling, inferencing and automated decision making started from the collected personal data, which can be further categorized in:
  - **Device Trust**: Need to interact with reliable devices.
  - **Processing Trust**: Need to interact with correct and meaningful data.
  - **Connection Trust**: Requirement to exchange the right data with the right service providers and nobody else
  - **System Trust**: Desire to leverage a dependable overall system. This can be achieved by providing as much transparency of the system as possible [2].

3.2 Technological challenges

Progress in science and technology is driving a range of disruptive developments that are leading to profound societal and business change. The convergence of physical, digital and virtual worlds brings disruption from new conectivity and manufacturing paradigms, advanced interconnected robotics, artificial intelligence, blockchain technology, machine learning, augmented and virtual reality technologies. The present section, lays out eleven key technological challenges that will influence the landscape of IoT technologies and applications in the coming years. The technological challenges depicted by the European IoT research community during the last year are presented in Figure 6.

Figure 6: Technological challenges

3.2.1 Future of Internet connectivity and convergence

Mobile internet usage is growing as the cost of bandwidth declines. The Internet connection are moving in the direction to become permanent, automatic constant and streamlined to the point where no individual "connection" is really necessary. Universal Internet the trend, and overlap between systems establish a layer of redundancy that prevents worries of service outages or bad connections. AR and VR will use the mobile devices to access the Internet in the real world and project the Internet, or embed it, into the real world through a form of augmented reality. Intelligent machines will use the ubiquity of the Internet, to provide services and new experiences and a federation of digital platforms and open architectures.

The future Internet and the Internet of Everything will still have to deal with the challenges pose by privacy, security and trust as the number of services and connections will increase exponentially and behind the various things will be both artificial and natural intelligence.

Businesses and individuals will be challenged to adapt to the increasing rate of change, and machine learning increased computing power and the development of Internet-based technologies will require self-regulating algorithms and complex interrelated systems to regulate in real-time the Internet context-based features.

3.2.2 IoT virtual worlds convergence of physical, augmented and virtual reality technologies

The augmented reality (AR) and virtual reality (VR) technologies are converging with the digital mesh to form IoT seamless systems of devices capable of orchestrating a flow of information that comes to the user as hyper-personalized and relevant apps and services. IoT integration across multiple mobile, wearable, sensor/actuator-embedded environments extend virtual applications beyond single node and single-participant experiences. Environments and spaces become active with cognitive things, and the connection through the mesh appear and work in conjunction with interconnected virtual worlds.

3.2.3 IoT artificial Intelligence, cognitive computing and machine learning

Artificial intelligence, cognitive computing and machine learning include technologies and techniques i.e. deep learning, neural networks, natural-language processing that are increasing the intelligence of IoT applications and move beyond traditional rule-based algorithms to create IoT systems that understand, learn, predict, adapt and operate autonomously. This will increase the IoT intelligent implementations, including physical devices (robots, autonomous vehicles, consumer electronics) as well as apps and services (virtual services, smart virtual devices).

It will also strengthen IoT's role as key enabler of digital transformation innovation accelerators. Its ability to digitize "things" and stream data is opening opportunities for enterprises to offer physical products as digital services and create new digital services that harness and supplement data generated from sensors attached to physical things. In today's digital era, IoT's influence is growing as many more European organizations recognize its ability to transform businesses and industry sectors.

To deliver fully on this promise to be key enabler of digital transformation, IoT analytics requires a more all-encompassing approach, one that moves beyond simply leveraging basic statistical techniques to one that aims to uncover forward-looking and predictive insights from data. Furthermore, by leveraging advanced analytics techniques such as those closely associated with artificial intelligence (AI) and machine learning, analytics systems can autonomously learn from new available data to draw conclusions and optimize recommended actions or forecasts over time. As a matter of fact, advanced analytics disciplines are at the heart of many recent advances in IoT solutions. As an example, IDC predicts [8] that growth in analytics is set to rise rapidly, and by 2020, 100% of effective IoT efforts will be supported by machine learning in some form or other,

while still a nascent discipline and technology area, analytics holds real potential to drive value from IoT by helping organizations leverage insights to improve decisions, and help environments and products get smarter and more intelligent in monitoring, diagnosing problems, and optimizing performance.

3.2.4 IoT co-bots, chatbots and networked business bots

New intelligent things such as robots, drones and autonomous vehicles will evolve to impact a larger segment of the market and support a new phase of digital business becoming intelligent things interconnected into IoT applications and delivering cognitive enabled systems in homes, office, manufacturing floor, healthcare facilities and public spaces.

This is illustrated by the advent of **Virtual Personal Assistants** which offer a **new way to interact with the digital world** through the use of **voice and natural language**. The progresses in speech recognition and more generally natural language processing creates opportunities for better understanding user requests and create new interactions with digital devices.

However, the promise of Virtual Personal Assistant goes beyond being just a new way for end users to interact with their devices (User Interface). They are seen (and marketed) as **intelligent assistants** able not just of understanding but of taking decisions, supporting and potentially replacing human in several tasks. The features of a Virtual Personal Assistant should thus extend beyond being a simple interface and be able to:

- **Follow a conversation**: taking in account other recent questions and queries to answer a query.
- **Be context-aware:** taking in account the context of a query (time, location, etc.) to answer it.
- **Be customized:** taking into account user habits and preferences to answer queries
- **Learn over time:** being able to improve by itself its behaviour and accuracy over time.
- **Be proactive:** being able to proactively make recommendation and send notification to the end user (sending reminders of events or ideas to the user).

In its full extent a Virtual Personal Assistant is thus relying heavily on artificial intelligence to fulfil its intent and can increasingly perform **tasks that are, for now, limited to humans**.

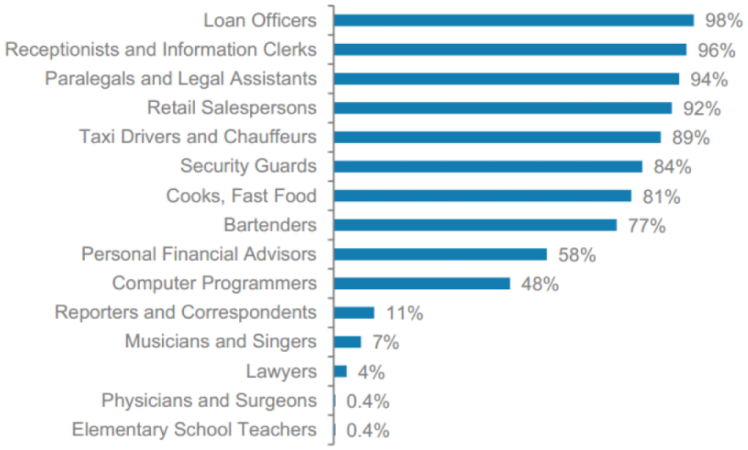

Figure 7: Probability of a job becoming automated in a 20-year timescale (Source: Morgan Stanley).

The long-term vision of the development of VPA is that they will become capable of more and more tasks, being for example able to follow entire professional conversations and seek documents in a company information system related to specific requests. It could profoundly **change the consumer experience** as the customer will be increasingly faced with a software agent instead of a human worker. Combined with progresses in automation and robotics it might even replace completely existing jobs.

VPA are seen as disruptive as they could **replace repetitive human labour** currently depending strongly on natural language understanding such as call centres, information desks and assistants. But thanks to their potential strong knowledge of the end user habits and expectations, they also promise to **offer customized customer care and shopping experiences**.

This development, parallel to the development of the IoT will have important impact in its interaction with the IoT.

The IoT, offering a digital interface, will enable Virtual Agents to get access to more physical devices. This will enable bots to have more and more control on real life interactions, machinery and devices. It will also provide them with the large amount of data that are required by the underlying Deep Learning engines. A good example of this kind of interactions between the IoT and Virtual Agents is the development of autonomous driving.

At the same time, the development of Virtual Agent will offer new interfaces for the IoT, enabling human beings to handle the complexity of the very large amount of data that can be gathered by a fully deployed IoT sensor network. Natural Language interfaces will be of high importance for IoT applications such as Healthcare, Farming or Industrial IoT.

Eventually IoT intelligent things will evolve and shift from a stand-alone to a collaborative model in which intelligent things communicate with one another and act in concert to accomplish collaborative tasks that involves intelligent robotic things such as co-bots, chatbots and networked business bots.

3.2.5 Physical-digital integrations, embedded sensing/actuating

Integrations between the digital and physical world with increasingly detailed reflection of the physical world in the digital and virtual space and the digital world to appear as part of the physical world creating fertile ground for new business models and digitally enabled ecosystems.

Smart products, and services are characterized by intelligent sensing/actuating technology that is integrated with Internet technologies as part of IoT technologies, allowing the products/services to react to and communicate with the dynamic environment around them, leading to optimal operations and improvement in efficiency.

3.2.6 IoT hyper convergence and wireless intelligence

IoT hyper convergence will unify storage, computing, networking, and virtualization and provide wireless intelligence at the edge. The wireless intelligence is expending through the use of Wi-Fi, Bluetooth, Low Power Wi-Fi, Wi-Max, regular Ethernet, Long Term Evolution (LTE), Li-Fi and the new forms of wireless connections, such as 3GPP's narrowband NB-IoT, LoRaWAN, and Sigfox. The wireless intelligence will be embedded in devices based on terahertz waves used larger capacity to carry data that can provide 50 gigabits per second, leading to a new generation of ultra-fast Wi-Fi.

3.2.7 IoT edge computing and edge cloud interactions

The IoT edge computing and cloud services to the edge of the network are pulling the power of the cloud closer to where data is used and stored providing more efficient and reduces data transport. Combined with cognitive computing is increasing the amount of data to improve the learning environment and increase the possibilities of what can be done with edge analytics – making sensors capable of diagnosing and adapting to their environment without the need for human intervention. Cognitive IoT technologies combine multiple data streams that identify patterns and give much more context to the existing environments and applications. IoT autonomous systems, networked automation and internet of robotic things

3.2.8 Blockchain, distributed ledgers digital identities, trusted and adaptive security architecture

Blockchain is **a technological disruption in secured infrastructure**. It is based on a combination of encrypted algorithms and duplicated data storage on a network of computers. Used as a secured infrastructure, **it can meet the strong demand for security coming from a variety of industries.**

From a Technological perspective, Blockchain is a **data storage infrastructure technology**. It makes it possible to store data securely (each entry is authenticated, irreversible and duplicated), with **decentralized control**: there is no central authority that controls the information on the chain. This is achieved through the use of encryption technologies (hash function and asymmetric cryptography) and a computer network of independent nodes.

Blockchain technologies were initially designed to be used with the **Bitcoin cryptocurrency**, where they were employed to create **a reliable ledger** of all of the financial transactions. But Blockchain technology is also developing in ways that are opening up new prospects:

- The use of Blockchains as a **ledger of transactions** (the initial use case)
- The use of Blockchains to **archive and dat**e accurately important pieces of information
- The introduction of **smart contracts**: automated conditional transactions that are executed without human intervention or the involvement of a trusted third party;
- The advent of **decentralized applications**: apps that use the blockchain as their execution infrastructure, without a centralized IT platform.

The information architecture used by Bitcoin technology provides a source for the development, contextualization, exchange, and distributed security of data needed for IoT.

Blockchain for IoT transform the way business transactions are conducted globally through a trustworthy environment to automate and encode business transactions while preserving enterprise level privacy and security for all parties in the transaction. Blockchain solutions are for instance being developed to **identify IoT objects, and to sign automatic and decentralized contracts between connected devices.**

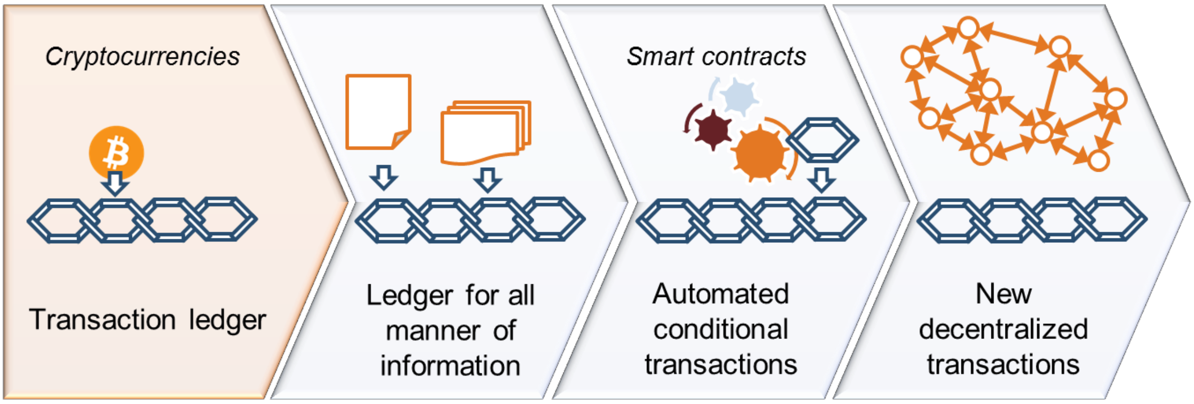

Figure 8: Evolution of the blockchain (Source: IDATE DigiWorld, Blockchain, October 2016).

IoT devices will be used in building blockchain-based solutions to support applications improve operational efficiency, transform the users' experience, and adopt new business models in a secure, private, and decentralized manner, so all participating stakeholders gain value. This is especially the case of Blockchain applications willing **to track and control property**: from asset management applications (IoT device being used to **track asset along the logistic chain**) to radical transformation of business relationship : transition toward world where **any property or object can easily be rented out to another user**, securely and without having to interact directly with the user (The user signs a rental smart contract which, once payment has been made, gives him access to the lock for a set period of time).

3.2.9 IoT digital technology platforms and open architectures

IoT platforms are agents of digital transformation that connect devices, collect data, handle various developers, a multitude of standards and scale to thousand to hundred thousand devices exchanging millions of messages, while offering cognitive, security, privacy, insight generation and close loop automation.

The IoT Platform market represents a new dynamic segment that emerged few years ago, and as in any new markets, the landscape is complex and changing very rapidly. The immaturity of the current IoT platform market is evident due to the sheer number of providers actively offering solutions. However, guidelines for designing IoT architectures are also emerging, to promote interoperability between the various IoT layers and thus overcome the proliferation of incompatible and mission-specific IoT siloes. The IoT platforms implementations across different industry verticals reveal the use of more than 450 IoT platforms that are using Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS) deployments. IoT PaaS platforms are built based on event-based architectures and IoT data and provide data analysis capabilities for processing and managing IoT data. IoT-as-a-Service can be built on these different deployments. All the deployments (i.e. SaaS, PaaS and IaaS) have their challenges and security is one important issue that is connected to identity and access management.

Much of the IoT potential to empower businesses, government, and individuals in their decision making will be revealed in the next few years and be driven by major developments in IoT platforms and advanced analytics. With them, the vast amount of data generated by end-points can be gathered, analysed, and turned into customer value. IoT platforms are evolving rapidly and their architecture is gaining significant sophistication. At a basic level, they essentially connect devices, collect and manage vast amounts of data and expose new insights to enterprises' back-end systems or to third parties. Their ability to support the development of new applications that can underpin better and faster decision-making is crucial.

IoT platforms are the "brain" in an IoT solution that manages all the other important organs, and most importantly creates the value-add. It is the IoT platform that manages the component parts, and takes the data harvested and "does something with it" - i.e., turns data into actionable information. To create information out of reams of data requires the ability to take context into account, pick out the relevant information from vast amounts of data in real-time (such as data pointing to an imminent hardware failure), but also initiate action. The ability to provide business insight by integrating large volumes of data with existing enterprise back-end applications is also a vital function of any IoT platform, as is the ability to support the development of new applications that can underpin better and faster decision-making.

IoT platforms are a means towards achieving the end-game of digital transformation. Connecting things ("the rush to connect" as we have described it) is well underway. What most manufacturers are missing today is an adequate way to analyse and interpret plant floor data in terms of what are the potential impacts and risks for the business. In this context, the value of a scalable, real-time IoT platform that works with traditional systems of record and augments them with sophisticated analytics and machine learning is obvious. It has a tremendous business impact on those manufacturers that have the vision to implement this end to end.

In the manufacturing industry, for example, factories are at the centre of the fulfilment process in many organizations, and this is where satisfaction - or dissatisfaction - starts. Very few manufacturers are able to have full visibility into environment-related metrics, such as energy or water consumption, emissions, and energy costs per unit of product. The challenging and tricky point in this case is the ability to gather, access, spread, and analyse vast amounts of detailed data from the plant floor in real time. And particularly when overall equipment effectiveness (OEE) is extended to an entire plant, or portfolio of plants, gigabytes of information should be collected

each day. IoT platforms answer this need, with the cost of technology needed to collect and analyse gigabytes of information dramatically decreasing. Wireless networks on the plant floor are proven; sensors are low cost, databases cheap, so manufacturing execution systems (MES) are becoming ever more practical and reliable.

A number of barriers need to be addressed before IoT platforms can reach their full potential, chiefly security concerns, lack of industry standards, and RoI:

- Security and privacy are the top obstacles to IoT deployments in Europe. Users lose trust and underrate IoT when they feel their IoT platform is inadequately protecting personal data and privacy. Given the upcoming European General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NIS), IoT platforms that do not demonstrate mature comprehensive attention to data protection and privacy will quickly fall behind the pack.
- A lack of common industry standards is transforming the promising cross-industry vision of "the IoT" into many siloed "intranets of devices" seriously impeding innovation and growth. This barrier exists primarily because the largest, best established IoT companies are in no hurry to standardize.
- The common practice of low dollar value quotes "to get a foot in the door" has made users unconfident as to the amount of infrastructure a company needs to acquire and implement before the full benefits of an IoT solution can be achieved. Vendors' inattention to careful analysis of total cost of ownership for IoT deployments has further reduced user confidence.
- This industry is highly fragmented and dynamic, and subject to much M&A. No single vendor dominates this market, but some large players are rapidly positioning their platforms and striking up partnerships with large tech firms to create smart business solutions. Interestingly, they all have a powerful cloud infrastructure underpinning a PaaS strategy.

IoT platform vendors' success is measured by their business ecosystem and their ability to attract and nurture app developers, SaaS vendors, SIs, and other IT companies to build solutions on top of their platform. Such bottom-up expansion is crucial for their survival. Needless to say that openness is top commandment for such a collaborative model to survive. IoT platforms with strong integration or open programming interfaces have a good chance to thrive in their ecosystem.

3.2.10 IoT business models and ecosystems

New IoT business models are reshaping the landscape of the IoT applications and business environment and there is a move from value chains to value networks and value for many that implies producing and selling to mass markets in developing countries or leveraging the market globally for maximum value delivery.

As IoT deployments move from proof of concepts to genuine production environments, a set of new business models is emerging. These business models reflect the needs and maturity of a company becoming a digital company and as such change the way that IT will engage with IT suppliers. Two of these business models are becoming particularly relevant:

3.2.10.1 IoT Business Model 1.0

Under the IoT Business Model 1.0 scenario, businesses realize that they produce products that get delivered into their supply channel and that is the last that they see or know about them. It is only when there is a fault or a maintenance issue that customers contact the manufacturers or the retailers that sold them the product. Beyond that, businesses have no insights into their customers. This is one of the best and simplest business propositions for an IoT solution. Here, businesses are using IoT sensors to create an asset track and trace (very similar to an RFID implementation back in the late 1990s). The IT requirements are simple and easy to fulfil. They include:

- Preferably running the IoT application on a cloud environment (a cloud environment is preferred but is not a prerequisite, as many of these businesses don't have much in the way of IT skills, and therefore a scalable, relatively inexpensive public cloud solution meets their business needs)
- An IP-based network so that the IoT sensor attached or embedded in the business' products can be enabled and monitored
- A simple or rudimentary analytics platform to generate low-level reporting
- Little or no need for systems integration or service support as these IoT applications are run on a cloud platform for a standalone business unit (There are very few IT suppliers in this business model.)

3.2.10.2 IoT Business Model 2.0

With the IoT Business Model 2.0 scenario, businesses have made commitments to both IoT solutions and a digital transformation strategy. Here, businesses are looking for as much information about their products, customers, suppliers, and competition in real time or near real time. Business outcomes are created from a rich source of internal, external, and IoT-device-based measurements. In this model, IT and the lines of businesses are engaged in a very different way compared with the first IoT business model. Here, the following characteristics have been observed:

- Communication networks play a critical role as sensors need to be connected in a variety of locations where connectivity isn't always available, nor is it always inexpensive.
- A robust cloud infrastructure is a core requirement. The cloud strategy will require the ability to process both private and public data onto a single platform. Data management will become another core requirement, given the variety of data sources that IT will have to ingest and present to an analytics engine.
- Complex analytics and cognitive/machine learning processes are required to seek outcomes that will drive business change.
- Back-end office (or ERP-like) systems must be connected to the analytics platforms to enable a feedback system for all the interested parties (customers, machines, cross-company departments, product suppliers, supply chains, logistics, etc.).
- Management and systems integration partners will be needed to help drive seamless cooperation of business outcomes across the company's complex ecosystem.
- Finally, companies that embark on the IoT Business Model 2.0 are companies that have committed themselves to digital transformation. They see and run every aspect of their business as a service and, as such, expect IT to be fully committed to this too. Running IT as a service requires a very different asset-funding model (both internally and with-IT suppliers) as IT becomes driven by an OPEX model and not CAPEX. Openly sharing business outcomes with any business unit becomes a core value of IT while at the same time maintaining a highly securable data and information environment.

4. IoT in Different Technology Sectors and Across the Sectors

4.1 Agriculture

The multi trillion agricultural industry is in transformation in order to address the high demand for food with an increased supply and integrate technology for providing advancements to increasing food production and efficiency and overcome challenges such as limited land availability, management costs and increased water shortages as the consumption needs are going to grow dramatically in the next few decades.

IoT applications are addressing multiple agricultural needs, leading to more efficient production processes and higher yields.

Even IoT applications and technologies in agricultural-food domain are still fragmentary, lack seamless integration the existing solutions are used for gathering data about planting field conditions for better resource management, use integrated GPS based sensors to provide accurate weather information, which can then be analysed and drones and sensors to accumulate real-time data on crops, livestock and seeds.

The Food and Agriculture Organisation, the United Nations' agency [13] is predicting that by 2050 agricultural production will have to rise by 70% than it did in 2006 in order to feed the growing population of the Earth and to meet projected demand. As most land suitable for farming is already farmed, the growth has to come from higher yields.

Agriculture has undergone yield-enhancing shifts over the years, from use of handheld tools the cotton gin during the Industrial Revolution grain elevators, chemical fertilizers, and the first gas-powered tractor in the 1800s, mechanisation before the second world war and the introduction of new crop varieties and agricultural chemicals in the green revolution of the 1950/1960s and use of satellites for planning and monitoring in the late 1900s.

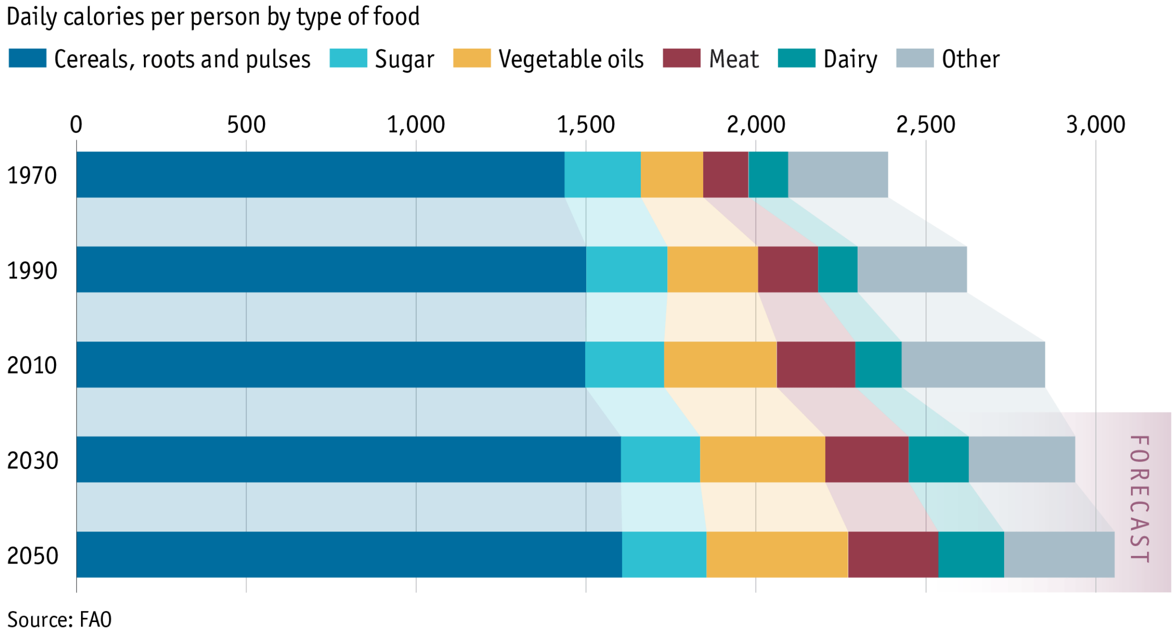

Figure 9: What is on the world's menu (Source: FAO)

The IoT is set to push the future of farming to the next level. Smart agriculture is becoming more commonplace among farmers, and high-tech farming is quickly becoming the standard. The future agricultural sector will rely on IoT for automated data collection, data analysis, AI and machine learning and is poised to improve processes and productivity and cut costs associated with producing food.

The concept of "smart data farming" refers to the utilization of smart data to make more informed farming decisions, which, in turn, bolster production and profit figures. In addition, "precision agriculture" is the technique of closely monitoring the variability in crop yields (within single fields and across multiple fields), and tackling such changes effectively. These two concepts are vital for understanding the essence of smart, information technology-driven farming.

The future of food and agriculture trends and challenges report of FAO [14] shows that there is a need of transformative change in agriculture and food systems worldwide and highlight 10 key challenges that need to be addressed in order to succeed in eradicating hunger and poverty, while making agriculture and food systems sustainable.

Those challenges include the uneven demographic expansion that will take place in the coming decades, the threats posed by climate change, the intensification of natural disasters and upsurges in transboundary pests and diseases, and the need to adjust to major changes taking place in global food systems. In addition, as the global population is escalating (and the demand for food is increasing), the percentage of workforce employed in the agricultural sector is going down.

In this context, smart farming is one of the best possible ways to improve, and maintain, productivity levels.

The report analyses 15 global trends that provide insights into what is at stake and what needs to be done. Most of the trends are strongly interdependent and, combined, inform the set of 10 challenges to achieving food security and nutrition for all and making agriculture sustainable.

The agriculture trends are for next few years are summarized in the following paragraphs.

Global market size of smart farming industry in the next ten years, is expected to have a 4X growth. By 2026, the market is expected to reach a value close to US$ 40 Bn, increasing at a CAGR of 11.2% during the forecast period. The global smart agriculture solution market is forecast to represent incremental $ opportunity of a little more than US$ 25 Bn during the projected period. In terms of basis point share, the hardware sub-segment of the component segment is likely to grab more than half of the share of the global smart agriculture solution market in 2026. By solution, the variable rate technology segment is expected to register a CAGR of 13.4% amongst the other sub-segments in the global smart agriculture solution market [16].

Market key drivers represented by enhanced agricultural productivity are supporting the growth in demand for smart farming, together with factors that are contributing to the need for using high technology in agriculture, such as greenhouse farming practices, smart livestock management, and irrigation management (i.e., preventing wastage of water). Technologies are used to help producing high-quality crops, while minimizing costs and making optimal use of available resources.

Key sensor manufacturers (e.g. Robert Bosch, Lab IX, etc.) are focusing on investing in various small- and medium-sized agricultural solution providers in order to enhance the presence of their offerings in the market.

IoT technologies, including more than 75 million IoT devices will be installed in various applications in agricultural sector by 2020, which represents a rise of 150% from the 30 million figures in 2015.

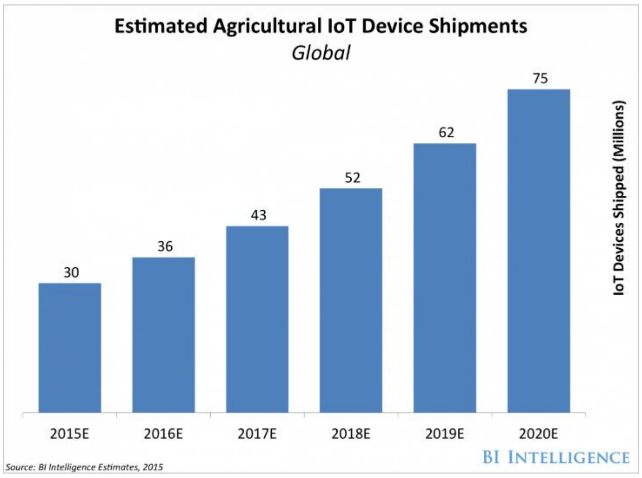

Figure 10: Global estimated agricultural IoT devices shipments (Source: BI Intelligence)

The average volume of big data generated and managed by individual farms show an increase between 2017 (<0.5 million data points) and 2050 (>4.0 million data points). The use of technology is resulting in more agricultural information being generated and processing the data is helping increasing productivity and efficiency.

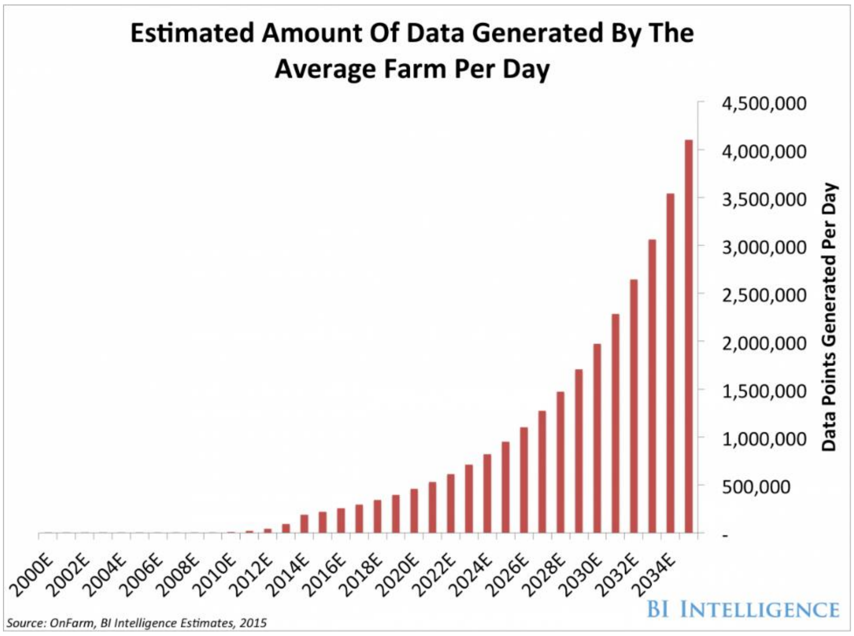

Figure 11: Estimated amount of data generated by average farm per day (Source: BI Intelligence)

The smart farming components and technologies include mobile applications used remotely to track and manage yields, costs and farm metrics, sensing technologies (on-field sensors) , hardware tools and software solutions and smart positioning technologies (GPS), and are the elements that support the development of agricultural sector. . Communication technology (4G/5G other cellular and wireless technologies, LPWANs, are key components of smart farming that are used together with advanced data analytics tools and IoT platforms. Each of these technologies are evolving every quarter – and smart farming as a whole is becoming

Global market leaders are still based in North America, that has $5000 million smart agriculture market and until 2026. By 2026, the North America smart agricultural solution market is expected to reach a value of more than US$ 15 Bn, increasing at a CAGR of 9.8% during the forecast period. Latin America is expected to record a CAGR of 12.3% during the forecast period along with reflecting a Y-o-Y growth rate of 12.1%. The APEJ smart agricultural solution market is forecast

to represent incremental $ opportunity of more than US$ 5,000 Mn between 2016 and 2026, increasing at a CAGR of 13.7% during the forecast period.[16].

Smart water management is an important trend for smart farming as agriculture consumes 70% of the total world's, which goes hand in hand with assuring food security [17]. This trend emphasizes the importance of optimizing irrigation management with technology, and cutting down on wastage of water resources. Smart farming is helping in reducing the total amount of water required (for irrigation) in a farm by as much as 8% [19].

Hardware components are leading smart farming and until 2022, there will be an increase in the use of hardware tools and devices for smart agriculture (e.g. variable rate technology tools, GPS receivers, sensors, smart steering and guidance systems, etc.). The trend is to minimise the inputs/resources, upgradation of quality, and maximise of output through the use of advanced technology. This will fuel the need for standards for automation and control systems to allow economies of scale and further the growth of smart farming.

As the use of high technology in the agricultural sector is growing and its benefits are becoming more and more apparent, investments in this sector are rising investments and several are created between different companies involved in smart agriculture value chain and IoT ecosystems as investing in agricultural technology, can bring potentially big returns.

Autonomous systems, vehicles and drones are useful tools for crop data generation and general surveillance of cultivation lands and several agricultural solution providers companies are including autonomous systems , vehicles and drones in their services for smart farming applications.

Interlink between smart agriculture ecosystems and IoT ecosystems is increasing with farmers, farm managers and technology providers of innovative software applications/mobile apps, IoT sensors/actuator and tracking devices, IoT platforms, communication channels, data analytics tools and other smart equipment creating new value networks of cooperation, collaboration and new business models.

Fish farming is another field that benefits from the deployment of smart IoT technologies such as GPS tools to track the migration of fishes and selecting the best locations for fishing, tracking feeding patterns and detecting probable diseases, information about the water quality and advance analytics using IoT platforms.

The smart agriculture barriers to growth are many ranging from land tenure arrangements, access to credit, farmers' attitudes to risk, the lack of tenurial security, low output prices additional technology expense. The factors depend on farmer and farm household characteristics (i.e., age and gender), farm biophysical characteristics (i.e., farm size and slope), farm financial/management characteristics (i.e., tenure and labour requirement) and price fluctuations and access to extension services. Technology and knowledge gap plays an important role in the adaptation of new solutions. The cost-factor remains an important barrier (setting up the required infrastructure requires significant upfront investment by farm-owners). Data security considering the large investments, and the impact of politics and weather elements on agriculture, are important points of concern. The wireless technologies coverage like broadband and Wi-Fi network in rural areas are not uniform. The use of legacy systems and the compatibility and interoperability of different IoT standards, data ownership and cellular communication standards discourage farmers from investing in smart agricultural applications. Deployments of IoT applications and technologies in smart farming domain are still fragmented, lack seamless integration and advanced solutions are still in an experimental and pilot stage of development. Operational applications are mainly used by early adopters and still focus on basic functionalities at a high granularity level. A large-scale take-up of IoT in agriculture is prevented among others by a lack of interoperability,

user concerns among others about data ownership, privacy and security, and by a lack of appropriate business models that are also suitable for small farms.

4.2 Transportation

The segmentation of the IoT/M2M market is presented in [18] using a semi-circular format, including 9 key service sectors (including transportation), key applications groups within sectors, and examples of connected devices within each sector at the outer edge.

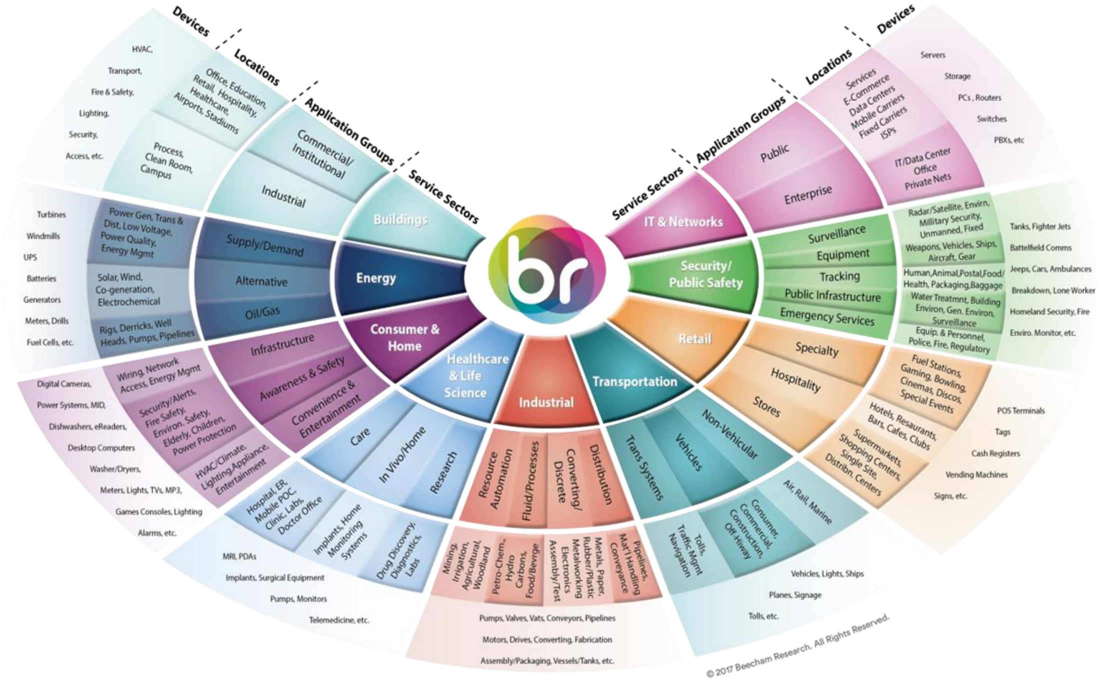

Figure 12: IoT sector map [17]

4.2.1 Aerospace

The deployment of connected objects is transforming the aeronautics industry. This affects the manufacturing process with new tools and services that generate a drop-in production costs. It also enables the development of new business models cantered on a service approach. The European industry has to invest both in technology and skills to sustain its position in a global market.

4.2.1.1 Opportunities of IoT Solutions

The expected impact of digitalization, in the aerospace industry is evaluated to a drop of costs by up to 3.7% per Year and an increase in revenue of up to 2.7% [2].

4.2.1.1.1 The connected factory

The use of IoT technologies in aeronautics manufacturing provides increased labour efficiency by providing contextual information to human workers. Increased connectivity also enables tighter integration of the value chain

Precision manufacturing

Developing an airplane is a complex process and involves myriad thousands of steps which operators must follow, with many checks in place to ensure quality. Contrary to other industries, such as the automotive industry, the use of automation and robotics is low. Most of the assembly

process of an aircraft, as well as a significant part of manufacturing of the component is done by human workers.

The key toward "Smart Factory" in the Aeronautics manufacturing is thus in supporting human workers with digital enhanced tools that increase their productivity.

IoT enhanced tools

By connecting the worker and their tools to an IoT platform, manufacturing accelerates as critical information flows seamlessly across the assembly line.

Airbus is applying the IoT technology not only to its products, but also to the tools its employees use in the manufacturing process. Hence, an Airbus employee on the factory floor who can use a tablet or smart glasses to scan an airplane's metal skin can determine what size bolt is needed in a given hole, and the rotation force necessary to installing it. That information can be spontaneously sent to a robotic tool, which completes the task

The smart factory (internally called 'Factory of the Future') aims to streamline many thousands of steps in the assembly of an airplane – it involves up to 400,000 bolts and screws alone, using 1,100 different tools. The main interest is that with those tools being connected, the process is much quicker and it is even more reliable than if the bolts were being tightened manually.

Location tracking

Another major challenge of the smart factory is to deploy technologies able to keep track of manufacturing equipment locations in real time with precision and across the factory floor and value chain.

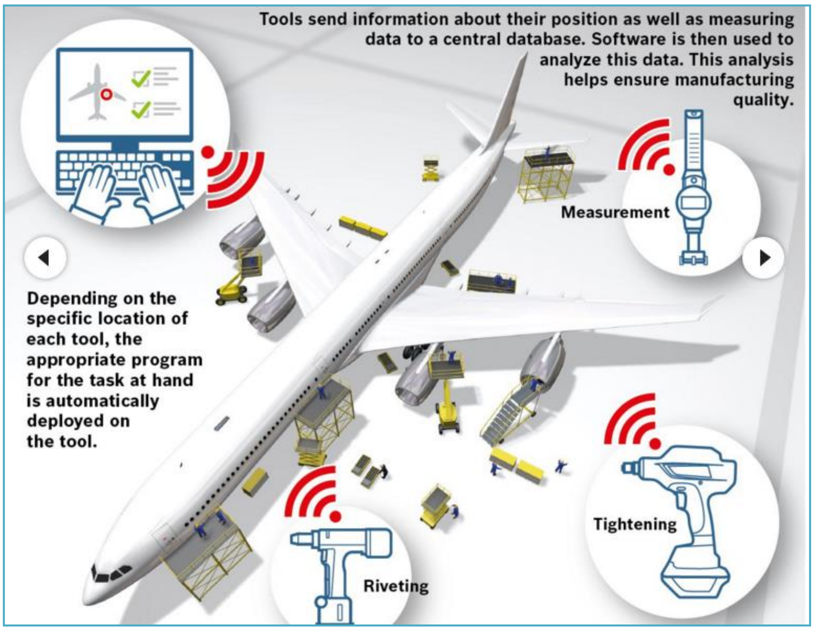

Figure 13: Aircraft manufacturing

The challenge is not only to identify where every tool is on the factory floor but also to keep track of operator usage data and behaviour. This enables increased operator safety and production security (by validating that only authorized and trained employees are using specific equipment). There are tight regulations regarding aircraft construction, requiring constant oversight and regular audits and quality checks.

The use of automated tracking technologies can help reduce the burden of regulation compliance and significantly speed up the manufacturing process while increasing quality. Additionally, one

objective is also eventually to identify optimization opportunities in workflows by applying data analytics to the location data.

The Industrial Internet Consortium (IIC) recently launched the setup of a joint industrial test bed gathering Bosch, Tech Mahindra, Cisco and National Instruments. Aircraft construction is a prime target for such technologies.

4.2.1.1.2 Connected services

The integration of IoT into the aeronautics industry will provide considerable benefits as new services enable optimization of airline operations and asset management.

The new services target the pain point of the industry, from maintenance and fuel cost to optimization of traffic.

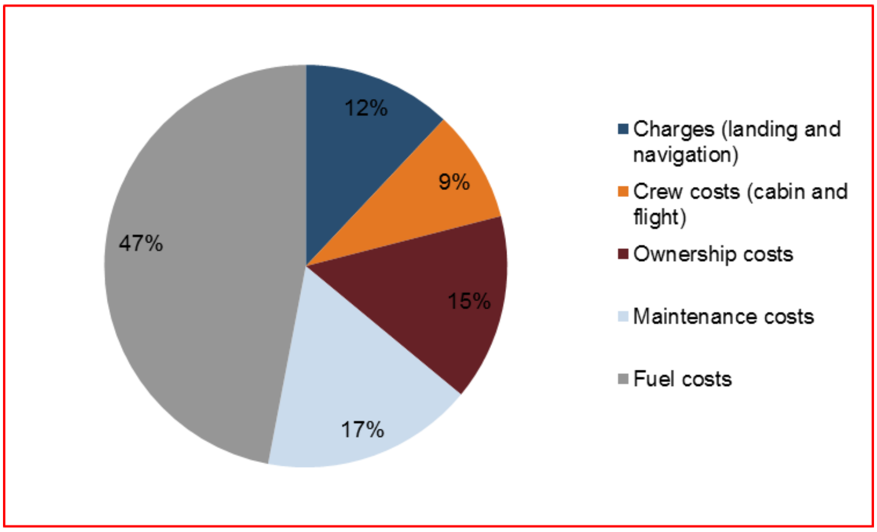

Figure 14: Direct costs of an Airline Company

Preventive maintenance

The development of preventive maintenance services will help reduce aircraft downtime and increase the safety of the industry.

Aircraft on ground (AOG) time is a critical cost factor for the airline industry. It can cause major disruption and damage an airline reputation (The cost of a grounded A380 is evaluated to about 1.25 million USD per Day).

Large numbers of sensors are now deployed in the aircraft. They monitor in real time critical performance parameters and thanks to the IoT, the data can be transmitted in near real time. It helps ground staff to rapidly analyse the data, detect any issue and take corrective action rapidly. It overall reduces both the time and the cost of maintenance.

Increased fuel efficiency

Applied to engine performance, data analytics and predictive maintenance can result into important gains in fuel efficiency.

Pratt & Whitney's Geared Turbo Fan engine is equipped with more than 5000 sensors that constantly monitor key indicators and enable a precise modelisation of the engine behaviour. Data analytics enable the real-time prediction of fuel demand in order to adjust thrusts levels.

This result in reduced fuel consumption by 10-15% as well as environmental benefits through reduced emissions and engine noise.

Optimization services

Connected objects enable the development of entirely new lines of services dedicated to using the data collected to optimize airline operations.

GE Aviation and Accenture have formed a joint venture company called Taleris[7], to provide airlines around the world with intelligent operations services. The objective is to predict, prevent and recover from operational disruptions. This platform allows GE to provide a new business line, centred on the aircraft fleet optimization service.

4.2.1.2 Key challenges

To take advantage of the digital transformation, actors have to rapidly adapt their organization to new practices and develop new skills.

Accordingly, companies need to invest consequently in new technologies but also to consider several critical questions about the adaptation of their organization to this phenomenal change.

4.2.1.2.1 New skills and organization required

To support their transformation, the companies of the aerospace industry need to rapidly develop the qualification of their employees in software and data sciences.

The lack of qualified employees is named as Number One concern, in a 2016 survey of BCG of the manufacturing industry.

They also need to consider evolutions toward services in their business models, and how it will impact their organization. More focus on customer care, the set-up of new service offerings, continuous improvements and lasting relationships.

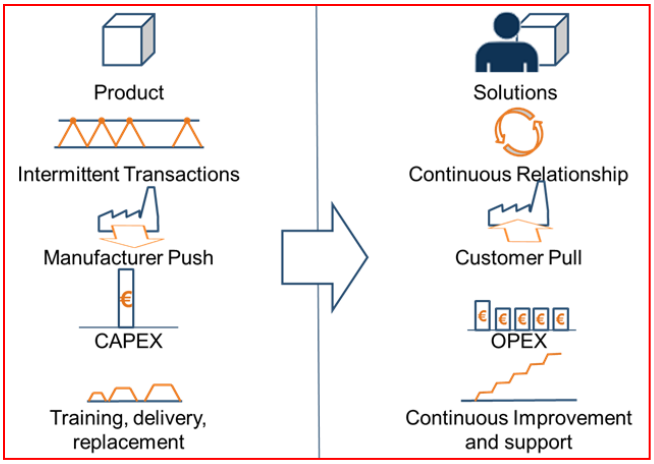

Figure 15: Effects of servicization on customer relationships

Finally, to fully take advantage of the transformation, the industry needs to develop mechanisms ensuring that every actor in the supply chain, including SMEs, are integrated in the process.

4.2.1.2.2 Investing to sustain productivity

The potential benefits of connected objects and industry 4.0 are well understood by the industry leaders.

However, the capacity to invest in time in new technologies and adapt to changing production needs remain critical for the European industry to remain competitive in a globalized economy. A dedicated and voluntary approach is needed.

There is a high aversion to risk and a global attitude of caution in regard to ICT technologies in the industry. They are often considered as potential hazards in terms of security and with high upfront costs and deployment times. Supporting, initiatives that promote both investment in technology but also changes in business practices can have an important structuring role.

4.2.2 Automotive

The automotive industry is going through a disruptive change with huge volumes of data being generated by the connected vehicle technology. With vehicles that are increasingly intelligent the vehicles manufactures are changing their business models and the concept of mobility to consumer-driven preferences that extend beyond the vehicle itself.

4.2.2.1 State of the Art

Urban mobility and the role of the automobile are undergoing a profound change. This transformation is driven by changing attitudes toward car ownership, new and disruptive models of mobility, increased focus on the environmental impacts of driving and congestion, and a rising concern over the impact on quality of life related to how residents, workers, and tourists move. While car sharing has already altered urban mobility, the advent of semiautonomous and autonomous vehicles in the next decade will have an even more dramatic impact. However, the road map to adoption and implementation is far from straightforward.

Today's car has an average of 60-100 sensors that cover everything from engine operation, braking, safety, and emissions to climate within the car cabin. The number of sensors is expected to increase to as many as 200 per car by 2020, as sensors are added to capture how the vehicle interacts with its environment. The technology that will have the greatest impact on the intersection of connected cars and Smart Cities is vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. V2V applications include driving safety, accident avoidance, and optimizing the overall flow of traffic. V2I applications include automatic road toll systems, traffic signal interaction, road condition warning, and parking assistance. The possibilities for V2I applications will continue to grow, but will be limited by the cost of upgrading infrastructure to support new applications.

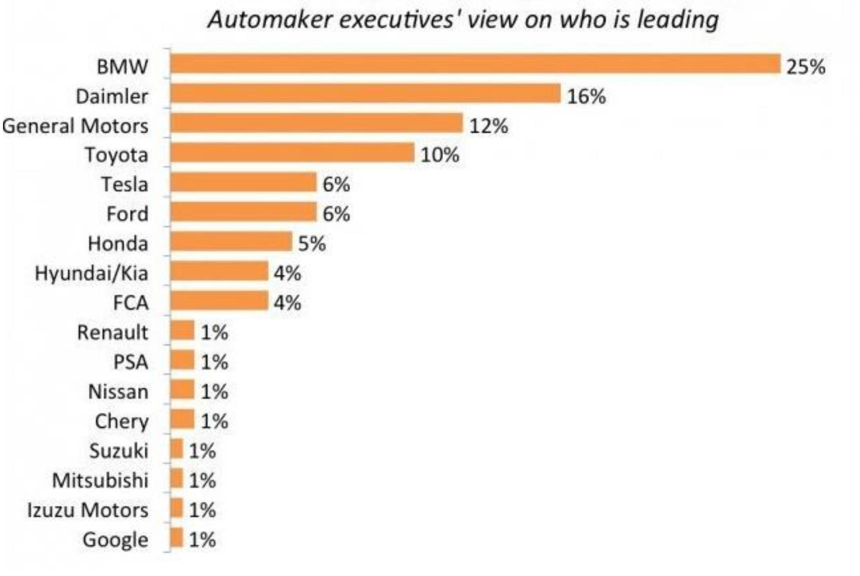

Figure 16: Global OEM leading connectivity and self-driving cars (Source: KPMG, 2016)

The connected car ecosystem is complex and involves a myriad of players, as Figure 17 shows. The connected car evolution has been ongoing for more than a decade, as automakers increasingly

leverage software and Internet connectivity to automate, enhance, and adapt vehicle systems to improve safety and operations.

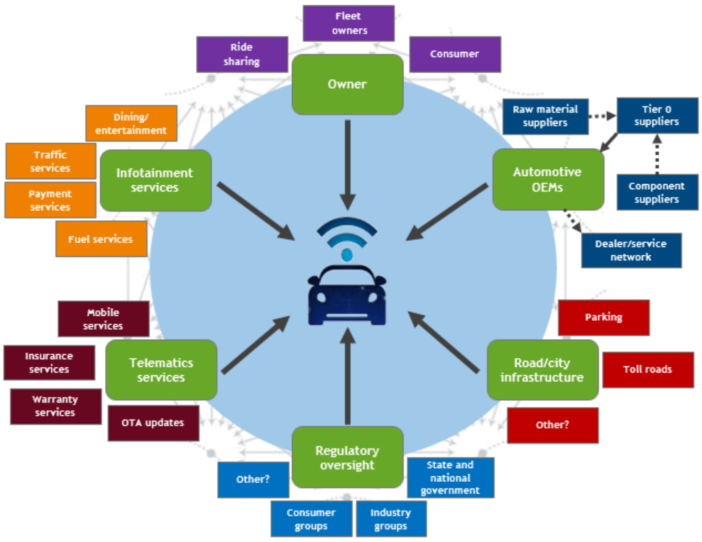

Figure 17: Connected car ecosystem (Source: IDC, 2017)

With the rise of the connected car (and hyperconnected residents), Smart Cities are even more focused on using connected devices and software to create smart streets, which provide safer, multimode roads and reduce urban congestion.

According to IDC estimates, by 2020, Connected Vehicles will generate 30% of Worldwide 5G Data Traffic and 75% of cars shipped globally will have the hardware, software, and IP connectivity that makes a car connected, and that will amount to more than 250 million connected cars on the road. As connected cars become the most common type of consumer vehicle on the road, their opportunity to interact with the infrastructure of cities and society grows exponentially.

4.2.2.2 Challenges and Inhibitors

Future automotive developments across industry are facing a number of challenges and inhibitors as presented below:

- Lack of standards and integration - As the technology infrastructure for Smart Cities evolves in parallel with the technology for connected cars, there is a risk that there may be a divergence of different standards and initiatives that best serve the purposes of each party. This could significantly delay the opportunities previously outlined as well as slow the overall progression of connected car adoption and interaction with city infrastructure.
- Finding the right operating model - Given the nascent state of the market for many of the connected car services, there is still a considerable amount of uncertainty around how to monetize many of the service opportunities. Automotive OEMs may be on the opposite side of the table from Smart City planners in terms of who is able to gain monetarily from sharing data and providing services like connected parking.
- Ongoing security and data privacy concerns - Overlaying the entire connected car and Smart City ecosystem with Internet-connectivity that links all vehicles and infrastructure into a network holds promise for a plethora of value-add, but it also opens up very real and very significant concerns about security. The well-documented potential for connected car hacking as well as dangers within the city of hacking into the network are persistent threats to the success of both connected car and Smart Cities. Further, data sharing of user driving patterns and behaviour will provide a level of reluctance by drivers that may not want their driving to be monitored

- Lagging policies and legal frameworks - More often than not, state and municipal policies lag behind innovation, as we have witnessed with reactions to Uber, Lyft, and other transportation newcomers. Potential new services may need to be supported by new policies or regulation in order to be adopted. An example of this is platooning. While an interesting ecoservice to highway drivers, technically, this would be considered dangerous driving and tailgating. To allow this service, changes must be made in policies. Parking policies are also key in many aspects of urban transportation; OEMs must be aware if there are strategic changes to parking regulations for new developments, which may nudge behaviour toward lower vehicle ownership and increase adoption of shared car-leasing or other car-sharing options. IDC estimates that by 2018, 10% of Global Central and Regional Governments will begin to enact legislation for semiautonomous and autonomous services like Platooning, Eco-Driving, and Driverless Vehicles.
- Differences in customer segmentations - Automotive OEMs and city leaders are trying to meet the needs of a common customer, but the city must also deal with many other customers; of particular concern are those who may be left out of opportunities because they lack access to that latest technologies such as smartphones or premium connected car services. Cities are also trying to balance the needs for many types of urban transportation beyond vehicular, from bike lanes to walking streets. This means that their investment dollars are stretched beyond just the areas of interest to connected cars.

4.2.2.3 Requirements for future development

In this context, the requirements for future developments are expected to be as listed below:

- Automotive OEMs and Smart City leaders will need to work closely to ensure the continued development of and support for connected car capabilities and services such as vehicle-to-vehicle and vehicle-to infrastructure communications that will increasingly include autonomous operations.
- Accelerate the pace of change via agreements while waiting for government mandates – The more quickly both sides can reach agreement about the scope and extent of standards and legislation for connected car operation within cities, the better. An example of this working well is the recently announced safety standards to which most automakers have. An important aspect of this agreement is that it is not a government mandate but rather the result of collaboration between automakers and government that will yield results faster than formal rules would.
- Make automotive OEMs the leaders in bringing stakeholders to the table - Following the strategy used by BMW, automotive OEMs should use their considerable resources to target key cities for best practice pilots and implementations and begin by bringing in key community and city stakeholders to strategy sessions. This would include city leaders for relevant departments, academics, non-profits, foundations, and private sector IT partners to discuss urban mobility strategies and identify key areas for coordination and advocacy. The end result would also be a deeper understanding of high-level strategies, from infrastructure development and parking policies on the part of cities to OEM investment and product road maps for EV, autonomous vehicles, and car-sharing services
- Forge creative efforts for funding and investment of initiatives - Leverage funds from industry groups on the automotive OEM side, alongside government entities to drive collaborative initiatives. Automotive OEMs have a particular incentive here to remain competitive and avoid displacement by transportation disruptors. In addition, technology providers that are integral to providing the IT infrastructure for smart street and connected car interaction have an opportunity to contribute at the pilot stage to further advance efforts
- Watch the cities with robust open data platforms and open data APIs - While many aspects of V2V and V2I require an ability to communicate in absolute real time without any latency in

data transmission, other value-added services that can be provided in the vehicle dashboard or via a smartphone may rely more and more on developments in open data from cities. Automotive OEMs should follow these developments carefully not only for the data provided but for the start-ups that are capitalizing on the data and for new models in government that are combining private and public-sector data into one platform.

4.2.3 Rail

The rail transport is facing major challenges, and must meet the needs for greater mobility and provide a valid alternative to other modes of transport [88]. The aim of the EU commission is to promote an efficient, safe, secure and environmentally friendly mobility and to create the conditions for a competitive industry. [89].

EUs initiative Shift2Rail contributes to smart and sustainable growth by supporting research and innovation in the railway sector [90].

The purpose is to achieve a Single European Railway Area (SERA), to enhance the attractiveness and the competitiveness of the European railway system to ensure a modal shift from roads towards a more sustainable mode of transport such as rail.

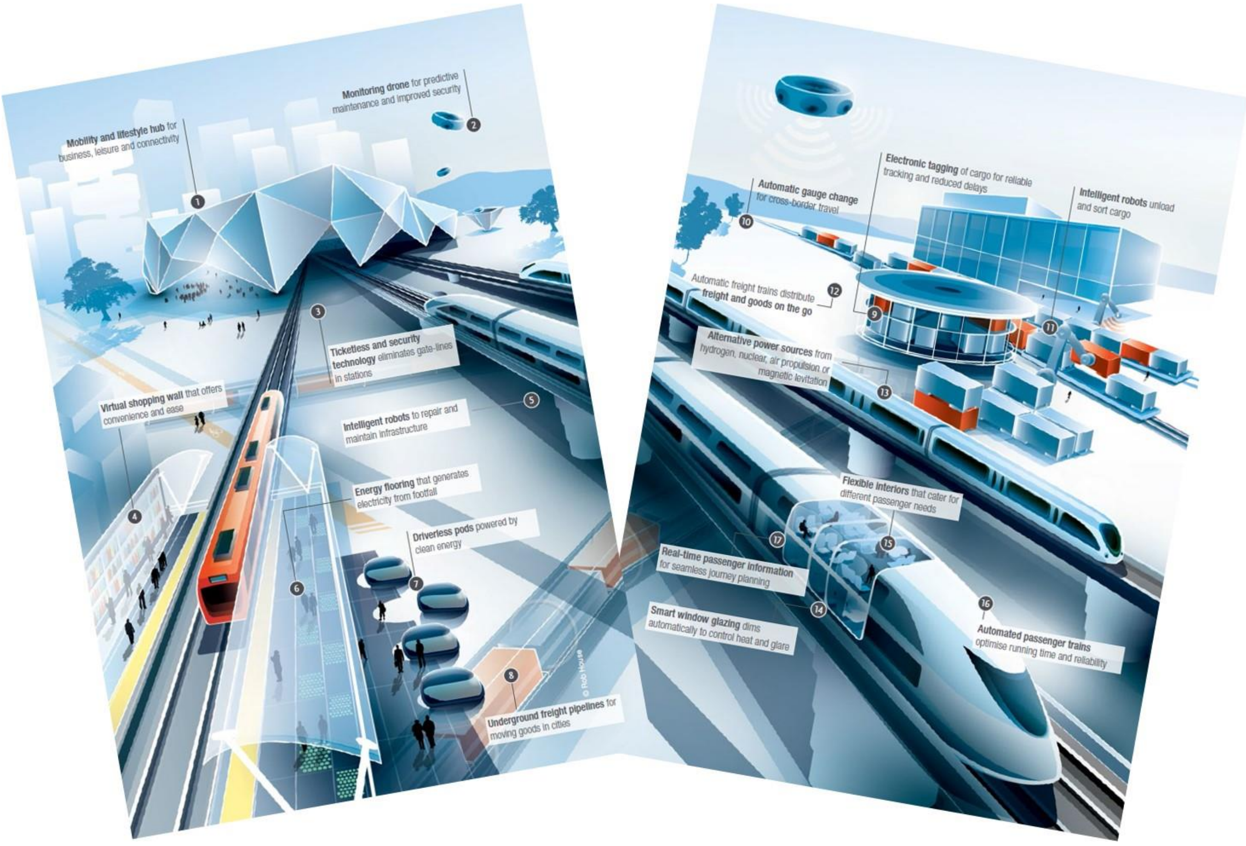

Figure 18: Rail oriented trends, (source: ARUP [91])

Separate accounting for railway infrastructure and the operation of rail services, and opening up national freight and passenger markets to cross-border competition is a major step towards the creation of an integrated European railway area and of a genuine internal market for rail [88].

Greater technical harmonisation of rail systems and the development of key cross-border rail routes are helping to break down barriers to a more competitive rail sector.

The European Railway Agency (ERA) plays a central role in promoting interoperability and harmonising technical standards, as well as monitoring and reporting on rail safety in the EU [88].

An important part of ERAs work concerns the European Rail Traffic Management System (ERTMS), which is a major project to unify signalling and speed control on European railways. Harmonising the hardware and software are important for technical compatibility of infrastructure, rolling stock, signalling and other rail systems.

IoT is already on its way. Some technologies and applications are already tested or even implemented; others are more future-oriented as illustrated in Figure 18. Personal transport smartphone applications allow trips to be chosen according to optimal routes and prices, and may find more applications in the future [91].

Planning, booking and paying for journeys across all modes leading you to the right railway platform etc., providing a seamless real-time multimodal door-to-door journey planning and information tool. Allowing the user to prioritise which is most important to their journey (carbon emissions, trip duration, delays, facilities, handicapped accessible, personal needs, etc.).

Driverless locomotive includes automated systems in operation, which optimise the running time of trains and increase the average speed of the system, allowing more trains to operate closer together, reducing the time it takes a train to slow down at stations, and increasing reliability [91].

Wireless sensor technology and applications are increasing rapidly, and wear and tear on both the railway track and train set could be time consuming to detect. Smart-sensors that are communicating with engine driver or the company's communication centre will be able to foresee necessary maintenance and improve safety.

Aerial drones or UAVs (unmanned aerial vehicles) for improved mobile coverage, safety, reliability, operability, inspection, or even see around curves. Drones equipped with infrared cameras/sensors can make predicative maintenance a reality [91]. For example, check the switch point heating systems on its tracks.

Using the drone's images, you can see whether the switch point heating systems are operating correctly. If switching points are frozen, trains can no longer use the track, which can result in substantial delays or at worst cause accidents. Checking the switch points manually is labour-intensive and can be dangerous, so drones can offer a number of advantages.

4.2.4 Naval maritime

Already in 2009, the EU Commission presented the main strategic objectives for the maritime transport system up to 2018, which identified the key areas that will strengthen the competitiveness of the maritime sector while enhancing its environmental performance [99].

The developments and achievements until 2015, and the areas where further work is needed is presented in a Staff working document on the implementation of the EU Maritime transport strategy. The focuses are on the five areas:

- Maritime safety and security;
- Digitalisation and administrative simplification;
- Environmental sustainability and decarbonisation;
- Raising the profile and qualifications of seafarers and maritime professions and
- EU shipping: A stronger global player [100].

Marine Traffics' online services gives an overview of the maritime activity in Europe [102]. In the illustration below, all types of vessels are included at a randomly chosen time in September 2017. Most shipping companies are looking closely at the benefits that digitalization and automation can bring in operational gains.

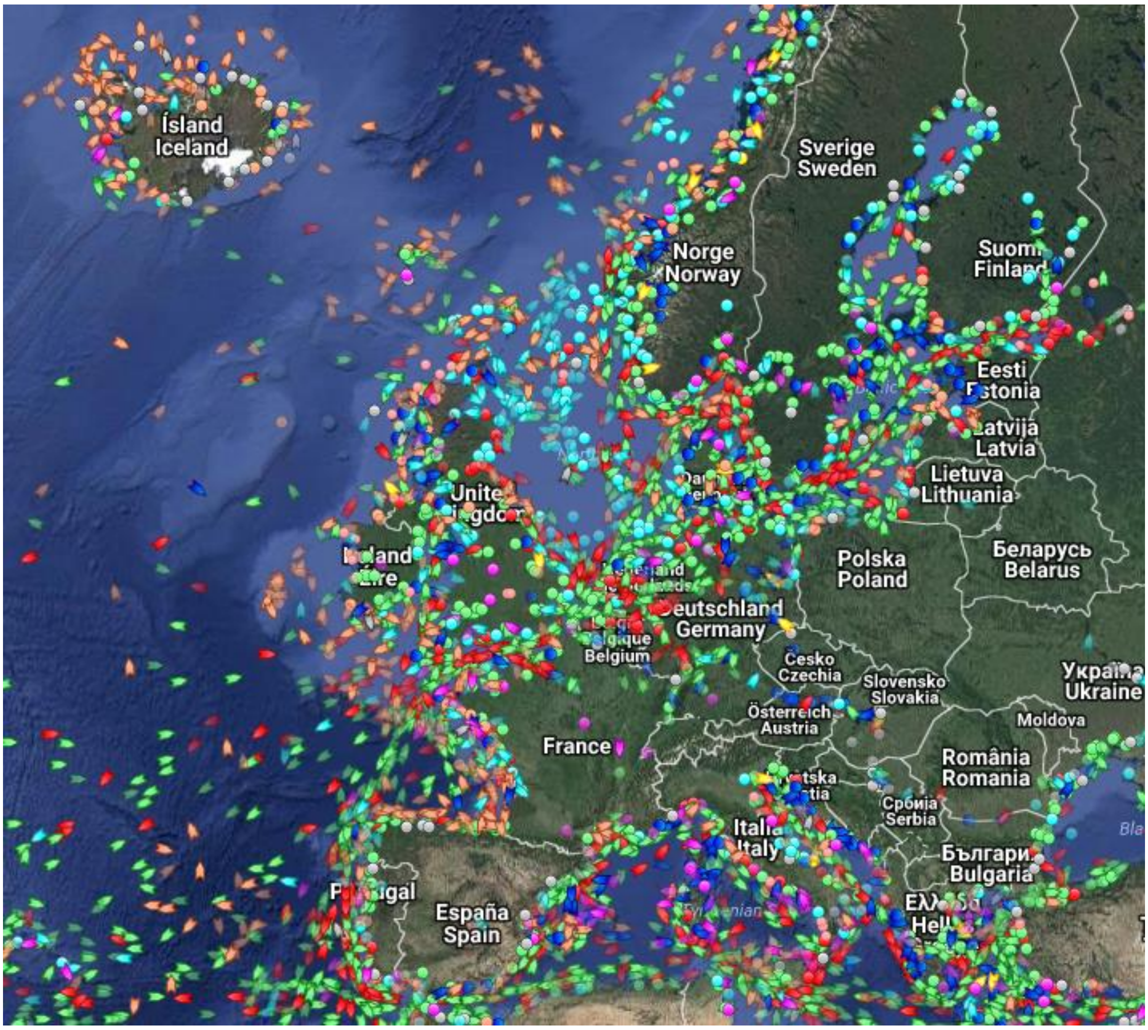

Figure 19: Maritime activity in Europe, overview Sep. 2017. (Source: Marine Traffic [102]).

The rapidly increasing digitalization and automation in merchant shipping, and the similar developments onshore called Industry 4.0, links to the term Shipping 4.0 and was proposed by SINTEF (MARINTEK) at Singapore Maritime week 2016 [101]. The maritime future and Shipping 4.0 are illustrated in Figure 20.

Digitalization is already on its way and digital solutions change the way we are working or doing business. Some technologies and applications are, as for the other transport modes, already tested or even implemented, and others are more future-oriented. Battery powered vessels and unmanned ships or autonomous shipping playing along with conventional ships [104].

Condition monitoring processes, including wireless smart sensors, diagnostics and prognostics. Camera-equipped drones (UAVs) with sufficient quality for inspection purposes, or cleaning up oil spills and garbage floating on the water.

Smart shipyards using 3D-models and virtual reality for smart design and building, where information based on Big-Data from ship operation is sent back to improve the consecutive designs and lead to the term "Shipyard 4.0" [104].

New Artic shipping routes are enabled due to melting polar ice and availability and reliability of communication in this area is getting more important. Geostationary satellites are struggling beyond 70-75º north, non-geostationary systems will be needed to provide reliable connectivity along these routes [105]. Iridium is an existing alternative but in the future, we may also see new systems using highly elliptical orbit (HEO) to provide connectivity in polar region [105].

Figure 20: Shipping 4.0 (Source: SINTEF MARINTEK)

Some examples on research initiatives concerning unmanned navigation and maritime cloud are given below. The Maritime Unmanned Navigation through Intelligence in Networks (MUININ) research project was co-funded under the 7FP. The aim was to develop and verify a concept for autonomous ships, which are seen as a key element for a competitive and sustainable European shipping industry in the future [108]. Three major projects around the world (EfficienSea2, STM Validation, SMART-Navigation) is working with the Maritime Cloud is a communication framework/connectivity platform enabling efficient, secure, reliable and seamless electronic information exchange between all authorized maritime stakeholders across available communication systems [107]. The Maritime Cloud, illustrated in Figure 21, is not completely operational yet, but can contribute to much easier for mariners to find the recommended services.

Figure 21: The Maritime Cloud (Source: EfficienSea [107])

4.3 Logistics

The supply chain optimization is always a hard barrier to overcome, because of the number of different actors involved, processes and standards. Different research European (iCargo, CASSANDRA, Core, etc) projects have focused about the need of sharing information in order to improve the different logistics services and have demonstrated how hard is to integrate new technologies in an, already, so complex and heterogeneous scenario. According to Monetizing the

Internet of Things – by Capgemini consulting [149], *“only 13% of organizations offer IoT solutions that integrate with third-party products and services”*.

The current quantification of data posted by IoT devices, and combined with mobile computing, data analytics and cloud technology is transforming the way delivery and fulfilment companies run their businesses. The clearest example is given by the asset tracking. It enables full optimization of supply chain and logistics operations, providing valuable tools for decision-making and time/money-saving tasks.

Maritime vessels tracking system (VTS) and Automatic Identification System (AIS) can monitor, track and trace, in real time, maritime traffic and vessels. A proper management of this information, by port systems, will improve multimodal synchronization. Like the example of Port of Hamburg, considered one of the most modern ports [9]. Sensors in the port can detect, and prevent, infrastructure failures, such as, railway switchers, malfunctions in bridge’s pieces, and taking measurements of structural strains.

These kinds of tools enhance customers' purchases but also enable customs security processes anticipating relevant information. Main logistic service providers and freight forwarders are improving track and trace tools to satisfy customers' demands.

In the last chain of logistics, retailers are already using analytics to understand market trends and to improve user’s engagement a shop experience. Main efforts are done about optimizing inventory across multiple channels [22], which implies a better integration and sharing of data during the full execution of a supply chain.

These are other example about how IoT will impact in the different phases of a logistic process [10]:

- Smart warehouses (where goods are identified, tracked and monitored in real time for optima storing, maintenance and delivery).
- Going beyond track and trace in freight transportation (with contextual information, conditions and alerts. New sensors can produce all this information out of the box, like the DHL Smartsensor [11].
- Fleet management not only about position but also about current state of the fleet, security, maintenance, etc.
- Last Mile Delivery opens a wide world of possibilities, because of interacting with consignees, about dynamic management of final delivery. Consignees, are usually, more used to adopt new kind of services.

The lack of standardization, and therefore, the integration difficulties derived are the main barriers about modernizing logistics processes.

4.4 Process industry

For decades, large parts of the equipment in industrial environments uses data communication for operating, managing and monitoring purposes, using systems as SCADA and Programmable Logic Controllers. This paragraph focuses on applications in the process industry that use sensors, actuators and output devices and particularly applications that (are likely to) use wireless connections. Most common buzzwords to describe the IoT trends in this area are ‘Industrial Internet (of Things)’ and ‘Industry 4.0’. This refers to a wide range of connections of industrial machine sensors and actuators to local processing, to the Internet, and to connections in, to and between industrial networks. The Industrial Internet faces challenges such as the need for more precision and timing optimization, adaptability and scalability, security, maintainability and extendibility (updates and meeting changing requirements), and flexibility.

The cost effective and flexible deployment of "IoT" capabilities such as monitoring and remote management creates an opportunity to introduce new business models for industrial applications. This is seen in a change from buying or hiring equipment to 'using the equipment as a service', where a pricing model is used based on how many times and for what purposes the equipment is actually used.

In the long term, this will result in 'smart factory' with better connections between enterprise networks and manufacturing, further optimizing availability of assembly lines, precision and reliability and with better real time "dashboard monitoring" of factory performance, use of resources, security threats etcetera.

4.4.1 Emerging Applications

Some of the most visible application fields of the Industrial Internet are mentioned predictive maintenance and remote asset management, improved worker productivity, and improved safety and working conditions.

Another example is Automatic Guided Vehicles, indoors or at container terminals, especially when combined with intelligence in the network and use of combined sensor information.

Industrial applications include a wide range of applications ranging from unmanned aerial vehicles to inspect pipe lines to monitoring food safety using sensors.

Location tracking of vehicles and equipment using GPS and sending location (and other) information via GPRS to a centralized coordinator is already common practice in fleet management applications and in the transport and logistic sector in general. In practice there is a trend that all kinds of tools are (getting) connected for monitoring, asset management and maintenance purposes, like robot welding machines communicating using GPRS and tightening tools with sensors, intelligence and wireless remote communication via ZigBee or other protocols.

4.4.2 Connectivity need and connectivity growth estimate

The number of installed wireless IoT devices in industrial automation reached 10.3 million in 2014, and expected to grow to more than 40 million in 2020, according to research reports.

Other examples include 4D Seismic Acquisition surveys reservoir dynamics using sensors throughout the field on the seabed, and the Smart Mobile Worker, where workers use a tablet device and a helmet camera to discuss situations with field experts in the head office.

Operational ranges are often local or metropolitan for in-house or on-site wireless connectivity, but also wide area networks are used when machines directly communicate with suppliers or maintenance companies. Industrial applications tend to optimize for robustness and reliability so in most cases use wireless communications for non-critical purposes, but also here applications often start as 'nice to have' and slowly may become critical from a business continuity perspective.

4.4.3 Technology and stakeholders

Industrial applications are typical large scale but at a static location, and specific for the kind of manufacturing that is taking place. Relevant stakeholders in industry are: Industrial companies, industrial internet consortia, governments and ICT standards development organizations.

Industrial companies (factories) that deploy IoT in their processes and sometimes develop their own IoT solution using their in-house R&D. These could be multinationals or SMEs.

Industrial Internet Consortia that develop standards and protocols especially for industrial purposes. Examples are the Industrial Internet Consortium (founded in 2014 by industry players such as such as AT&T, Cisco, General Electric, IBM, Intel and SAP and academic and government

institutions) with the goal to accelerate the development, adoption and widespread use of Industrial Internet technologies and the Open Interconnect Consortium (founded in 2014 by Cisco, GE Software, Intel, Mediatek and Samsung), to strive for more standardisation of open IoT platforms and protocols.

Governments can decide to fund the national industry or to fund research to make industries higher tech and adoptive to IoT.

ICT Standards Development Organisations develop standards and protocols for industrial purposes, these organisations are mostly international organisations that include large multinationals.

4.4.4 Trends and bottlenecks

Process industry/Manufacturing is expected by some to be one of the largest segments of the IoT market in revenues. In manufacturing and industrial environments, with relatively low mobility of equipment and with a need of high robustness and availability of tools, much of this is wired. Wireless communication is mainly used for non-essential communication, or when other communication is difficult and robustness by design is possible.

A potential bottleneck for further introduction of Industrial IoT applications is the variety of standards and their interpretation, both of existing industry automation and data exchange standards, as well as emerging M2M and IoT specific standards. Currently the interoperability between many 'islands' of manufacturing and industrial application platforms is still an issue but as is shown above there is a slow trend towards more uniformity of interfaces.

In general, Industry4.0 stresses the importance of strengthening the foundation of knowledge, skills and ICT parameters and it carries out research programme aimed at the development of software tools, with a view to chain cooperation, standardization and interoperability, and building on a robust and secure ICT infrastructure for Smart Industry.

Both governments and multinational industrial companies are possible enablers of IoT in industry. By funding R&D or initiating and coordinating industrial consortia, like Germany, Finland and the Netherlands do, these governments are possible enablers of IoT. Multinationals have their own R&D, take part of consortia that decide on which protocols and standards to develop and adopt for Industrial IoT, and have negative power to governments and mobile network providers to push these standards to be implemented. Finally, multinationals are also the end-users that ultimately will use the technology.

The applications of the Industrial Internet that are mentioned most commonly are predictive maintenance and remote asset management, and applications that improve worker productivity, safety and working conditions.

An example is Thames Water Utilities Limited, a major UK water and wastewater services utility company using sensors, analytics and real-time data to respond more quickly to leaks, changing weather conditions and other potentially critical situations. Other applications range from unmanned aerial vehicles to inspect pipelines to sensors for monitoring food safety. An example from oil and gas company Shell are the Smart Well, with downhole sensors and flow control devices monitored and controlled from the surface.

More application can already be seen in practice: examples are for instance robot welding machines with sim cards for remote monitoring and tightening tools and other tools with sensors, intelligence and wireless remote communication via ZigBee or other protocols for monitoring, asset management and maintenance purposes. Other examples are Automatic Guided Vehicles using sensor information and intelligence in the network.

In the long term this will result in 'smart assembly' with better connections between enterprise networks and manufacturing, further optimizing availability of assembly lines, precision and reliability, 'the visual factory' with better real time 'dashboard monitoring ' of factory performance, use of resources, security threats etcetera, 'Plant-wide Visibility' where globally dispersed production sites are integrated, and better standardization and uniformity of 'plant alarms an event resolution'80

4.5 Manufacturing

Industry 4.0 and the digital transformation of manufacturing are the two fields in which most Industrial IoT case studies are being conducted. This is due to the fact that manufacturing is not only the clear leader of all industrial activities but also among all IoT sectors. This is reflected on a total expenditure on IoT of $178 billion in 2016 [12], which is twice as much as the immediate follower, namely transportation.

Several use cases are leading the current implantation of IoT in manufacturing, as they provide direct efficiency, automation, customer-centricity and competitive benefits. On the following, some of these use cases are explained, together with their inherent challenges:

- **Manufacturing operations**. Several items are covered under this topic, such as asset management, intelligent manufacturing, performance optimization and monitoring, planning, human-machine interaction, etc. This is, by large, the most widespread use case for manufacturing, covering 57% of all IoT investments.
- **Asset management and maintenance**. On the one hand, this topic covers tracking some asset relevant and quantifiable metrics, i.e. location, quality, performance, etc. As a result of continuous gathering of this information, modelling and analytic/forecasting techniques can, on the other hand, assist on the asset maintenance, anticipating failures and extending the asset lifetime.
- **Field service**. This IoT-related area differs from the previous one as it goes beyond the factory itself and the manufacturing process to cope with product and business-related topics.
- **Other**. IoT is present and being implemented in a wide plethora of other manufacturing use cases, although the three previous ones' account for the vast majority of the investment. Among the rest use cases, worker safety/productivity, asset tracking, environmental/dangerous material monitoring or facility management are also relevant.

4.5.1 State of the Art

According to the most recent IDC European Vertical Market Survey IDC, 33% of Western European manufacturers are already using IoT to collect data about their products and operations, which is well below their U.S. counterparts. Also, most are using those tools on transactional and structured data.

By 2020, IDC estimates that 80% of large manufacturers will update their operations and operating models with IoT and analytics-based situational awareness to mitigate risk and speed time to market. IoT sensor data coming from product and processes, analysed in combination with other enterprise data sources (customer, supplier, product data) and external data (demographics, environmental conditions, POS) provides the situational awareness for manufacturers to better reconcile supply and demand without adding unnecessary risks.

Popular IoT deployment areas include security systems, fleet tracking, people tracking and warehouse management, with IDC data predicting the largest growth. Figure 22 shows all three of the major use cases in manufacturing - smart manufacturing (or connected assets), connected supply chain, and connected products gaining ground.

European manufacturers are in the process of instrumenting existing factory floor equipment and substantially improving connectivity to bring the pieces together, transitioning from segregated to coordinated and eventually fully integrated.

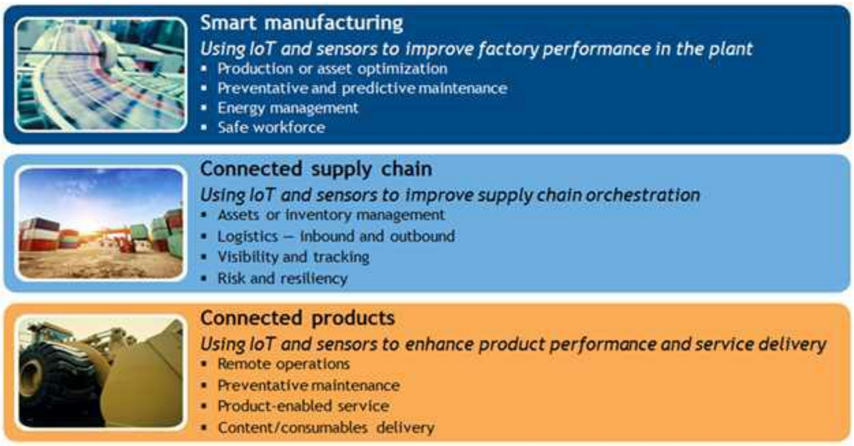

Figure 22: Major use cases in manufacturing (Source: IDC, 2017)

According to IDC surveys, top factors driving the investment in an IoT solution are process automation and improving business productivity, both internally and across customer relationship

While product quality has long been a priority for design and engineering, there's an increasing emphasis on service quality as well, largely in response to growing emphasis on customer centricity. In fact, service often offers the greatest opportunities to increase and improve customer interactions across manufacturing value chains. With connected products, manufacturers will gain access to data about actual product performance, usage, and quality. As a result, it becomes possible for manufacturers to sense and respond to quality issues more quickly and effectively.

Rising adoption of adjacent technologies such as robotics/3D printing and Analytics will specifically increase productivity, improve quality, and reduce safety concerns

4.5.2 Challenges and Inhibitors

The following challenges and inhibitors are expected for manufacturing sector in the following years:

- With the amount of data expected to be hosted online, data security is another key concern that IT is expected to address, particularly in the Manufacturing sector both internally and to ensure data security prevails in the products they produce.
- In addition, according to IDC European IoT Survey 2016, up-front costs, security, and privacy issues represent stumbling blocks in the way of fully transforming business models within the Manufacturing sector. A second group of current inhibitors relates to the difficulty in proving the RoI related to IoT investments, the perceived complexity of deployment and the lack of internal skills to address the IoT needs such deployment would require.
- One of the key challenges for the Manufacturing sector's IoT developments relates to the integration of supply chain, plant operations, and product and service life-cycle management. Today, Western European companies are actively figuring out how to provide information effectively across their organization and, at the same time, changing how they buy and use business applications.

4.5.3 Requirements for future development

The following requirements for future developments are expected in the manufacturing sector:

- Manufacturers looking to deploy IoT solutions will need to create an analytics layer that can ingest all of the different streams of data coming from products, service events, and customers, and provide actionable insights to the appropriate stakeholders.
- Digital architecture best practices and IoT security entity management techniques (as opposed to identity management) will be good starting points to redefine security architectures.
- Smart manufacturing initiatives must integrate IT and OT systems to achieve advantages in efficiency and response time. All "Industry 4.0" initiatives rely on integrated IT and OT systems to improve operational performance and asset management. IDC surveys also show that only about half of the equipment is connected to a network in the plant, resulting in pockets of integration. European manufacturers must instrument existing factory floor equipment and substantially improve connectivity to bring the pieces together, transitioning from segregated to coordinated and eventually fully integrated.
- European manufacturers will have to create IoT capability, either in-house or outsourced, to enable direct-to-consumption shipments and home delivery, as well as the ability to manage the smart chain

4.6 Energy

Energy sector current digital transformation is completely reshaping the business architecture. The traditional boundaries are being redefined, while the relationship between users and providers is being strengthen [20]. The traditional energy model, where power was generated from centralised conventional plants is no longer applicable. Renewable energy sources and decentralised production are now taking a very relevant role.

In addition, the liberalisation of the energy market facilitated the creation of new players serving energy to the customers and providing new energy services, such as ESCOs and aggregators. Customers are no longer passive recipients, they are becoming more active in terms of energy self-production and interests in value-added services beyond energy.

The process is characterised by an extensive use of data at every single level. These data is being produced (or expected to be produced) by deploying IoT devices all along the value chain. Energy utilities are currently adopting early measures to cope with these new challenges. Moreover, by 2020 it is expected that data analytics will reach a global value of 3.5 B€ coming from 650M€ in 2012 [21].

The challenges to be overcome differ depending on each piece of the value chain:

- **Generation**. This is the part of the value chain in charge of producing the energy. It ranges from traditional big energy plants to current local distribute and renewable energy sources. IoT is expected here to help on plant monitoring and predictive maintenance [22]. Gathering extensive information regarding each critical component in a plant is very valuable for modelling purposes. The generated models can predict failures before they happen and extend plant lifetime accordingly. Moreover, for renewable sources, external and/or environmental monitoring and prediction is also key to guarantee efficient operation of the whole network by anticipating potential peaks and valleys on energy production.
- **Distribution**. This applies to the way energy is directed from the energy sources to the customers. In addition, this central part of the value chain covers also the new need of transmitting information from customers back to the producers [23]. The way this energy grid is enhanced and operated is being changed currently, adding to the requirements concepts such as flexibility, balance and bi-directionality. IoT is impacting in this case on the grid predictive maintenance, especially considering substations.

- **Retail**. In this case, the IoT impact is evident, as most EU countries are currently rolling our smart meters on each energy customer, being some countries above 90% adoption rates. The ingestion of such a huge amount of information being periodically posted is an enormous challenge for energy utilities. A proper use of this information is the seed for implementing novel user engagement techniques such as Demand Response and other value-added solutions for customer in exchange for their data. Moreover, the connection of not only smart meters but also smart appliances inside buildings will suppose both a great source of information for utilities and a great IoT challenge.

The smart energy will in use the networking of IoT intelligent devices embedded within Distributed Energy Resources (DER) to cover the needs of different areas of the energy system i.e. consumer appliances, heating and air conditioning, lighting, distributed generation and associated inverters, grid-edge and feeder automation, storage and EV charging infrastructures. The future energy systems are characterized by 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.

The DER have diffused within end-user premises, new transactive energy (TE) control approaches and require to facilitate their coordination at various scales of the grid system through real-time pricing strategies. Aggregators and energy supply companies are developing new flexibility offers to facilitate DER coordination virtually through ad hoc virtual power plants, raising new connectivity, security and data ownership challenges.

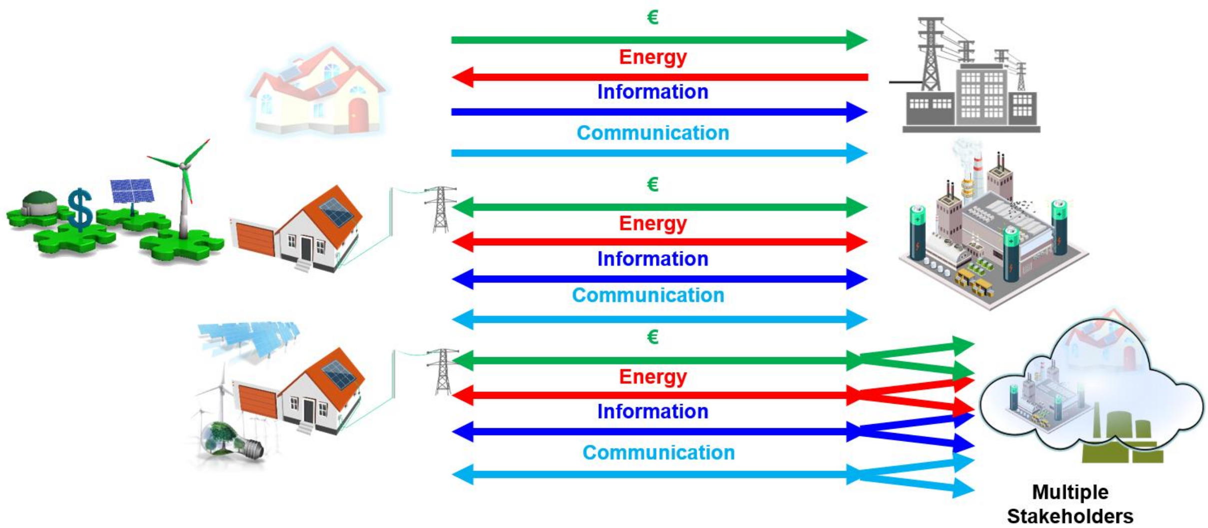

Figure 23: Flow of energy, data and money in Internet of Energy [24]

By 2030, the future utility value chain will have transformed significantly. Navigant Research argues that current distribution network operators will have transformed into distribution service orchestrators; they will be responsible for far more than just network operations. Likewise, the current energy supply business - already transitioning to a service-based model—will be fully transformed into an energy service provider (ESP) model. Companies will offer end-to-end energy services that have little in common with today's volume-based approach to revenue generation. The resulting new business models will require new IT infrastructure that relies heavily on the analysis of huge volumes of data.

Distribution orchestration platforms will rely on the integration of existing advanced distribution management systems (ADMSs) and DER management software, as well as the incorporation of a market pricing mechanism to reflect the changing value of millions of connected endpoints

throughout the day. ESPs will rely on TE platforms that enable prosumers to sell their power into the market, incorporate customer portals to provide in-depth account details, and provide billing and settlement functionality [25].

The high number of distributed small and medium sized energy sources and power plants can be combined virtually ad hoc to virtual power plants. Internet of Energy (IoE) that is defined as a dynamic energy network infrastructure including energy cloud storage based on standard and interoperable communication protocols that interconnect the energy network with the Internet allowing units of energy (locally generated, stored, and forwarded) to be dispatched bidirectionally when and where it is needed is the solution to these types of deployments. In this context, the related information/data and financial transactions follows the energy flows thus implementing the necessary information exchange together with the energy and financial transfers [24].

In this context, the following are the characteristics of the future smart grid [24]:

- The grid is two-way, networked, distributed, clean, and intelligent. Distributed energy resources (DER), (i.e. solar PV, energy storage, and EVs) are ubiquitous.
- Transactive energy (TE), allows DER owners to trade their self-generated power.
- End-to-end energy services and energy distribution orchestrators
- Utilities rely on IoT, machine learning and analytics-driven automation to manage the grid.

The 2030 energy landscape, presented in, has the customer in the centre of the Internet of Energy and Energy Cloud with the following characteristics [25] [26]:

- Ubiquitous solar PV and storage create a customer-centric energy value chain where customers' consumption is largely met by self-generated electricity.
- Utility-scale and distributed renewables account for 50%-100% of generation; distributed energy resources (DER) uptake is widespread, accounting for most new build capacity.
- High penetration rates of EVs put a strain on network capacity, which is managed using pricing signals and automatic demand response (DR).
- Data is as valuable a commodity as electrons. While in 2017 the industry struggled to maximize the value of enterprise data, in 2030 the energy supply chain is fully digitized and its efficient operation is heavily based on analytics-based automation. This automation relies on the huge volumes of data created by technologies within the Energy Cloud and Internet of Energy.
- The industry has undergone significant digital transformation. Data and artificial intelligence (AI)-based algorithms become important competitive differentiators. Data offers visibility into each prosumer's electricity exports and imports, providing the fundamental basis of the transactive energy market. This data also allows the newly formed distribution service orchestrators to actively manage the dynamic and volatile distribution networks, either through pricing signals or by actively interrupting the power supply.
- Utility business models have transformed from supply- to service-based. Rather than focus purely on the delivery of grid-sourced power, energy service providers (ESPs) offer individualized products and services to suit their customers' specific needs. These services will include DER sales, maintenance, and aggregation; DR; energy efficiency initiatives; flexible, time-of-use charging; and TE platforms.
- Markets are far more competitive in 2030 compared to 2017. The convergence of the old regulated supply business model and deregulated service-based model creates opportunities for new entrants. Many new service providers have entered the market, exploiting the new value streams from decentralized electricity.
- The smart grid of 2017 has transitioned to a neural grid. The new grid is nearly autonomous and self-healing, leveraging innovations in AI and cyber-physical systems (e.g., IoT, self-driving EVs, and the smart grid).

- Distribution operators have evolved into distribution service orchestrators to manage this neural grid. Advanced platforms incorporate advanced distribution management systems (ADMSs), DER management systems (DERMSs), and pricing signals to manage the more volatile and dynamic grids.
- Technology platforms such as TE and distribution orchestration platforms enable prosumers to sell self-generated power on open markets and manage the highly volatile and dynamic distribution networks.
- In 2030, prosumers trade their self-generated power on the open market. This is a dramatic change from relying on the subsidies or net metering that supported residential solar PV in 2017. Electricity is bought and sold at market rates and revenue from a TE platform alone totals $6 billion per year.

The challenges that need to be addressed include security, safety, robustness, resilience and self-healing of the energy grid, with economic, political, regulatory constrains that need to consider the regulatory changes, unbundling, new actors, competitors, new business models, investors' pressure and need to improve profitability.

New technologies such as IoT, smart metering, batteries for energy storage, analytics and artificial intelligence will change the energy sector landscape, new energy sources, demand side management, distributed generation, renewable energy, energy storage will increase the efficiency and change the business models of the energy sector in a disruptive manner.

4.6.1 State of the Art

Utilities (Energy included) often fall on the conservative side of the spectrum when it comes to the adoption of new technologies. But when it comes to the IoT, utilities are not so far behind the Western European (WE) cross-industry average of 23% adoption. WE utilities across the various segments of the value chain have a current adoption rate of almost 19%, with 13.7% of respondents planning to adopt said technologies in the next 12 months.

According to IDC survey results, WE utility suppliers indicate higher adoption of IoT technologies (21.7%) than their transmission and distribution (T&D) peers (15.2%).

WE utilities main areas to leverage IoT include: demand management, asset maintenance and connected homes and to a lesser extent, remote asset control, quality control and weather sensors.

Reducing operational costs remains the top driver for utilities to invest in sensors and devices. Worldwide utilities said improving business productivity and internal efficiencies is their number 2 driver, while European utilities, driven by liberalization, chose reaching new customer target segments. Other drivers include process automation, improve productivity, creation of new revenue streams and improving time to market.

Escalating cyber threats to utility grids and assets are pushing European utilities to increase their investments in sensors and devices to enhance their security systems (video surveillance, motion detectors).

4.6.2 Challenges and Inhibitors

The following challenges and inhibitors are foreseen for the energy sector:

- Despite cybersecurity, concerns being the top barrier to IoT deployment for European utilities, the actual share is relatively low (around 20%). In fact, there are more utilities that see IoT as a way to increase security rather than a threat
- Upfront costs, lack of data analysis skills and lack of holistic offers and maintenance costs are the main barriers to IoT adoption amongst utilities, as figure shows.

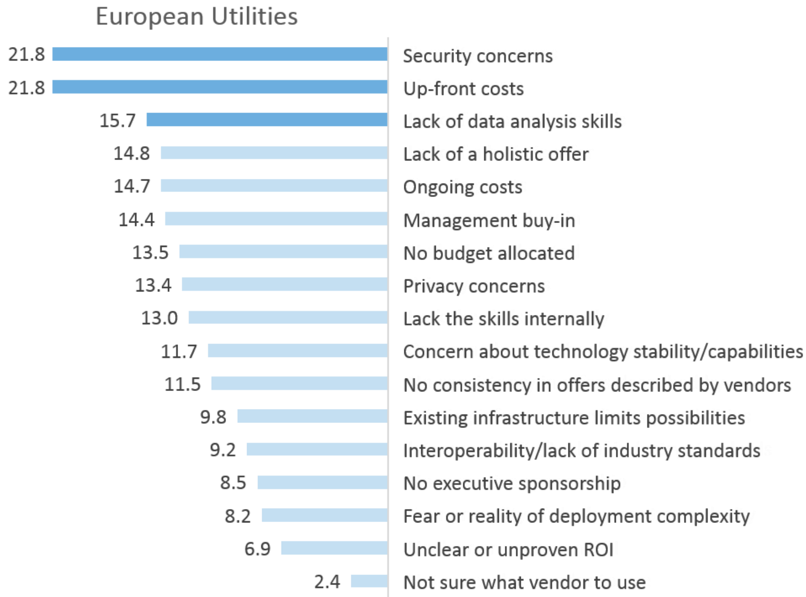

Figure 24: Flow of energy (Source: IDC's Global IoT Decision Maker Survey, 2016 (n = 242))

4.6.3 Requirements for future development

The requirements for future development in the energy sector are:

- The lack of universal standards for IoT data, formats and integration required to share data between systems is acting as an imminent barrier to IoT adoption amongst the Utilities/Energy sector across Europe. Further developments are needed around this areas
- Addressing limited market availability of certified equipment for specific use cases (i.e. smart metering)
- Addressing potential regulatory concerns related to, for example, the long-term implications of using cellular technologies (GSM based) when GSM licences expire, ensuring certain long-term stability to potential investments
- Private and public organizations must start retraining both field and office workers on necessary skills to work with latest IoT/Data analytics technologies, devices, software, etc. This encompasses serious organizational challenges for a large number of organizations who may not have the required resources nor ability to address this problem.

4.7 Buildings

4.7.1 State of the Art

The rise of connected smart devices aimed at the Home environment is undeniable. From smart thermostats, to smart alarms and heating and lighting systems, the variety of solutions is mind-blowing. IDC estimates the Western European Smart Home market to reach just under 10,000$Mn in 2017, booming to just under 23,000 $Mn by 2021 primarily driven by the demand for home automation, security and smart appliances.

Companies like Google, GE, Amazon, Centrica etc. are all entering what is an already complex and crowded market. From consumer goods manufacturers, to security and equipment vendors, the ecosystem is complex.

4.7.2 Challenges and Inhibitors

The following challenges and inhibitors are expected for the smart buildings sector:

- Security – Security is by far the primary challenge to Smart Home developments. This is important if we consider that the various smart devices appearing in homes may not be shipped with embedded security functionality and controls. Yet they represent a potential point of weakness through which malware and other forms of security attack can gain entry to home networks.
- One of the key challenges to address the Security problem is the fact that most Consumers are not fully aware of the real threats they face, and the industry as a whole is struggling to convey a message that strikes the right balance between the consequences of a lack of security and avoiding an alarmist message that deters demand altogether.
- Integration of home systems is crucial in creating and sustaining a well-oiled smart home. Due to variance in the pace of innovation of technology, consumer devices and smart home commercial systems, integration can either make or break a smart home.
- Energy consumption – with the rapidly increasing number of connected devices around the home, energy consumption and its impact on home budgets can become an area of concern for some users.

4.7.3 Requirements for future development

The requirements for future development in smart buildings sector is estimated to address the following issues:

- Overcoming the initial hurdles around security can eventually lead to a subscription based security services model for the Connected Home.
- Efficiency improvements are fundamental to reducing energy consumption, an important concern for consumers of multiple smart devices around the home. Reducing energy consumption and the resulting power bill is an important reason many consumers purchase smart home systems. But efforts to reduce energy consumption are moving beyond basic energy saving. Products are now working more efficiently while still meeting user expectations and offering more interactive functions. For example, the Ecobee3uses small wireless room sensors to control room temperature and enable smart energy saving. Honeywell’s Evo home thermostat system allows users to set different temperatures for different areas in a room.
- Personalized services to meet user habits and preferences: Smart home products have already started using AI self-learning technology to improve the user experience. For example, the latest smart bulbs from BeOn can discern patterns in user behaviour and learn to automatically turn lights on or off as appropriate. These bulbs can also turn lights on when visitors ring the doorbell. They therefore meet the needs of individual families and also play a role in basic home security.
- Entertainment to drive demand for a wide range of smart home products. In addition to security and energy efficiency, future smart home products will form a home entertainment system, with a single device allowing users to quickly and conveniently control multiple smart entertainment devices in a variety of tailored scenarios. For example, Amazon’s Echo and its mini version Echo Dot, unveiled in January at CES 2017, can connect with more than 7,000 different apps and services. This greatly enhances the entertainment options available in the smart home.
- Open ecosystems are essential to connecting smart home products and services. Smart home ecosystems provide convenient and simple products and services that meet user needs in different situations. Therefore, improving compatibility between different smart home products is the foundation for connectivity, while establishing open platforms is the key to expanding smart home ecosystems. Companies such as Amazon and Google are working towards open smart ecosystem platforms, but many outstanding smart home devices, such as the BeOn smart bulbs and the Scout Home Security System, still cannot connect with multiple platforms.

4.8 Communities

Smart communities are a collection of interdependent human-cyber-physical systems, where IoT represents the sensing and actuating cyber-infrastructure to estimate the state of human and physical systems and assist in adapting/changing these systems. Smart communities are often classified along multiple dimensions:

- IoT technological (cyber) workflow dimension including (a) sensory "things" development and deployment, (b) connection of "things", (c) digital data collection from "things", (d) processing, aggregation, analytics of correlation of data according to human-physical models and urban domains/applications, (e) comprehension of data and findings, (f) creation of new services and actions, and (g) actuation of "things" to gain new data. The technological workflow represents a full loop of digital data life cycle from data capturing, monitoring, to collection, processing, analysis and feedback to the cyber-system according to physical or human models.
- IoT urban domain and application dimension including (a) urban mobility (transportation system), (b) health care, (c) utilities (e.g., smart grid, water, gas), (d) urban living (smart home technologies), (e) public services (incident reporting), (f) safety and security (police, first responders), (g) sustainability.
- IoT stakeholders dimension including elected/appointed officials as decision makers to select usage of urban systems and to ensure economic development and cost-effective usage of municipal resources; city workers as the implementers of decisions made by officials; citizens as beneficiaries of smart city services; and vendors / developers / entrepreneurs as providers of smart city hardware, software, and services, partners in economic development. These stakeholder roles are unique to the smart communities IoT problem because, for example, elected officials interpret and act upon IoT data, hence IoT data collection, analytics, and comprehension research must provide high accuracy solutions, based on short training time, to enable fast and high fidelity decision making process; city workers are vital to the success and failure of IoT deployment across communities, hence IoT sensing, actuation, and connectivity research must provide scalable and easy-to-deploy solutions; citizens support IoT infrastructure investments, hence IoT development, deployment, and usage research must be connected to IoT economics; and vendors have vested interests in seeing their IoT solutions chosen over competing products, which requires research in creation of new IoT services and applications.

Next to the classification we see several Smart Communities IoT Challenges. From the cyber workflow point of view, IoT systems must satisfy requirements such as real-time, robustness, reliability, resilience, privacy and security to have a long-term impact. These IoT system requirements (e.g., real-time, robustness, security) represent major challenges for the cyber-workflow stages (e.g., data collection, analytics, comprehension, actuation stages) if we want these requirements to be satisfied in an end-to-end manner and ensure also a seamless integration into existing communities' testbeds and environments. Other challenges are related to Sensor Development and Deployment, Connection of "Things", Data Collection from Things, Analytics of Data, Comprehension of Findings, Creation of New Services and Actions and Actuation of Things.

In summary, Smart Communities IoT capabilities have a very promising and important place in solving the growing communities' challenges. However, to enable these IoT capabilities fully, trustworthy algorithmic and system designs must be integral parts of the overall Smart Community framework (and all of its dimensions) which includes not only the IoT cyber-systems challenges but also the physical and human systems, understanding their models, constraints and characteristics.

4.9 Healthcare

4.9.1 State of the art

In the last few years, various practical challenges for the integration of IoT functionalities in the field of healthcare have been examined by the research community. These challenges are divided in two main categories: 1) Network architectures and platforms, and 2) services and applications, interoperability, security and others. However, the research in this field is still in an early stage.

One of the most important parts of the IoT in healthcare is the IoT healthcare network (the "IoThNet"). The research on the IoThNet focuses on the network topology, the architecture and the platform. Equally important are the healthcare services and applications enabled in an IoT environment, which in many cases are confounded. Some of the provided services are: Ambient Assisted Living (AAL) that addresses the health care of aging and incapable individuals, the Internet of m-Health Things (m-IoT) which is used for the connection and communication of medical devices and sensors for healthcare services, Adverse Drug Reaction (ADR) which can occur from the medication intake , Community Healthcare (CH) for monitoring an area around a local community, Children Health Information (CHI) that tries to inform the general public for all the aspects and needs of children's health, Wearable Device Access (WDA) is a service for the integration of heterogeneous wearable devices, Semantic Medical Access (SMA) is used for the semantic interoperability of the medical information used, Indirect Emergence Healthcare (IEH) for the emergencies that cannot be addressed due to adverse conditions, Embedded Gateway Configuration (EGM) for the connection of network nodes, the Internet and other medical equipment and the Embedded Contect Prediction (ECP) which is a generic framework with mechanisms that enable the development of healthcare specific applications over IoT networks . A few examples of applications are blood pressure monitoring, body temperature monitoring, glucose level sensing etc.

4.9.2 Challenges and inhibitors

- Data protection: Devices and sensors in the healthcare field are gathering and/or processing vital private information such as personal healthcare data. Moreover, these devices are connected in global information networks which makes them vulnerable to potential attackers. Thus, the need for security is significant.
- Standardization: Devices and sensors produced do not follow specific protocols or design ruls, thus not enabling interoperability amongst them. Standardization should take place in all aspects, for example in hardware level but also in communication level.
- IoT Healthcare platforms: IoT healthcare platforms should be able to facilitate the more advanced and sophisticated sensors (hardware-wise) used in healthcare by setting the right approach through APIs, libraries and frameworks available to developers and designers.
- Technology transition: Healthcare organizations can update their medical equipment integration IoT solutions in their existing framework. Nevertheless, this is a time consuming process and there must be backwards compatibility for the transition period.
- Power consumption: Many sensors used for healthcare cannot be replaced frequently. Thus, they should be energy efficient.
- Scalability: An IoT healthcare solution should be scalable because more and more complex applications and operations are demanded.
- Continuous monitoring: There are many cases where long-term monitoring is essential.
- New diseases and disorders: It is crucial to be able to adapt to new conditions but also to discover new diseases and disorders in order to act fast.

- The quality of service (QoS): Healthcare services and measurements are highly sensitive due to their nature. Thus, reliability, maintainability, service level and system robustness and availability should be guaranteed.
- Mobility: Mobility of patients should be feasible at all circumstances.

4.9.2.1 Opportunities of IoT solutions

Through connected medical sensors and remote care services, IoT solutions make self-managed and home-centred care available. Such solutions hold potential to lower down overall healthcare expenditures by reducing hospital visits and admission, and increase care quality through continuous patient monitoring and data-powered preventive care.

At current stage, the overall cost-efficiency of connected health is still being explored by the industry. However, some programs [27] already proved that home-delivered care is effective in reducing complications while cutting the cost of care by 30% or more.

4.9.2.1.1 Remote patient monitoring

The principle application of IoT in healthcare is remote patient monitoring (RMP), particularly for those living with chronic conditions, senior and fragile population. Through connected devices and care delivery platforms, care givers, patients and funders are connected within health systems in a continuous manner.

Connected medical devices

Home-based medical devices are not necessarily wearable, but are incorporated with connectivity module so that they can communicate with the home health-hub (a gateway device), which then transmits personal health data to caregivers at preconfigured period. Sleeping respiratory problems, cardiac vascular disorders, diabetes and falling detects are among the main targeted diseases.

It is the trend that even consumer wearable devices are moving into medical device markets, in order to provide more clinical-reliable data for both users and physicians, thus promoting user engagement and utilization value. Besides, cellular connectivity is taking lead, as it has already replaced PSTN as the de-facto standard communication technology for most types of connected home medical monitoring devices and will account for 25.2 million connections [28] in 2021.

Remote patient monitoring services

The application of connected medical devices brought forth a slew of new services in the healthcare industry. Among them, remote patient monitoring (RPM) is being widely developed. The following three blocks are indispensable to constitute effective RPM services:

- **RPM:** 1) Self-monitoring multiple vital signs via connected sensors, normally including weight, pulse, temperature, blood sugar, blood oxygen, and ECG or respiratory conditions. 2) Medical apps allowing share self-measured health data with designated persons (doctors or families), accessible in a patient-controlled manner. 3) Access to health data and analytics.
- **Telemedicine**: virtual consultation with doctors that enlarges care access. In the meantime, it allows an interpretation of self-measured data without physical visits to doctors.
- **Tele-assistance:** 1) Immediate alert to monitored patients, their families and hospitals/doctors. 2) Redesigned home-care delivery by particular caring teams, for regular follow-up or emergencies.

Apart from remote monitoring of chronic diseases on real time, RMP services are also applied to continuous monitoring of discharged patients, so that healthcare resources associated with long-stay hospitalisation can be saved. Compared to chronic condition management, such application

requires more personnel intervention since the installation of medical materials (medical beds for instance) and necessary treatment cannot be performed by patients themselves.

4.9.2.1.2 Data-driven services

Care delivery platform

Care deliver platform is the key technological enabler for almost any other connected healthcare services. Care delivery platforms are typically software solutions that allow care efforts to be coordinated between patients, various caregivers and other stakeholders.

More technically speaking, a care delivery platform should encompass 1) health data storage with regulation-compliant security, 2) IS integration to assure smooth data relay between different systems and portals, and 3) data intelligence that provide clinical decision support for professional careers, and assists in workforce collaboration during care delivery.

Personalised care

Personalised care is expected to be the next step of connected health. Leveraging EHRs (electronic health records), home-based personal health data, "-omic" data, environments and lifestyles, the overarching objective of personalized care is to delivers the right treatment at the right time to the right person, in a proactive approach.

Indeed, there is no set template for a personalized care plan. The principles are to go beyond clinical treatment, taking a whole-life and -environment approach. Assembling and intelligence of the individuals' health and lifestyle data is the first step. Devices makers such as Apple, Fitbit, Withings, Jawbone and Epic are very active in research collaboration by opening API and providing software toolkits to access device/user-generated data. National and regional support is ongoing as well, personalised care has been put to a nation-level strategy in the UK and the US.

Besides, thanks to the development of big data, AI and genetic technologies, personalized care is hopefully moving forward with the capacity to foretell chronic diseases and prevent deterioration in the future, thus lowering the overall social and care cost down

4.9.2.2 Key Challenges

4.9.2.2.1 Business models

There are also obstacles, primarily associated with the financing models. Lack of reimbursement is often named as one of the main barriers. This is a more complex with large variations due to differences in how healthcare is funded country-by-country. In addition, patients have little willing to pay out-of-pocket money. On this basis, the payers (social systems and private assurance companies) are reluctant to go centre of play, before the real benefits of connected solutions to health industries are widely proved.

In this context, the health industries begin to focus on the senior population, as this demography has greater demand for high quality care and greater personal wealth, hence purchasing power, than the rest of the population. Another fact needed to point out is, by 2050, digital natives will have become senior citizens (< 65 years). So it seems likely that they will be far more receptive to IoT solutions than today's seniors, which will naturally influence the rate of acceptance.

4.9.2.2.2 Strict data regulation and security concern

Healthcare industries operate in a highly regulated space, which differentiates it from other IoT markets. Although consumers are relatively more open than before to sharing health data, the health data access and processing is still constrained by to-be-solved data silo problems, related

regulation and policies (HIPAA, GDPR, the European mHealth Green Paper and likewise). Due to those constraints, the data-driven power (for example, in personalized care) is yet to unleash.

Beyond that, cyber security also arises a lot of concerns. The most recent and severe attack was caused by WannaCry virus - around 50 NHS Trusts in the UK were badly affected. The increasing use of connected medical devices at home and processing of personal health data put more demanding requirements to increase cyber security level, and to standardize the personal health data use.

4.9.2.2.3 To-be-proven CAPEX/OPEX efficiency for carers

The financial incentives for other stakeholders than patients (caregivers, clinician and payers) to participate in connected health are, so far, insufficient, given the CAPEX/OPEX issues coming with new devices and care pathway alignment. Physicians have to purchase new hardware, software, and redesign their practices, as well as reconfigure or add medical office staff. However, the return on such investment is not yet clear.

Some countries are hence prioritizing investment in health IT and different connected healthcare solutions. For example, the UK has created an institute to calculate what it is worth (or not worth) to invest in for the healthcare transformation. Quite recently, since 2017, NHS has started to redesign healthcare services and delivery model at scale, with objective to accelerating the deployment of eHealth services in a cost-effective manner.

4.9.3 Requirements for future development

- End to end security: healthcare systems may comprise multiple heterogeneous systems and platforms, thus end-to-end security is required for protecting the user data across the whole data lifecycle from their generation on the IoT devices towards their exploitation in the IoT applications.
- Interoperability: due to the multiple of technologies, platforms and systems that are involved in healthcare systems, activities for standardisation and interoperability are of major importance to ensure the optimal performance of the applications
- Efficiency: due to the critical nature of healthcare applications, the efficiency of the systems is of utmost importance, especially with regards to data reliability and availability.
- Compliance with GDPR: data protection is becoming a mandatory requirement in the EU with the upcoming effectiveness of the GDPR, thus healthcare applications and systems should comply to all GDPR requirements, especially with respect to privacy by design and by default.

4.10 Security, privacy and trust

4.10.1 State of the art

Security, privacy and trust in IoT are only getting attention the last few years, while initially the focus was more on designing and developing the technologies for realising IoT products and platforms.

This has result in the situation where many IoT products and systems (even the ones that are available in the market) are not designed to be secure, trustworthy and privacy preserving, resulting in several incidents that have been released in the public. For example, there have been reports about smart fridges being hacked to send spam mails [30], smart lightbulbs having vulnerabilities that can allow attackers to gain access to the home network [31], smart plugs that can be controlled by anyone that knows their MAC address [32] and smart cars with weak pre-shared keys that can

be easily cracked allowing malicious users to control the car [33]. Additionally, in 2016 hacked IoT devices were implicated in an internet outage on October 21st in the US [34].

4.10.2 Emerging threats for security and privacy

According to a survey carried out by Altman Vilandrie & Company on 397 IT executives across 19 industries in the U.S., 46 percent of organizations have experienced at least one IoT security breach [30].

The study showed that preparedness helps. Companies that have not experienced a security incursion have invested 65 percent more on IoT security than those who have been breached. Other key findings: 68 percent of respondents think about IoT security as a distinct category, yet only 43 percent have a standalone budget.

The IoT is transforming everyday devices in ways we are just beginning to appreciate. Already, Intel estimates more than 15 billion smart Internet-connected devices are in operation, and we expect this number will reach more than 200 billion by the end of 2020. Many of these devices are inadequately secured; security in IoT is therefore gaining momentum.

In October 2016 the domain name service company Dyn was attacked with a massive and complex distributed denial-of-service (DDoS) attack. The analysis of the attack confirmed that the DDoS traffic originated from IoT devices infected by the Mirai botnet.

The malware spread through poorly secured routers and IP cameras; it targeted vulnerable devices by continuously scanning the Internet for IoT systems protected by factory default usernames and passwords.

By the same token, privacy issues have become central in IoT too. In September 2016 the Global Privacy Enforcement Network, which comprises 60 privacy regulators from 39 jurisdictions, performed a sweep on IoT. The study, which was carried out on 300 devices, revealed that [36]:

- 59 per cent of devices failed to adequately explain to customers how their personal information was collected, used and disclosed;
- 68 per cent failed to properly explain how information was stored;
- 72 per cent failed to explain how customers could delete their information off the device, and
- 38 per cent failed to include easily identifiable contact details if customers had privacy concerns.

As showed by the facts and figures above, security and privacy are two sides of the same coin in IoT, particularly in consideration of the policy shift produced by the General Data Protection Regulation, which mandates organizations to design IT and processes in general along the lines of privacy-oriented policies, in order to prevent that IoT devices become, on one hand, a tool for fine grained surveillance and, on the other hand, a gateway for harmful attacks to personal data.

4.10.3 Policy Trends

The issue of trust in the IoT, and the need to combine security and privacy is also at the core of the recent Cybersecurity Strategy of the European Union [37], whereby a proposal of the Commission on a EU cybersecurity certification framework is anticipated [38].

The Framework would lay down the procedure for the creation of EU-wide cybersecurity certification scheme, covering products, services and/or systems – including IoT - which adapt the level of assurance to the use involved (be it critical infrastructures or consumer devices).

It is particularly noticeable the focus that the EU is putting on the use of "security by design" methods in low-cost, digital, interconnected mass consumer devices which make up the IoT: schemes under the framework could be used to signal that the products are built using state of the

art secure development methods, that they have undergone adequate security testing, and that the vendors have committed to update their software in the event of newly discovered vulnerabilities or threats.

The latter priority goes hand in hand with the privacy by design methodology introduced by the General Data Protection Regulation.

It is also noteworthy that the strategy acknowledges the important role of third party security researchers in discovering vulnerabilities in existing products and services.

This approach indeed converges towards the strategy for certification outlined in Section 7.3., where the exploitation of certification schemes elaborated within EU research projects is proposed as the backbone of a Trusted IoT Label.

Certification of IoT

To achieve the goal of a Trusted IoT (Label), the certification mechanisms envisaged by Article 42 of Regulation 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter the "GDPR"), are crucial to establish a Trusted and Secure IoT Label, either at European Union or Member State Level. Such a label also aims providing transparent information on the varying degrees of privacy and security applied within the IoT ecosystem. As required, this label will also determine compliance with the European Union Network and Information Security Directive.

This unique label intends to combine IT security assurance and transparency in information transmission to consumers. Thus while, general IT security certification schemes are directed only at the infrastructure and governance sections of the IoT ecosystem, the goal of Trusted IoT will take into account the changing dynamics of the consumer market and provide transparent information about relevant products, while maintaining the required levels of security. Such a label will also account for the fact that security is not a homogenous or static concept and cannot be (easily) adequately measured given the vast range of ICT products in the changing IoT landscape. Thus, while a given ICT device may enjoy a high-level of security in a specific time-frame and environment, the degree of associated or perceived security may vary in different environment and at different time intervals. The certification schemes related to Trusted IoT will take this aspect into account and will carefully ensure that the information on devices being utilized are continuously updated such that the security of the IoT sphere is not compromised at any stage.

To initiate and support the development of this label, a survey to collect and identify requirements shall be carefully crafted. In order to further consolidate this Trusted IoT label, relevant aspects of this label shall be submitted to the ITU-T Study Group 20 on IoT and Smart Cities and Communities to promote international standardization based on this world.

4.10.4 Challenges

There are several key challenges for IoT security, privacy and trust as seen below:

- Constrained devices capabilities: IoT devices span from tags, RFIDs and sensor platforms to mobile phones and other powerful machines. However, most IoT devices are constrained in terms of memory, CPU, storage and battery, which means that either they are not capable of running security, privacy and trust algorithms or they can only sun very lightweight versions.
- Device heterogeneity: due to the fragmentation of IoT system and technologies, IoT systems normally comprise devices that come from different vendors and use different technologies for networking and communication. This device heterogeneity poses several security challenges, since it is not always possible to implement efficient protocols and algorithms on all the devices across the many IoT application areas.

- Cyber physical systems and actuators: IoT systems of the initial era were almost exclusively devoted to gathering information from sensors. However, lately, there is a turn towards actuators for the development of more advanced applications. Security challenges in systems with actuators are more complicated, since the actuators allow the virtual world to affect the physical world. Thus, issues of safety are now becoming critical in IoT systems.
- Distributed environments: scalability in IoT systems is one major challenge, since billions of IoT devices are supposed to be interconnected in the near future. Centralized systems won't be able to overcome the load and there is lately a trend towards creating distributed IoT systems. Security in distributed systems is much more complex, due to issues such as identification in distributed environments and authentication of devices.
- Linked data and privacy by design: the main concept of IoT allows data interoperability across platforms, systems and applications, allowing the linkability of data and the creation of "linked data". However, this contradicts with the main requirement for "unlinkability" of the privacy by design concept in order to protect the confidential information of users.
- Secure system bootstrapping: manual bootstrapping and configuration of large-scale IoT systems is impossible, thus self-x functionalities are normally utilized. However, these present new attack surfaces, especially at the initial bootstrapping phase of the devices, where malicious third parties can play the role of gateways/servers to intercept data and get access to the system. Initial security credentials should also be distributed in an optimal way.
- Contextual adaptations of security and privacy: in IoT systems, normally, security and privacy policies are statically defined by the system administrators. However, these policies should be allowed to dynamically change according to the context of the situation, i.e. in emergency situations.
- Trust management frameworks: to improve the adoption of IoT systems by the general public, these systems must become more trustworthy in several aspects, i.e. their availability, their security, and the reliability of the services they provide. In this respect, trust management frameworks should be embedded in IoT systems, calculating the reputation of users, devices and services, and applying corrective actions when issues arise.
- Compliance with GDPR: the EU GDPR will be effective starting May 2018 and provides regulations on the handling of user data. IoT systems must be compliant with the GDPR, applying the concepts of privacy by design and privacy by default, in order to give power to the users to handle their data and not gather or distribute unnecessary user data.

5. European IoT National Strategies

5.1 Austria

The digital transformation and the IoT and Services have a huge impact in the society and economy, in the life and work of each person.

IoT Austria - The Austrian Internet of Things Network is a platform, where people, companies and institutions can meet for sharing their knowledge, experiences, technologies, contacts and resources and could start collaborations in order to bring forward the Internet of Things and Services and the Open Concepts spirit (Open Collaboration, Open Organization, Open Knowledge, Open Access, Open Data, Open Source, etc.) in Europe.

Above all stands the conscious and responsible use of technology based on ethical values for the benefit of humans. IoT Austria is based on volunteering work and is not-for-profit - all the events are for public access and free of charge for any visitors [39]. IoT Austria sees in the open source technology for the Internet of Things the decisive basis for future developments. In addition, the organisations aim for the "democratization" of technology, through free access and free use of knowledge, indispensable to the society and the common good as well as the economic development in Europe. IoT Austria takes actively part in open source hardware and software projects and supports the open source projects.

5.2 Belgium

IoTBE VZW - Internet of Things Belgian - is a vibrant expert group and open innovation platform in which research, business & government come together to build a disruptive future. The IoT Innovation Center or IoTIC helps companies in the industry & service sector and the government to tackle the IoT challenges and opportunities [40].

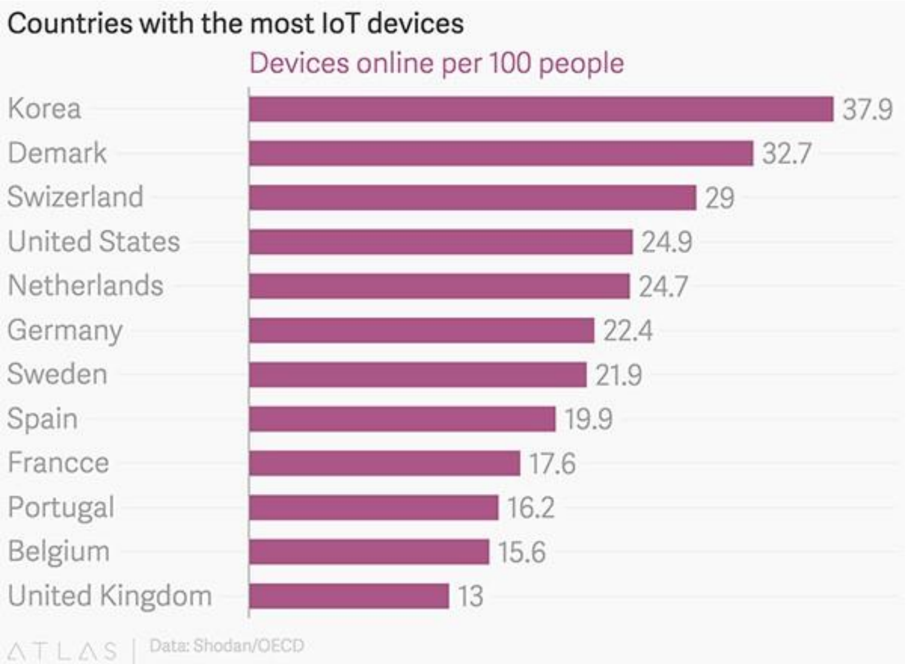

Figure 25: IoT devices deployed in different countries

According to the Organization for Economic Cooperation and Development (OECD) and search engine Shodan, Belgium ranks among the top Internet of Things early adopters worldwide. As an IoT early adopter, Belgium plays a key role in helping the IoT technology go mainstream.

One of the important area is the Brussels High Tech ecosystem. Several companies and start-ups are active in various sub-domains, such as Smart Cities, Smart Building, Telematics, Smart Industries, etc. All the IOT software, hardware and telecom expertise are present in Brussels! IOT incubators, accelerators and fab-lab also help gather and develop all those skills. All major IOT dedicated networks are deployed in Belgium: SigFox, LoRa and of course M2M (4G/LTE), making from Brussels and Belgium a perfect testbed for IoT projects. Moreover, IoT has been declared as one of the Top 3 priorities of the regional plan for IT Entrepreneurship, in the NextTech. Brussels plan voted in 2017 by the Brussels region government.

Belgium supportive government and R&D-friendly tax system intersect to create an attractive business environment and may receive support in the form of subsidies and grants. Generally, there are 5 organization types for R&D activities that are eligible for one or more of Flanders' R&D tax incentives: Global R&D centre, Young Innovative Company (YIC), Contract Research Organization (CRO), Manufacturing company and/or R&D consulting company.

5.2.1 IoT innovation examples

Sensolus: Designs, builds and sells turnkey solutions for low-power long-range networks [150]. They provide a care-free tracking of non-powered assets directly from the cloud. Their technology is extreme low-power as it works for 5 years on a single battery, easy to install and offers a care-free solution to stay in control on assets out there in the field. They have many years of expertise in wireless sensor design, firmware and cloud-based sensor management, analytics and applications. SENSOLUS is one of the 73 partners in the H2020 IoT-01-2016 Large Scale Pilots Project IoF2020 consortium. The project is a powerful driver that has the potential to transform the entire farming and food domain into smart webs of connected objects that are context-sensitive and can be identified, sensed and controlled remotely.

Rombit: Rombit has grown from Flanders' Most Promising start-up (VOKA, Trends, JCI) into an experienced IoT service provider and product engineering firm. Rombit invests heavily in building readymade solutions that closely integrate with the existing customer infrastructure and tools, leading to low friction and high interoperability. The Romcore framework integrates the full chain from legacy hardware and software to IoT sensors, big data processing and analysis and finally a visualisation in the form of desktop and mobile applications. On top of its Romcore platform, Rombit has developed IoT applications ranging from power management for container ships in the Port of Antwerp, medical transport and supply chain management applications, smart city parking systems, to employee monitoring and tracking applications. The Rombit methodology and knack for solving difficult problems have made the company popular within the large industry ecosystem in Flanders and abroad: Rombit has grown to 50 employees in nearly 5 years. Early 2016 it secured the largest series A investment round to date in Belgium. Rombit is one of the partners in SynchroniCity, a H2020 IoT-01-2016 Large Scale Pilot Project delivering a Digital Single Market of smart cities for Europe, enabled by Internet of Things technology. Altogether 34 organizations from public and private, NGOs and academia have joined the forces to realize this goal. Starting in 2017 and continuing until autumn 2019.

Imec's City of Things: Imec's City of Things project aims to bring the intuitive Internet of Things to the city, improving the quality of living for its citizens. Concretely, they are transforming the city of Antwerp (Belgium) into one of Europe's largest smart city laboratories where we put key technologies for smart cities to the test. They bring together user groups, hardware developers, app developers to accelerate the development and implementation of the Internet of Things in the city. Companies can test their innovative IoT applications under realistic circumstances, in a real city

and with real users. When the City of Things project will be running at full speed, there will be 100 gateways spread across Antwerp – virtual gateways for the possibly tens of thousands of wireless sensors worn by local residents or attached to vehicles, the traffic infrastructure or buildings in the city. Today there are already around 20 of these gateways operating, with the remainder gradually being installed. These gateways are genuinely 'open'. This means that anyone can use them to send data or to develop or evaluate smart applications. It also means that the technology is heterogeneous and not based on a single solution or protocol; it understands a whole range of communication standards, such as ZigBee, WiFi, Cellular, LoRa, SigFox and others. But these sensors and gateways are just the first layer. Behind them is an infrastructure for storing data and analysing it in real-time. This infrastructure is technology-neutral and offers an extensive set of tools for converting data into real knowledge. Next to that they are involving the inhabitants of Antwerp and recruiting test panels of users for various applications. Also, the City of Antwerp is part of SynchroniCity (see above).

5.3 Bulgaria

The overall Value at Stake in the public sector in Bulgaria is estimated at $2.8B. It will result from Internet of Everything's (IoE's) ability to help public-sector organizations manage assets, optimize performance, and create new business models. Cisco's economic analysis estimates that 70 percent of that value will come from agency-specific implementations, while 30 percent will derive from cross-agency use cases. The five primary drivers of IoE Value at Stake for the public sector are: 1) employee productivity, 2) connected defence, 3) cost reduction, 4) citizen experience, and 5) increased revenue. More than two-thirds of IoE's Value at Stake for the public sector (69 percent) will be powered by citizen-centric connections (person-to-person, machine-to-person or person-to-machine). Cities will generate almost two-thirds (63 percent) of IoE's overall public-sector value at stake [41].

Table 5.1: Bulgaria's $2.8B public sector IoE opportunity detail [41]

Opportunity	Estimated Value [$M]	Opportunity Area	Estimated Value [$M]
Video Surveillance	$52	Virtual Desktop	$8
Smart Parking	$46	Particulate Monitoring	$11
Smart Street Lighting	$55	Disaster Response	$6
Waste Management	$15	Smart Buildings	$146
Road Pricing	$16	Correction Visits	$2
Public Transport	$23	Bridges Maintenance	$3
Offender Transport	<$1	Fleet Management	$26
Telework	$165	Local Metro	$15
BYOD	$114	Travel avoidance	$145
Connected Museum	NA	Smart Tollbooths	<$1
Connected Learning	$169	Chronic disease	$53
Gas Monitoring	$51	Inpatient Monitor	$2
Water Management	$63	Counterfeit drugs	<$1
Smart Xmission Grid	$150	Cyber Security	$71
Mobile Collaboration	$1,332	Drug Compliance	$4

Considering the specific opportunities of Bulgaria in the energy industry, new opportunities around IoE-enabled smart grid and "smart building" strategies can reduce costs while generating a positive environmental impact. IoE enabled tourism with technologies like mobile collaboration and connected marketing and advertisement can encourage the generation of new revenue streams

for targeted advertisement and provide more choices for users and customers. Bulgaria's agriculture industry has been one of the country's strongest, and is culturally and emotionally woven into the way of living of Bulgarian people. Using smart sensors and other networked and Big Data technologies can help to improve food quality and quantity and ecological control. It can be used to create higher returns for a variety of agricultural products and segments and can open new opportunities for jobs and markets. Smaller countries, which are nimbler and have fewer barriers to change, may provide leading examples for more established economies to follow, showing what can be done with high-level leadership that is committed to improving public services and private sector efficiency [41].

5.4 Croatia

In Croatia, FER is the leading institution driving IoT domain in the country [151]. They are actively involved in FP7 and H2020 IoT projects. On the commercial side, Microsoft is actively promoting IoT and its applications through a series of events.

Awareness of potential benefits of IoT among commercial organizations have increased significantly over the last year. This is demonstrated by companies interested to smarten-up their products and offer connected devices and services, ranging from those related to public lighting and electric energy distribution to agriculture and transport. However, the most widely spread application is fleet management, used rather extensively by enterprises. These applications are not used to monitor locations of the vehicles only, but are integrating a large number of sensors and used to optimize working processes.

Mobile operators in all these countries are also increasingly interested in providing IOT services and entering new markets. The forerunners are the operators with operations in several countries.

5.5 Cyprus

Large-scale state infrastructure projects and PPPs are under consideration for the construction of digital infrastructures in Industrial Areas / Zones for the purposes of establishing cloud computing / Internet services, IoT, Industrial Internet, and Big Data Analytics in both urban and rural areas.

5.6 Czech Republic

The responsible state institution for financing and administrating of the R&D in the Czech Republic is the "Ministry of Education, Youth and Sports" [133]. However, the "Research, Development and Innovation Council" defines strategic visions for the future. In the field of applies research, the "Technology Agency of the Czech Republic" was recently established to streamline the governmental support in the applied research while the "Czech Science Foundation", finances the basic research.

National Research and Innovation Strategy for Smart Specialization (National RIS3 Strategy) represents a strategic document providing efficiently focused support to research, development and innovations areas [134]. As a main activity, National RIS3 Strategy provides efficient focus of European, national, regional and private funds on the most promising sectors of research and business. Building of efficient relationships between academic institutions and the business sector represents a partial goal of National RIS3 Strategy. National RIS 3 Strategy constitutes with a preliminary condition for EU funding programmes for research, development and innovations.

The innovation process in the National RIS3 strategy comprises the following [135]:

- Identifying new customer needs and finding technical solutions to satisfy them.
- Searching for, acquiring and coordinating the management of necessary resources (including research results, if needed) and competences.
- Launching the innovation onto the market so that it is well received by customers and so that the launch takes place ahead of the competition.

Research and development and innovation priorities are identified through the entrepreneurial discovery process (EDP) within National Innovation Platforms [135]. The priority topics for the "Digital economy and digital content" area are given below (for further information on other areas, we refer to National RIS 3 Strategy).

- Development of high-quality infrastructure providing fast or superfast Internet access.
- Support for the development of digital content industries, introduction and utilisation of new technological concepts, (e.g. Support for the introduction and utilisation of new technological concepts such as the cloud, IoT, big data, artificial intelligence and others).
- Ensuring the government's coherent approach to the provision of loans, borrowings and/or guarantees for loans, including development of venture capital financing.
- Support for the development of technological concepts and their application in national economy sectors, (e.g. Internet of Things and cyber-physical systems, robotics, methods and techniques for cybernetics and artificial intelligence (agent systems, service-oriented architectures, learning and self-organising systems, machine perception systems, intelligent robotics), development of new algorithms and analytical tools for working with large quantities of data, tools for working with the Czech language in ICT, digitisation of the distribution system; Adaptation of technological concepts to the needs of national economy sectors, solutions based on the principles of the sharing economy, e-commerce, technological interconnection of digital content, the Internet of Things, assistive technology).
- Cybersecurity, (e.g. Protection of ICT infrastructure and data against attacks, data and network security; Secure data storage and backups; Modern and secure digital communications; Defence against malware propagation; Cybercrime prevention.
- Social impacts of society digitisation
- Research into technology impacts on society and individuals within new creative industries
- Media production.
- Memory institutions

The Internet of Things are incorporated in the "National cyber security strategy of the Czech Republic for the period from 2015 to 2020" [132], prepared by the National Security Authority National Cyber Security Centre.

5.7 Denmark

Through several initiatives, Denmark is supporting the IoT activities and actively addressing the current challenges with digital transition and shared digital standards, while also discussing questions on pilots, public data, architecture and more.

5.7.1 National IoT Standardisation

The Ministry of Industry, Business and Financial affairs requested Danish Standards to produce a roadmap to be used by Danish companies in their digital transition. The document "Roadmap on standards for Internet of Things (IoT)" explains the needs and challenges of Danish companies, as well as the need for standardisation, or information regarding existing standardisation, from an industry perspective [103]. Three IoT engagement themes were the focus of Danish Standards. These themes are expected to play a key role in creating future profits and increased export:

- Automation and robotics
- Smart farming/agriculture
- Smart city

As part of the mapping, several challenges and recommendations were noted within three main areas. Solutions to these challenges must be found in order for Danish companies to fully profit from the use of IoT-solutions. The areas are:

- Interoperability and reference architectures.
- Information security and privacy.
- Small and medium-sized enterprises' challenges.

A primary recommendation by Danish Standards is to actively participate in the work surrounding IoT standardisation in ISO/IEC with a focus on IoT, Smart city and information security. (ISO/IEC JTC1, Joint Technical Committee Information Technology WG 10 IoT, WG 11 Smart City and SC 27 IT Security Technology).

5.7.2 Forum for IoT and Standardisation Committee

Denmark has established a "Forum for IoT" which is financed by the Danish Business Authority. The forum has 75 members and high numbers of attendance (50+) at each meeting. One important aspect of the forum is to communicate knowledge on new standards to Danish companies and organisations.

Recently, a new standardisation committee was established for IoT DS/S-840 IoT following the work in the international committee IEC ISO/IEC JTC 1/SC 41: Internet of Things and related technologies.

5.7.3 Industry Partnership for Advanced Production

As part of the governments' strategic work towards economic growth in Denmark (Danmark i vækst) it is a priority to follow the developments of Industrialisation 4.0 [109]. To support the digital and technological transition of the Danish production companies, the government has created the Industry Partnership for Advanced Production initiative (Erhvervspartnerskabet) [110]. Their mission, in the next 4 years, is to communicate knowledge about new production technologies and their implementation, while giving further support to the transition through multiple open calls with a total amount of 42 Million. DKK.

5.7.4 Research: Internet of Things in Danish Industry

Danish Business Authority developed a business analysis "Connected Opportunities" ("Forbundne muligheder") from October 2015 to January 2016 on the use of IoT by Danish companies [111]. The analysis shows how IoT-technology is used to a lesser or larger extent within 42% of the approached industries and that IoT-technology use is most widespread in-home automation, supply and energy, and finally engineering. Health- and welfare sectors use IoT-technologies the least. Barriers and challenges are also addressed in the analysis. Only few companies have the necessary knowledge to be able to individually cover all aspects of an IoT-solution, therefore, new collaborations across the organisations as well as new partnerships with other companies are necessary. In addition, there is a need for the integration of IoT-solutions in different systems. The empirical basis of the analysis is a questionnaire with 600 responses as well as in depth interviews with more than 30 Danish IoT-experts and companies.

5.8 Estonia

According to "Europe's Digital Progress Report (EDPR) 2017 Country Profile" [122], Estonia is ranked highest with regard to online provision of public services, and are well skilled in the use of digital technologies and use a variety of internet services. Estonia is strong on mobile broadband, but the fixed fast broadband coverage is low. The key challenge is the digitisation of companies.

The Digital agenda 2020 for Estonia declare the general objective [136]: "Estonia will have a well-functioning environment for the widespread use and development of smart ICT solutions. This will have resulted in increased competitiveness of our economy, well-being of people and the efficiency of public administration". The progress will be measured with the following indicators [136]:

- Take-up of 100 Mbit/s or faster internet connections. Starting point (2012): 3.6% and target level (2020): 60%
- Share of internet non-users among 16 to 74-year olds in Estonia. Starting point (2013): 18% and target level(2020): 5%
- Satisfaction with the quality of public services:
    - Among adult population aged in Estonia. Starting point(2012): 67% and target level(2020): 85%
    - Among entrepreneurs. Starting level (2012): 76% and target level (2020): 90%
- Share of ICT professionals in total employment. Starting point: 3% and target level (2020): 4.5%

5.9 Finland

According to a study report made for the Finnish government in 2015 [112], the upheaval brought on by the industrial internet is an opportunity to increase Finnish well-being and productivity and to make Finland an attractive target for investment. The report estimates that if successful, business activities of the industrial internet would bring € 12 billion in investments and 48,000 jobs by 2023. This will be possible only if both enterprises and public players commit to actively promoting the industrial internet. If Finland does not succeed in rapidly advancing to the front line in the industrial internet, productivity, investments, and the number of jobs will continue to decline.

The report draws three possible paths of development for how the industrial internet changes our society, and puts forward 15 concrete measures which can help turn Finland into a brave pioneer in the utilisation of the opportunities provided by the industrial internet.

- Finland's industrial development has been weak in recent years and investments and productivity have been on the decline. The working group estimates that if nothing is done, this trend will continue, and 16,000 jobs will be lost in the coming four-year period.
- A second alternative is for Finnish companies and other players to rapidly utilise the new opportunities offered by technology in their business, in which case we can achieve growth of € 4 billion in investments and 16,000 new jobs.
- If, on the other hand, companies take on the role of key players in platforms and ecosystems of the industrial internet, then according to the working group, growth as high as € 12 billion in investments and 48,000 new jobs can be achieved.

5.9.1 Fifteen measures for reaching the best path

New technologies and innovative solutions can be advanced by, for instance, using five per cent of all public procurements on alternatives that advance the industrial internet. Large companies must also work more in funding growth companies and serving as their partners. In the United

States large companies are behind about 10 % of all capital investments into startup companies, whereas there is very little of this kind of activity in Finland. Capital investments into startup companies should be seen in taxation as a part of the additional deductions made by companies for their research and development activities.

According to researchers, it is the task of government to create favourable conditions for investments and growth through means of new active industrial and ownership policy. It is the task of companies to invest in the development of digital talent and to create growth based on new business opportunities and markets.

5.9.2 Industrial internet

The industrial internet refers to a phenomenon in which both the internal business processes and the products and services that are sold are linked with the internet. This requires that all matters and objects related to production and service processes should have a digital identifier which passes on data to the different players of delivery and value chains. A fixed connection to the internet allows for predictable operation.

5.9.3 Internet of Things

Even though the first operational implementation of the Internet of Things was presumably developed in Finland in 2001 [113], it still seems like there is a great emphasis on the Industrial Internet (or Industrial Internet of Things), as shown by the active and industry-driven Finnish Industrial Internet Forum (FIIF) [152]. However, it seems like there initially has been a smaller interest and for consumer-driven IoT, as the kind of services needed for citizen-focused Smart Cities. This might be seen as quite typical for Finnish research and development in general, which tends to be focused on B2B solutions rather than on developing services for consumers.

5.10 France

France has been actively supporting the development of the IoT industry through different initiatives, emerging from different organisations and covering different focus.

5.10.1 National Industrial Strategy

The French Ministry of Economy launched in 2013 a plan toward a **"New Industrial France" (Nouvelle France Industrielle)**. The main objective of this plan was to improve French Industry competitiveness (Industry share as part of the GDP dropped significantly over the 2000-2010 decade, from 23 to 19%, it remained around this value since). A side objective was to create jobs, France having lost over 2 million industrial jobs in the last 30 years.

Although this plan didn't target specifically the internet of things, it covered several topics related to the IoT (among the 34 topic of the plan), such as: **Autonomous Vehicles, Smart Textiles, Connected Objects, Future Factories**; and related topics (BigData, Cloud computing). The plan main action focused on legal and fiscal means (incentives) and direct public funding (through the "plan investissement d'avenir") with a total of 3.7 billion EUR of public investment.

The plan evolved in 2015 with a tighter focus on 9 strategic domains, seeing a stronger focus on IoT: among the 9 selected domains figure **Smart Objects, Digital Trust and Data Economy**. this French government initiative has defined five priorities:

- **Technology development,** with both project funding and the development of a technological test bed platform to develop and validate technologies.
- **Support to adoption**, with dedicated actions to encourage SMEs to adopt new technologies and practices.

- **Employee training,** with the development of dedicated courses on key technologies.
- **International cooperation**, especially at European level.
- **Visibility,** with the launch of showcase initiatives to improve the visibility of French industrials.

The focus of the French Government on the IoT increased further with a more recent (December 2016) **"Roadmap" fully dedicated to the IoT**. The roadmap is an extension of the Nouvelle France Industriel plan, with ties to the three domains of Smart Objects, Digital Trust and Data Economy. It defines 4 axes and 11 objectives to promote the development of the IoT in France. The goal of the roadmap initiative is mainly to present and coordinate various existing initiatives from the different organizations.

5.10.2 Telecommunication Regulations

The French telecom regulator the ARCEP published in 2016 a white paper on the Internet of Things following a public consultation on the topic. The objectives of the white paper were to identify the key challenges and to prepare the set-up of targeted tools to support the development of the IoT in France.

The five identified challenges are:

- Ensuring connectivity through multiple resilient technologies and a low cost.
- Providing the needed spectrum frequencies to the development of the IoT.
- Ensuring an open market
- Contributing to public trust into industrial and their handling of personal data
- Support the emergence of a dedicated IoT ecosystem.

Three tools are considered to support the IoT development:

- A dedicated initiative to support experimentations by industrials and start-ups
- A portal gathering the current usage of unlicensed spectrum frequencies by the different stakeholders
- The set-up of dedicated events to follow the development and needs of the industry.

5.10.3 Local Industry Strategy

The French support to the IoT also goes through more local initiative targeting local ecosystems of industrials, academics and start-up. This goes through the set-up of clusters ("pole de competitivité") set-up in 2010.

The clusters follow the "triple helix approach" principle [53] **mixing together academic research, leading private companies, startups and local ecosystems**. The objective of this approach is to facilitate technology transfer between academics and businesses while taking into account the user needs by grounding research and developments in local ecosystems.

The following clusters can be mentioned as having dedicated actions on the IoT topic:

- **System@tic**: located in the Paris area and focusing on telecom, future factories, and trust and security applications. The cluster also has dedicated applications in automotive, transport and energy verticals.
- **SCS (Secured Communicating Solutions)**: located in Sophia-Antipolis and focusing on Microelectronics, Telecommunication and Software.
- **Minalogic**: located in Grenoble and focusing on Micro and Nanoelectronics, Photonics and Software.
- **Images et Réseaux (Images and Networks)**: located in Rennes and focusing on Network Infrastructures.

- **Cap Digital**: located in Paris and focusing among other topics on Robotics and IoT, with a stronger focus on consumer applications.

5.10.4 Focused actions targeting start-ups

Finally, French also has an initiative dedicated to supporting Start-up companies called “La French Tech”. The initiative provides support (including financial support) and has a strong focus on visibility (with promotion in international events).

The initiative is structured through local bindings (active in most of large French cities and regions) and through a thematic binding. One of the Thematic Networks is focusing on the Internet of Things and Manufacturing.

The thematic network provides networking opportunities between the different start-ups focusing on IoT and aims at creating a common roadmap of actions to strengthen the growth of the industry.

5.11 Germany

In 2014 Germany adopted the Digital Agenda for 2014-2017, and in 2016 the Federal Ministry for Economic Affairs and Energy presented the *Digital Strategy 2025* [122]. The German government has already implemented a number of important projects and measures in the context of the Digital Agenda, and has expanded the scope of future areas of involvement [143]. The federal programme for promoting broadband deployment has been set up, over one hundred specific practical examples of Industry 4.0 were introduced at the 2015 National IT Summit, the inter-ministerial programme Smart Networks Strategy was initiated, and the funding programme Digital Technologies for Business was started. In addition, SMEs are assisted in the digitisation process by setting up "Mittelstand 4.0" Centres of Excellence.

The strategy defines ten steps towards the future [143]:

- Creating a gigabit optical fibre network for Germany by 2025.
- Launching the "new start-up era": Assisting start-ups and encouraging cooperation between young companies and established companies.
- Creating a regulatory framework for more investment and innovation.
- Encouraging "smart networks" in key commercial infrastructure areas of our economy.
- Strengthening data security and developing informational autonomy.
- Enabling new business models for SMEs, the skilled craft sector and services.
- Utilising Industry 4.0 to modernise Germany as a production location.
- Creating excellence in digital technology research, development and innovation.
- Introducing digital education to all phases of life.
- Creating a digital agency as a modern centre of excellence.

To turn the Digital Strategy 2025 into reality, an Action Programme on Digitalisation is developed, and defines twelve points on the digital future [144]:

- Promoting digital hubs in Germany.
- Accelerating digitalisation in SMEs.
- Expansion of Gigabit networks.
- Making private investments in digital technology easier.
- Securing digital value creation networks.
- Mobilising more venture capital.
- Driving forward digital communication and eGovernment, reducing bureaucracy.
- Digitising the energy transition.

- Digitising the healthcare industry.
- Strengthening FinTech in Germany
- Moving forward on digital mobility
- Enabling more sharing through a social sharing economy.

5.12 Greece

According to "Europe's Digital Progress Report (EDPR) 2017 Country Profile" [122], Greece features wide availability of fixed broadband but take-up is progressing slowly in connectivity (fixed broadband, mobile broadband, broadband speed and prices). The price remains relatively high and the transition to fast broadband connections is slower than in other EU countries. However, they are more actively using internet for online content and video calls, but low performance in digital skills risks acting as a brake on the further development of its digital economy and society. In integrating digital technology, companies use social media at the level of EU average, but do not use more sophisticated technology such as cloud services and electronic invoices.

The report "ICT Adoption and Digital Growth in Greece" [131], look into (among other things) the strategic framework and digital priorities in Greece: "The Ministry of Administrative Reform and e-Governance presents the main vision of the Greek e-government strategy for the period 2014-2020 which can be specified as follows: "Greece aims to build a more efficient, transparent and accountable administration, through the use of ICT and the support of the necessary governance and monitoring mechanisms, while maximizing constituent satisfaction, increasing participation and recovering confidence by offering constantly enhanced electronic services and promoting a new digital culture", driven by the fundamental principles: Interoperability, compliance or justification, integration, conservation - non recurrence, single data entry, feasibility - sustainability, transparency - confidence recovery, e-accessibility, security - Privacy, and citizen participation. In order to develop e-government and efficient ICT penetration within the public sector, the strategic targets for the period 2014 - 2020 are [131]:

- Modernization of public administration.
  - Simplification of procedures through the use of ICT.
  - Electronic management of documents - digitalization of procedures.
  - Single use of the resources of the public administration.
- Reconnection of citizens with public administration.
  - Unified relations management among the state, the citizens and the businesses.
  - Creation of a single point of contact with the public administration.
  - Citizen authentication.
  - Digital inclusion and digital literacy.

MIT Enterprise Forum Greece (chapter of the global MIT Enterprise Forum), was established in 2013 as a non-profit association by a group of experienced entrepreneurs and business professionals with strong engineering backgrounds [130]. The forum informs, connects, and coaches technology entrepreneurs enabling them to rapidly transform ideas into world-changing companies. Events like Internet of Things - Technology that matter, Start Smart Greece, and Enterprise Forum - making Greece a Technology Hub by 2021 has been arranged. Their goals is to be game-changer for Greek entrepreneurship and add significant value to the troubled economy.

In 2016 Athens International Airport surpassing 20 million passengers, which include more traffic and greater environmental impact [129]. An ongoing pilot project for air quality monitoring, aircraft location, analysis and reporting where started and led by Ex Machina, a Greek company specializing in IoT. LoRa communication is used for real-time sensor data transmission and device

control/orchestration, and GPRS is used for secure device management, over the air firmware upgrades, configuration of firmware parameters and the bulk upload of sensor data as back-up.

The first Greek Narrowband Internet of things (NB-IoT) smart city pilot was implemented in Patras 2017 [128]. The pilot are financed by the Deutsche Telekom Group's subsidiary COSMOTE, and developed in cooperation with the municipality of Patras. The joint project is a an example of the infinite potential the IoT can bring to urban areas, and will offer the citizens and visitors smart parking and smart lighting solutions in selected locations in the city centre. As part of the NB-IoT pilot implementation in Patras, specialized smart parking sensors have been installed, and the car drivers will be immediately informed about free parking space locations and how to get there, through a specialized mobile application. The installed smart lighting systems will be adjusted to different light intensity levels according to the season and time of the day, reducing electric power consumption by up to 70%.

5.13 Hungary

According to "Europe's Digital Progress Report (EDPR) 2017 Country Profile" [122], Hungary performs well on connectivity (fixed broadband, mobile broadband, broadband speed and prices), due to the wide availability of fast fixed broadband and 4G as well as to the increasing broadband take-up on fixed networks. Mobile broadband take-up is, however, not yet accelerating. The businesses are increasing the use of social media, cloud, digital services and commerce. But business sector is not exploiting the opportunities offered by digital technology as much as the other EU countries. Hungary plan to access and leverage funds under the European Commission’s Investment Plan for Europe (EC IPE, "Juncker plan"), for the development of digital technology as well as transport and energy infrastructure [123].

The Hungarian Academy of Sciences (HAS) is the most important learned society in Hungary [124]. Its mission is distribution of the results of science, supporting research and representing the scientific community. It has 11 research units (eight for life sciences and three for social sciences) and runs 15 research institutes.

The Hungarian IoT Creativity Meetup founded in 2015, addresses electronic developers, software developers, embedded programmers, mobile phone programmers, product developers, and investors creating concepts and ideas of IoT applications [125].

Some examples of companies addressing digitalisation and communication are T-Systems Hungary and Telenor Hungary. T-Systems, owned by Magyar Telekom, is the largest Hungarian service provider that can cover the entire range of ICT technologies, using the latest technological advances and business trends [126]. Telenor Hungary offer customers, such as unlimited mobile internet, internet security solutions, and special needs for which the company has developed customizable products, from mobile management tools to IoT solutions [127].

5.14 Ireland

Ireland supports the development and growth of the necessary infrastructure and services that enable the IoT functionalities. The efforts are mainly made by the national and government initiatives that are described below, but there are a lot more research institutes and companies based in Ireland that either develop IoT oriented products and services, or do research on the evolution of IoT.

IDA Ireland [55], is a non-commercial, semi-state body promoting Foreign Direct Investment into Ireland through a wide range of services. IDA reports that Ireland is “the natural choice” of companies that develop IoT products and services. Ireland has the infrastructure and the

knowledge base to support the collection, the connection and the transformation of data that is needed in an IoT ecosystem. It has a successful industrial heritage in semiconductors and microelectronics. Intel's IoT chip, the Quark chip, was designed in Ireland, proving that the country has the expertise needed for the production of a globally recognised IoT chip and platform. Furthermore, it has the seventh fastest broadband speed in the world, making the country a perfect location for data centres. It also provides the option to test and trial access to the radio spectrum, while Vodafone's M2M technology in Ireland is powering connected solutions in everything from airlines to power feed. Last but not least, Ireland has some of the most-established data analytics centres, such as those by Accenture and SAP but also Insight Centre for Data Analytics, the biggest publicly funded data analytics research centre in Europe.

Pervasive Nation [54] is Ireland's IoT testbed. It is operated by CONNECT, the Science Foundation Ireland Research Centre for Future Networks headquartered at Trinity College Dublin, the University of Dublin. The initiative's main objective is to provide a large-scale testbed to scientific groups from the research and the industry domain for experimentation and innovation. The testbed uses Low Power Wide Area (LPWA) technology, software defined radios (SDR) and Application Enablement Platform (AEP) technologies. This testbed is particularly suitable for connecting small devices installed in not easily accessible areas, which depend on batteries and have restricted data rates.

Another active non-profit initiative in Ireland is the Open & Agile Smart Cities initiative (OASC)[56]. Its objective is to create a Smart City market and launch the use of a shared set of methods to develop systems and make them interoperable across a single city as well as between multiple cities. OASC provides the network for cities all over the world to share best practices, compare results, and avoid vendor (and city) lock-in while advocating for de facto standards.

5.15 Italy

In 2016 Italy experienced a substantial growth of the IoT market, which was worth 2.8 billion euros, 40% more than the previous year [39], driven by both consolidated applications that leverage mobile connectivity (€ 1.7 billion, + 36%) and those using other technologies (€ 1.1 billion, + 47%). This boost was mostly due to public policies requiring the installation of at least 11 million gas smart meters by 2018.

In addition to gas smart meters, Smart Cars drove the market, with 7.5 million of circulating connected cars: these two areas alone account for more than half of the IoT turnover. The two mentioned areas, together with IoT deployments in buildings (Smart Building), especially for security purposes, make over 70% of the total market value.

In 2016 the number of "objects" grew too: 14.1 million objects are now connected by mobile network (+ 37%), without counting the objects that use other communication technologies, such as the 36 million electrical smart meters connected through PLC connected (Power Line Communication), the 1.3 million gas smart meters that communicate by radio frequency, and 650,000 smart luminaires connected via PLC or radio frequency.

The main segment of the IoT market (34% of the total) consists of Smart Metering and Smart Asset Management in utilities, where the regulatory requirement for gas meters has led to an explosion of IoT solutions: the market has grown from 500 million euros in 2015 to 950 million in 2016 (+ 90%). At the second place (20% of the total) in the market there is the segment of the Smart Car, which has grown by 15% and reached 550 million euros, despite the reduction of the prices for GPS/GPRS box prices, which in absolute terms weakens the market value growth. The third largest share in the Italian market belongs to the Smart Building solutions (510 million euros, 18% of the market), an area that grew by 45% compared to 2015, particularly driven by the

supply of security-related solutions in buildings. Smart Logistics solutions for transport occupy the next spot (250 million euros, 9% of the market) used for fleet management and satellite burglar control. Smart Home is worth 185 million euros and 7% of the market (+ 23%), with a strong prevalence of security applications [39].

Other domains have still to express their potential, in particular, three areas should be monitored: Smart City, whose potential is still widely unexpressed, Retail, where IoT could serve as a collector of data for customers' profiling and behavioural advertising within the stores, and the Smart Agriculture, where the IoT offers opportunities not only in terms of product traceability, but also in the management of agricultural activities.

The delay of Smart City applications is noteworthy in the IoT market. Their value is estimated in 230 million euros, or 8% of the total market's turnover. In the Smart City domain IoT is deployed in limited areas - such as public transport with 200,000 remotely monitored vehicles and intelligent lighting with 650,000 lighted-light poles [39].

In the near future, a further acceleration of the IoT market is expected for the Industrial IoT, which is supported by the incentives provided in the National Industrial Plan 4.0, which will include in the next four years investment in research and development and tax incentives for companies investing in technologies and projects to support the Fourth Industrial Revolution.

Key points of the Plan [44], incorporated in the Budget Law 2017 [45], are:

- A public investment of about 20 billion euros;
- A super and hyper amortization of 140% and 250% for newly acquired capital goods supporting the technological and digital transformation of the production processes;
- A 50% tax credit on R&D investments;
- Incentives on investments in start-ups and innovative small businesses.

5.16 Latvia

According to "Europe's Digital Progress Report (EDPR) 2017 Country Profile" [122], the shares of fast broadband subscriptions are increasing and the delivery of public services improving in Latvia. The businesses are exploiting the technology in a limited way.

The Latvian "Information Society Development Guidelines 2014 - 2020" define an overall goal [137]: "To provide an opportunity for everyone to use the possibilities offered by ICT, to develop an knowledge-based economy and to improve the overall quality of life by contributing to the national competitiveness, and increasing an economic growth and job creation". Seven action directions for the policy planning period 2014-2020 are proposed [137]:

- ICT education and e-skills.
- Widely available access to the internet.
- Advanced and effective public administration.
- E-services and digital content for public.
- Cross-border cooperation for Digital Single Market.
- ICT research and innovation.
- Trust and security.

5.17 Lithuania

According to "Europe's Digital Progress Report (EDPR) 2017 Country Profile" [122], Lithuania performs particularly well in connectivity (fixed broadband, mobile broadband, broadband speed and prices) and the integration of digital technology. The internet users are active online in using

new services over mobile, like payment instruments, mobile e-signature, car parking, and banking services. Concerning the digital public services, Lithuania is continuing its progress.

The purpose of the Lithuanian Information Society Development Programme for 2014 - 2020 Digital Agenda is to define the goals and objectives of the information society development with a view to maximising the economic advantages provided by information and communication technologies (ICT) [138]. Primarily the Internet as a very important tool for economic, social and cultural activities, enabling the circulation of advanced electronic services, work, access to entertainment, social interaction and free expression of opinion.

The strategic goal of the Information Society Development Programme is to improve the quality of life for the population and business environment for the companies through the use of opportunities created by the ICT and, by the year 2020, to achieve in Lithuania at least 85% of Internet usage among the total population, and 95% of high speed Internet usage among the businesses [138].

5.18 Luxembourg

Luxembourg has undertaken an ambitious economic diversification strategy in respect of the digital sector [122]. The strategy for the digital sector is multidimensional, embracing education, economy, public services, and grouped under an umbrella initiative named "Digital Luxembourg" [141]. One of Luxembourg's strongest side is the IT infrastructure. Digital Luxembourg facilitate collaboration like regular meetings for players to discuss current needs and work on new opportunities for the ecosystem. The players receive regular updates on the government's broadband strategy, and topics like 5G pilot projects or blockchain developments are also addressed. The key objectives regarding the infrastructure are [141]:

- Keep players updated on the government's ultra-high-speed broadband strategy.
- Discuss innovative technologies and their potential for the local ecosystem.
- Identify new areas of infrastructure development for the country.

The key objectives regarding digital innovation ecosystem are [141]:

- Facilitate start-up creation and access to funding.
- Bridge the gap between innovation, research and the economy.
- Create physical space for innovation and entrepreneurship.
- Maximize the contribution of the digital economy to growth by encouraging multi-stakeholder co-operation.

Digital public services to achieve better service to the citizens involves multiply the channels via which citizens can interact with the government, providing easy-to-use and efficient digital services, simplifying procedures and the use of electronic signatures, and fostering transparency and innovation by making public data available and encouraging its reuse [141]. Investment in IT security to ensure highest security standards of the government's IT systems.

5.19 Malta

Digital Malta is the national information communication technology strategy for 2014 - 2020, i.e. a policy document with the following vision [142]: "Malta will prosper as a digitally-enabled nation". Digital Malta puts forward a suite of 71 actions for ICT to be used for socio-economic development, which will make a difference in areas such as the economy, employment, industry and small businesses, and how it can be used for the good of the country, empowering citizens and transforming government. The actions are categorized within the following strategic themes [142]:

Digital citizen, Digital business, Digital government, Regulation/legislation, Infrastructure, and Human capital. A number of goals have been prepared for each of the strategic themes, and define the desired outcomes and determine where effort should be directed.

5.20 The Netherlands

The Dutch economy is doing very well and is among the world's top 10, with leading sectors that can compete on a global basis. For example, the Dutch industry is particularly strong in providing tailor-made work based on an intensive customer relationship, but it certainly has excellent companies in mass production as well. In the area of digitisation, the Netherlands has numerous companies at the forefront. But behind this leading group there is still a world to be captured. A survey has shown that a significant number of entrepreneurs are still relatively uninformed about the upcoming digital revolution and its implications for their business.

This is consistent with the figures from the World Economic Forum. The Global Information Technology Report 2014 shows that while the Netherlands is doing extremely well in ICT, the adoption of new technology can be improved. It can also be noted that ICT is being used more by companies in their contacts with consumers than for business to business transactions. The survey and the many workshops that have been organized show that entrepreneurs see a variety of challenges. Two challenges can be singled out: (1) how can companies collaborate effectively and are they organized in chains and networks that make optimal use of data? and (2) how do companies develop new Smart business propositions with the deployment of new and state-of-the-art technology and knowledge?

The Dutch government is very active (e.g. Netherlands Enterprise Agency (RVO.nl)) and encourages entrepreneurs in sustainable, agrarian, innovative and international business. It helps with grants, finding business partners, know-how and compliance with laws and regulations. The aim is to improve opportunities for entrepreneurs and strengthen their position. This Agency works at the instigation of ministries and the European Union. Netherlands Enterprise Agency is part of the Ministry of Economic Affairs. The organization has been in existence since 2014 and is the result of a merger between NL Agency and the Dienst Regelingen. Netherlands Enterprise Agency focuses on providing services to entrepreneurs. It aims to make it easier to do business using smart organisation and digital communication. The Agency works in The Netherlands and abroad with governments, knowledge centres, international organisations and countless other partners.

One of the programs of the Dutch government which is supporting IoT innovation by giving grants and subsidy is called PPS (formerly TKI). In the Top Consortiums for Knowledge and Innovation, public and private parties collaborate in projects research and innovation. Nine top sectors are involved: Agriculture & Food, the Chemical Industry, the Creative Industry, the Energy Sector, High Tech Systems and Materials, Life Sciences & Health, Logistics, Water and the Horticultural and Starting Materials sector. The Dutch government encourages cooperation between entrepreneurs and researchers within the TKIs, with a bonus of 25 per cent on top of the private contributions to research organisations. This pertains to long-term collaboration projects and TKI-relevant research contracts between companies and universities, the Dutch Organisation for Scientific Research, the Royal Netherlands Academy for Arts and Sciences, the Netherlands Organisation for Applied Scientific Research, the Agricultural Research Service, the Large Technological Institutes and universities of applied sciences. As an extra stimulus, SMEs receive a bonus of 40 per cent for the first € 20,000 in private contributions to a research organisation in collaboration projects. The PPS bonus is allocated to the TKIs, which also determine what the bonus will be used for. This involves new public-private collaboration projects in the field of research and development, or the stimulation of innovation activities that are mainly aimed at increasing the involvement of SMEs in R&D.

5.20.1 Automotive and Transport

The 'ITS plan The Netherlands 2013-2017' aims to provide better real-time traffic and warning information and the introduction of eCall. Also, a number of pilots are conducted in the Netherlands under the FREILOT project, for example in Helmond with connected trucks that gain additional information about traffic lights they approach or even get priority at some traffic lights to increase traffic efficiency. This paragraph focuses on applications in cars and transport systems.

5.20.2 Industry4.0

The Dutch Action Agenda Smart Industry stresses the importance of strengthening the foundation of knowledge, skills and ICT parameters and it carries out research programme aimed at the development of software tools, with a view to chain cooperation, standardization and interoperability, and building on a robust and secure ICT infrastructure for Smart Industry.

5.20.3 Smartcity

In the Netherlands, there is a network of about 100 air quality measuring stations that are spread throughout the country. However, with the advent of cheaper sensors and programmable hardware modules it is now possible for people to have access to measurement equipment themselves. In a project in Amsterdam a Do It Yourself 'Smart Citizen kit' for air quality measurement is offered to hundreds of people. The system, based on Arduino and open source software, includes sensors that measure humidity, noise, temperature, CO, NO_2 and light intensity in a neighbourhood. Once the kit is put together, the sensors are placed outside windows or on balconies and connect to the internet using Wi-Fi. The data is collected on a central server, creating a fine-grained network of (citizen owned) pollution sensors. The 'Smart Citizen' project is an example of how IoT, due to cheaper sensors and the availability of communication networks (using people's Wi-Fi), can help citizens to be better informed and to actively participate in their community.

5.20.4 Healthcare

Long-term illnesses In the Netherlands (with a population of 17 million) there are over 5 million people with some chronicle illness, of which approximately 50 percent need some form of medicine, care or attention on a regular basis. It is to be expected that most of those will in the future be aided in their daily lives using IoT-technology, in the form of both sensors monitoring their specific condition, and smart technology to streamline medicine intake.

Examples include Smart Wireless Pill Boxes that remind patients to take their medicine based on the prescription, for example using audio-signals, connection to a smartphone-app or SMS. 'Smart injection tracker' for diabetes patients (approximately 800.000 in the Netherlands) that connects insulin pens to smartphones using Bluetooth. The application collects the data and forms a database, so that injection history can be accessed later and can be shared with the doctor if needed. And wireless heart monitors for arrhythmia patients (around 300.000 patients in the Netherlands) that collect and store data of the heart (ECG) and send it to mobile external monitor device.

5.20.5 Tourism

Besides facilitating to its residents, cities facilitate many visitors from outsides. IoT is bringing new features to allow this to happen. Personalised and real-time tourist information, based on, and adapted for, the needs of a specific tourist, can make a city attractive. The City of Amsterdam plans a pilot "iBeacon and IoT Living Lab" in 2016/2017 that uses Bluetooth based iBeacons for personalised direction information combined with other information on your smartphone. The plan is to create a zone in which the application will guide tourists and users to relevant locations, using points of interest and location information of the user. In the future dynamic (real-time) signs can

be programmed to show personalised location of special events, public transportation, or other relevant information. Ideas are for example ‘Pointsigns’ that rotate to show visitors the way to go. The signs are programmable and use internet connectivity (using Ethernet or wireless connectivity using for example LTE). This project gives an idea what personalised dynamic road-signs might look like in the near future.

5.20.6 Industry

The Netherlands has a major initiative on industry4.0 called SmartIndustry started by joint collaboration between TNO, the Ministry of Economic Affairs, VNO-NCW and the Chambers of Commerce.

The “Smart Industry, Dutch industry fit for the future” report describe potential threats such as hacking and information theft, both positive and negative aspects of internationalization and standardization. The resulting Dutch Action Agenda Smart stresses the importance of strengthening the foundation of knowledge, skills and ICT parameters by development of technical solutions, business models and forms of cooperation that simplify the exchange and use of data.

The ambition of Smart Industry is a strong Dutch industry that grows and creates jobs. The digitisation of industry offers the Dutch business community great opportunities to remain competitive in a new era of global competition. The Action Agenda supports the business community in that ambition. The Action Agenda is an enhancement of the current Dutch top sector policy and the Technology Pact. The aim is to make the industry more competitive through faster and better utilisation of the opportunities ICT has to offer. Three key pillars: capitalising on existing knowledge, accelerating in Field Labs and strengthening the foundation.

5.21 Poland

Approximately 310,000 cars, trucks, and other machines belonging to Polish organizations were monitored by about 300 companies in 2014. Given that the potential corporate market in Poland probably ranges from 700,000 to 1 million vehicles, agile fleet management providers have significant room for business development. One benchmark is the Benelux market, where 90% of the fleets of companies owning 100 or more vehicles were monitored in 2011.

Finder, which belongs to TomTom Telematics group, is one of the leading end-to-end providers of enterprise fleet-management systems. Following its October 2014 merger with AutoGuard, which was the second-largest company in the market, Finder now monitors approximately 70,000 assets deployed by some 7,000 customers.

PEKA, or the Poznan Electronic Agglomeration Card, is one of the most impressive Smart City projects. Owners of a card can use it as a ticket for public transport, to pay for parking, or to borrow a book from the public library. The card implements a solution developed by AMG.net and a communications layer delivered by Orange. Cards can be recharged at more than 250 points, and some 4,000 validators with touchscreens have been deployed citywide.

Virtual Warsaw, a $15 million project to install beacons in the Polish capital, launched in 2014. As part of its PoC, Polish start-up Ifinity installed a beacon system for the blind and visually impaired. The project and the city of Warsaw were among five winners of the Mayors Challenge organized by Bloomberg Philanthropies. The prize included $1.25 million, which was added to the project's budget, most of which was otherwise provided by the EU. Ifinity is also implementing the same beacon navigation solution in Doha, Qatar, for Mada, an education center for the disabled. The company has opened an office in Doha, and is participating in several PoCs in the Smart City Doha project.

IAB Poland reports that only 11% (2015) of internet users have met the term "Internet of Things". Rarely makes technology or industry visible to average users, even if they use a production solution.

“Even in 2014, the value of IoT investments in Poland amounted to USD 2 billion, but in 2018 it will amount to over USD 3.7 billion and in 2020 it will amount to USD 5.4 billion. This is the value of the entire IoT ecosystem - not just endpoints, sensors or meters - but also software, IT and telecommunications services, or IT infrastructure. We estimate that by 2020 IoT spending will grow at an average annual rate of 20.8%, " says Jarek Smulski, IDC analyst.

The main activities in the field of the smart cities in Poland are on the following areas:

- ITS (Intelligent Transportation System);
- smart metering
- Intelligent urban monitoring,
- An urban information system
- Smart lighting

Example are as following:

- 60% of street lighting in Gdansk is controlled by the intelligent CPAnet system. (brings 250 thousand. zł savings per year). The system based on M2M data transmission in Orange Poland
- The Municipal Heat Engineering Company in Olsztyn supplies over 60% of Olsztyn's flats and institutions with heat. The project has introduced current automatic reading of all heat meters and water meters used in this company.

In addition to existing cities activities there are initiatives towards becoming the smart city, by deploying the concept from scratch such as **Warszawa Modlin Smart City**. Modlin Fortress (rebuilt will 650 thousand square meters) - Europe's largest convention centre, hotels, shopping centre, the university, museum, residential lofts, resorts, shopping centres, medical centres, wellness centres, golf courses, offices. The cost of the investment amounts to nearly 1.5 billion zlotys. The Modlin fortress will soon become a smart city - a multifunctional facility with the smartest and largest congress center in Europe. The final investment project is expected to be completed by 2018.

Smart homes market [78] solutions are considering that Internet users - 77% (2015) use home Wi-Fi (2015). Use of this technology has wide appliances, as 86% (2015) of its users use wireless devices to support more than one device (2015). Among the expectations of the most advanced IoT products are energy savings (44%) (2015). Wearables Personal items, items and accessories IoTs are as popular as building automation - they are owned by a few percent of the surveyed. About 40% of Polish internet users have equipment that is available in different IoT ecosystems, and another 50% would use such devices as they could.

Well known worldwide Polish manufactures of the home automation systems are Figaro [79] from Poznań, with more than 90 percent of system customers come from outside Poland (2014), and Estimote, Inc. indoor location with Bluetooth beacons and mesh [80].

Smart transport applications are represented by Cloud Your Car that has created a GSM / GPS sensor with sensors in the lighter socket of the car, combined with a cloud and a user interface in the form of smartphone applications and Jarosław Smulski IDC is estimating that “the market for fleet monitoring solutions will be the fastest growing segment of IoT in Poland in the coming years. Its value reaches $ 379 million in 2018”

The idea of the Smart Campus laboratory in Poland is currently being developed in the project "Integrated Laboratory for Operational and Simulation for Green AGH Campus" at the AGH campus in Krakow. This is a project focusing on the development of energy saving technologies and ecology (monitoring of the collection and generation of electricity for individual dormitories, intelligent control and lighting in the campus). The goal is to build a modern, intelligent technological infrastructure for research and development on the management, quality and efficiency of electricity.

The Smart Energy applications are represented by major players on the market that are in the process of the deployment of the Smart Meters (AMI). The major players in the field are Tauron, Polenergia, Enea, Energa, RWE and few other. As an example, TAURON customers are the first in Poland to observe real-time energy consumption of individual devices at home or office. TAURON has released a feature that enables remote activation of the wireless communication interface in Smart Meters. This allows current energy consumption data to be sent directly from the AMI electricity meter to the home appliance (HAN).

The main IoT clusters in Poland are Polski Klaster Badań i Rozwoju Internetu Rzeczy [81] and IoT North Poland - (regional Digital Innovation Hub related to Internet of Things [82].

5.22 Portugal

The TICE.pt [63] is a ICT Portuguese cluster that aims to agglomerate the national IoT market and establish Portugal as a reference in terms of technology and international scientific excellence. It is constituted by the formation of several working groups with the objective of improving the network among the partners, identifying areas of work and promoting projects. These groups are: Software, Embedded Systems, Multimedia and Networks, 5G and IoT. The IoT working group have the goal to stimulate the cooperation between the national actors of ICET (Information, Communication and Electronic Technologies) with specific focus on IoT applications.

There are some initiatives and projects in Portugal that are financed by the European Commission and also by the Portuguese state. One of these projects is PROTEUS [64] that has the goal to develop an intelligent sensory system for real-time monitoring of physical and chemical parameters of water. Performed through an intelligent integration of chemical sensors based on carbon nanotube, MEMS based physical sensors together with a cognitive engine providing on the fly re-configurability tested in the context of water monitoring via deployment in the city of Almada (Portugal) water network. This project is funded under the H2020 program for research of the European Commission and have as stakeholders Unparallel Innovation Lda (an IoT tech provider and developer), SMAS de Almada (an innovative water municipal public company) and the UNINOVA (RTD on advanced micro-electronics and System-on-Chip).

There are several IoT pilot areas that are targeted by Tice.pt such as IoT hubs, water management, urban mobility, smart city initiatives, agrifood, monitoring and autonomous driving, health, energy and wearables:

- Development of services capable of making the urban mobility network efficient is the objective of the project TICE.mobilidade [65] (Mobility System User Centered). This project brings together several entities from this sector and several Portuguese Universities in order to the development of a digital platform that allows users to access mobility services, combining mobility, management of urban spaces, shared information and power optimization.
- The Competence Center for Future Cities [66] is a project that aims to guarantee multidisciplinary work with teams from different areas, through the cooperation with local and international companies, government agencies and international scientific and research institutions. With a co-financing by the FP7 Future Cities project and through a partnership

between the City of Porto and the University of Porto, allows the strengthening of research and the transfer of knowledge to the Portuguese industry.

- Innovation in the agrifood sector is a unique initiative carried out by the Centro de Frutologia Compal [67]. Privately funded by the Sumol+Compal S.A (a Portuguese food and beverages company) that itself in partnership with Terra Pro Technologies (a technology and services provider) and several other entities of agricultural and fruit sector, business and associations that includes research initiatives, training and awareness to enhance and promote Portuguese fruit at several stages of production, processing and consumption.
- Veniam [68] is a project in the car sector of the Veniam company in cooperation with the city of Porto, University of Porto and University of Aveiro that use hardware and software capabilities to deliver fully managed services and data on a network of connected vehicles. Some of these services are expand wireless coverage in cities, bring high-definition data from vehicle to the cloud, collect terabytes of urban data for smart city applications and delivers robust wireless networks for industrial environments.
- The Centre for Nanotechnology and Smart Materials [69] provides R&D engineering projects to increase the production of innovative smart materials and device in cooperation with CITEVE, CTIC, University of Porto, University of Aveiro and University of Minho and funded by Portuguese S&T Centre with support funds by National Science Foundation and RTD Projects (directly with Industry or funded by national/European funds). Some of the projects are: Wireless Socks (with FIORIMA business partner), Bombeiro PT 2.0 (with UNILEVER for advanced firefighter coats) and FP7 Inteltex project on Intelligent multi-reactive textiles.
- Narrownet [70] is a Sigfox Portuguese IoT branch which enables the creation of a dedicated communication network to improve the people's quality of life through a narrowband wireless communication technology (UNB - Ultra Narrow band) for low-cost IoT applications. In this way, is possible to connect to the internet any device with low power consumption and with maximum efficiency.

5.23 Romania

IDC predicts that IoT market spending in Romania will expand from $524.70 million in 2015 to reach $1.33 billion in 2020, representing a compound annual growth rate (CAGR) of 20.4%.

Telemedicine systems have gained adoption in order to support smaller hospitals that do not offer a full range of medical services. For example, the Targu Mures Emergency County Hospital is connected to another 40 hospitals in several counties in Transylvania, while the Floreasca Clinic Emergency Hospital in Bucharest is connected to several hospitals in the southern counties of Romania.

Smart parking solutions have been launched in Bucharest and other large cities such as Timisoara, Oradea, Cluj-Napoca, and Iasi, while GPS-based monitoring systems for public transport have also been implemented in various large cities. And the country's first traffic monitoring system was implemented in Timisoara with the help of SWARCO in late 2015.

Another effective implementation case is Brasov, where all buses are equipped with GPS systems. Collected data is used to offer estimated arrival time to travellers in the bus stations. Same time, during FP7 CityPulse [153] project execution a CKAN platform have been implemented aiming to offer a coherent instrument for a future open data strategy, covering transport, air quality and citizens information and feedback regarding public works in the city. All those systems are correlated with street lighting systems and public safety monitoring, targeting a meaningful and effective use of public services and resources.

A reference case for Smart City implementations is Alba Iulia, where a coherent agenda is in place, addressing strategic needs at all levels, being supported on specific areas by an ecosystem of large and small companies.

In terms of public safety and emergency response, the most notable achievement thus far is the cooperation between Vodafone and the SMURD emergency rescue service. More than 1,000 SMURD ambulances are connected to a telemedicine system and the on-board medical devices gather and transmit complex data in real time to the connected hospitals. According to SMURD officials, the system is used for more than 30,000 interventions each year in Bucharest alone.

Following the initial European Union recommendation that member states roll out intelligent metering to at least 80% of electricity customers by 2020, energy companies started deploying pilot projects throughout Romania. As of the end of 2015, it was estimated that nearly 300,000 smart meters had been deployed, and around 200,000 more were planned for deployment in 2016. Even though the EU extended the period until 2022 after taking into consideration the slow pace of smart meter rollouts in some countries, Romanian authorities are thinking of renegotiating the 80% target, as 8.2 million smart meters still remain to be deployed.

Carrefour currently utilizes a total of 600 beaconing devices across 28 of its Romanian hypermarkets, which work in conjunction with the Carrefour Smart Shopping app running on shoppers' Android smartphones.

One of the main reasons the Eastern European country is one of the fastest growing IT markets in the region is due to the deregulation of the telecom sector which allowed for significant investment in the ICT sub-sector. Over the last 15 years, they have developed to the point where Romania now has one of the fastest internet connections in the world. The activity in the ICT sector is one of the country's major growth drivers with a forecast of €4 billion by 2020. This is no wonder if we take into consideration the 7,000 students that graduate in the IT field each year. Universities across the country were very receptive to the market's needs and quickly adapted their educational programmes. In consequence, companies like Google, IBM, Microsoft and telecom players such as Vodafone, Telekom and Orange are provided with an educated and forward-thinking workforce. Having the means and the knowledge in place paved the way for new technologies to develop. Romanian start-ups deliver solutions for a whole range of products and services. From Zonga, the four-year-old cloud-based music player to Printivate, the 3D printing optimisation software start-up, Romanian incubators provide with innovative ways to manage the many different aspects of both professional and personal lives [57].

Looking at recent year another relevant aspect for overall technology exposure is the aquisition of Romanian smart watch producer Vector Watch by world leader in wearable devices – Fitbit – followed by the announcement of a new large R&D centre setup in Bucharest.

Looking at R&D activities we can observe a consistent growth of subjects' quality approached and the distribution of them, mostly in collocation with large technical universities as relevant sources of talent pools. Large companies like Continental, Bosch, Siemens, Adobe, Infineon, BMW, Elektrobit involve consistent R&D teams focused on future ready topics like Remote Diagnostics, car instrumentation, connected media. Focus on the subjects is supported by large developers' oriented events like DevTalks [154].

The RomanianStartups.com brings together, in one place, the Romanian technology and Internet/IoT related start-ups, founders, accelerators/incubators, events, co-working spaces, mentors, investors and makes it a one-stop-shop for all the information needed to get an overall view of what is happening in the Romanian tech field [58].

5.24 Slovakia

The Internet of Things is a natural evolution of IT technologies by connecting basic objects to the network. The IoT in Slovakia is only in its beginnings, appearing mainly in the manufacturing plants of foreign companies and individual parts have their own internet address and it is possible to monitor their entire manufacturing cycle [85].

IBM Slovakia opened an IoT workplace in Košice. It will develop cognitive solutions by using the functionalities of the IBM Watson platform, a cognitive computer system that replicates the human ability to answer questions. Watson enables fast processing and analysing of data, resulting in more effective team decisions.

The IBM centre in Košice provides solutions that improve the effectiveness of creating products and services. In addition, they are sought out by clients who want to provide additional value to their customers in the form of optimal interaction that does not trouble the end consumer.

Volkswagen has a tradition of interactive solutions in manufacturing known as Industry 4.0. This refers to the automation and data exchange in manufacturing technologies, using cloud computing and connecting the individual objects via the IoT. Currently, the IoT is used mainly in the automotive industry, but it can be used in any industry and in any manufacturing sphere.

5.25 Slovenia

In Slovenia, promotion of IoT domain was mainly driven by the Living bits and things event, organized annually since 2011 [155]. It gathers a mix of researchers and people from industry, addressing various topics and connecting Slovenian community with leading European IoT activists.

The DIGITAL SLOVENIA strategy is a commitment for a faster development of the digital society and the use of opportunities enabled by information and communication technologies and the internet for general economic and social benefits.

Along with the strategies from its scope, it envisages measures to tackle the major development gaps in the field of digital society: faster development of digital entrepreneurship, increased competitiveness of the ICT industry, overall digitisation, development of digital infrastructure, construction of broadband infrastructure, strengthened cybersecurity and the development of an inclusive information society. It foresees priority investment in the digitisation of entrepreneurship, innovative data-driven economy and development, and the use of the internet and, in these frameworks, in the research and development of technologies of the internet of things, cloud computing, big data and mobile technologies [84].

The internet of things is an increasingly efficient uniform environment, offering extraordinary development opportunities and an extensive range of services that are useful, functional, reliable, safe and flexible. In steering development activities, we must take into account the fact that economic and general development in contemporary digital society is closely connected with the development and use of the internet and digital literacy.

The internet offers exceptional opportunities for tackling economic, social and environmental challenges, so it is a key factor for future economic and social development; thus, its deployment strongly in the public’s interest. The challenges will grow even further with the development of the omnipresent internet of things and cloud computing. The priorities at the national level are co-financing RDI projects of e-services, mobile applications and ICT solutions in the field of the internet of things.

5.26 Spain

Spanish companies are leading in IoT, according to a recent HP Enterprise study, 42% of companies have adopted IoT solutions into their business, the highest number in Europe [74]. In addition, almost every city has an active Smart Cities initiative with Santander and Barcelona (supported by its modern telecommunications infrastructure) recognised as particularly significant international Smart Cities.

The current national digital strategy for Spain (2013), the responsibility of MINETAD, the Ministry for Energy, Tourism and Digital Agenda, is under public consultation to be completed in September 2017 which will result in a new National Strategy that brings it into line with the objectives of the European Digital Agenda for 2015 and 2020 as per the 2015 recent communication, A Single Digital Market for All [75] . The new Digital Agenda for Spain will centre around the five key pillars of [76]:

- Data Economy
- Ecosystems 4.0
- Intelligent Regulation
- Technological Infrastructure
- Citizenship and Digital Employment

The aim for this new agenda is to identify the challenges and experiences from the previous strategy and create a new living and flexible instrument that will deal with Telecommunications and Ultrafast Networks, ICT in SMEs and eCommerce, Stimulating the Digital Economy and Digital Content, Internationalisation of Technology Companies, Digital Trust, Development and Innovation in the ICT Sector, Digital Inclusion and Employment, Digital Public Services, eGovernance, Smart Cities and Boosting Natural Language Technologies. The current and future Digital Agenda for Spain are deliberate in their mapping onto the European

While a dedicated Internet of Things Strategy is not present, the areas of Data Economy and Ecosystems 4.0 support the proliferation of the sector and dovetail along with wider initiatives into the topics outlined in the Commission's working document on Advancing the Internet of Things in Europe. Within the Data Economy axis, it is proposed to identify, for data not considered personal and dealt with under the upcoming GDPR framework, ownership, value and ethics and the development of tools to advance the creation of the data marketplace in industry and public bodies in line with the European Single Data Market initiative. This will involve dealing with the challenges of regulations affecting the ownership, management, flow, storage and processing of data, the creation of a marketplace with adequate guarantees, and the role of public bodies. The Ecosystems 4.0 is concerned with the creation or support of platforms as foundations of digital transformation within SMEs, start-ups, digital public services and cybersecurity. The strategy will result in plans for investment in SME and start-up research, development and innovation, and supporting the adoption across industry and public organisations.

Currently, under the existing Digital Agenda for Spain, there are two active initiatives that are supporting IoT development and adoption within Spain. These are the Plan for Smart Cities and Connected Industry 4.0.

The Plan for Smart Cities, enacted in 2015 [77], has the objectives of increasing the contribution of ICT to the industrial sectors GVA, improving the efficiency and effectiveness of Local Bodies in the provision of public services through ICT, advancing the governance of Smart Cities system and boosting the standardisation, regulation and legislation of Smart Cities. This is being achieved through cooperation and collaboration of cities, supporting new projects through low-interest loans, grants, public-private cooperation, the purchase by local bodies of innovative solutions from SMEs and start-ups, development of internationalisation plans and supports.

The Connected Industry 4.0, was launched in 2017 in collaboration with key industry players such as Indra, Banco Santander and Telefonica and is a cross-section of the Agenda for the Strengthening of the Spanish Industrial Sector and the Digital Agenda for Spain. [72] The plan aims to accelerate the digitalisation of Spanish industry and manufacturing through the adoption of cyber-physical systems and automation, considered digital enablers. A previous report remarked IoT as a key enabler for the progress in the Industry 4.0 and the digital transformation. An analysis tool is offered to companies in order to evaluate their digital transformation status [73]

The plan will develop competencies and knowledge sharing through cooperation and training, support open platforms for multidisciplinary collaboration, foster the development of digital enablers, provide financial support to technology companies, create a regulatory and standardisation framework for the adoption of Industry 4.0 and the development of new projects. The technologies to be supported will be embedded systems, advanced robotics, 3D printing, cloud computing and platforms, connectivity solutions, cybersecurity, big data and artificial intelligence. Under the plan, SMEs in particular will be supported with financing for R&D projects, subsidies for training and for the development of a personalised digitisation strategy and action plan. This is in addition to the approval of an €80 million competitive internationalisation fund for projects involving SMEs in. Big Data, Cloud Computing, Internet of Things, Cyber Security and 5G, that are available to companies directly or under the EUREKA network of clusters.

AMETIC is the industrial body for IT and Electronical companies in Spain, leading the national field. It is in charge of representing business interests with an strong positioning on private research funding. This association is also aligned with the "Industria Conectada 4.0" initiative collaborating from the very beginning and helping companies to achieve a smooth digital transformation with, creating working groups, coaching, consulting, learning, etc.

5.27 Sweden

IoT Sweden [71] is a national initiative to make Sweden a leading force in the usage of Internet of Things (IoT). IoT Sweden is a Strategic innovation program. The Strategic innovation programmes are funded by government research councils Vinnova, The Swedish Energy Agency and Formas.

The Swedish national IoT agenda describes the importance of a strong and modern ecosystem within the IoT [86]. How such an ecosystem can be developed by national mobilization of research and innovation power to create a sustainable strong development of business and society.

The innovation program IoT Sweden consists of a board, members, a number of projects and a supporting program office. The office works to gather actors, increase interactions between stakeholders and finance innovation projects in the area of IoT.

IoT Sweden finance innovative projects in IoT. In the coming years IoT Sweden will work with Internet of Things for innovative societal development. Today the programs has four larger projects all of them starting from different societal challenges and with municipalities as coordinating organisations for the projects. In the coming months a new call for proposals will open with the aim of increasing the number of projects and challenges addressed.

The municipalities located in vicinity of Lund/Malmö, Göteborg, Umeå and Skellefteå coordinate the projects running today. In each project, there are a number of companies collaborating with universities, research institutes and the municipality. The project starts from the challenges as defined by the municipalities and are investigating how IoT can be used to handle the challenges. The challenges in the projects are in fields of elderly care, buildings, monitoring environmental pollution and the flow of people and vehicles in the city.

When results are being produce in the projects efforts will be made to make more municipalities and other interested organisations to adopt the results and systems developed in the projects.

5.28 United Kingdom

The United Kingdom (UK) has promoted the Internet of Things (IoT) in the last few years. In 2014, the government announced more than £40 million ($60 million) in funding for research in the area, and has created an umbrella program, IoTUK, to coordinate the efforts of the various organizations that are receiving a cut [139] [140]. IoTUK brings together elements of the Future Cities Catapult and the Digital Catapult, both part of a larger effort to stimulate the nation's up-and-coming industries. The program will work with the technology and business communities, as well as the public sector and academia.

The IoTUK programme will play a central role in coordination and programme integration of Innovate UK programme and ecosystem activities, and forms part of overall £40m UK Government IoT program. Program to run until March 2018, and the main elements planned for IoTUK are [139] [140]:

- Choosing a "city demonstrator" to deploy and test IoT technologies in the urban environment.
- Creating a research hub focused on security and trust in new devices and emerging networks.
- Forming a hardware accelerator to launch new products and devices.
- Building a "test bed" for exploring the use of IoT technologies in healthcare.

IoTUK Boost is an innovation support programme for SMEs that are looking to utilise a low power wide area network (LPWAN) to develop and prototype their IoT product or service [139]. With longer range, decreased power requirements and lower cost than a mobile network, LPWANs enable a much wider range of IoT applications. The IoTUK programme's aim is to advance the UK's global leadership in the IoT, ensuring that there is increased adoption of high quality IoT technologies and services which have the ability to transform businesses and the public sector.

5.29 Norway

In Norway, the IoT Value Creation Network in the last 5 years brought together key stakeholders from a variety of sectors (research institutions, trade and industry, policymakers/government agencies and other users) to work jointly towards a common vision of the Internet of Things (IoT) [87]. This created a unified IoT community in Norway, going across boundaries of disparate technology sectors, in order to create a joint strategic vision of the IoT and aligning this vision with the current developments on the Future Internet and IoT at European and Global level. The networked was financed partly by The Research Council of Norway and by the private actors involved in the network.

Among others things, the network worked on identifying the possibilities and potential for IoT within the oil and gas industry to address some key requirements:

- Embedded connection in the equipment, such that they can communicate directly with applications on whatever equipment from the supplier with user interface.
- Possibility for control of mobile military field units and the possibility for multi-unit-cooperation.
- Deliver new applications via IoT platform services in order to support subscription models.
- Peer-to-Peer functionality between sensors, equipment, systems and cloud for applications like surveillance, maintenance and logistics.
- Possibilities for integration of structured data, non-structured data and time series (real time) data.

- Application development tools adapted to the users and alike for third party service providers and integrators and standardized compatibility.
- Embedded and connected hardware design and IoT software/hardware application development and integration.
- Identification guidelines for RFID and IoT.

The goal of the network to start an IoT community and an environment in Norway, across the borders of the various technology areas, aligned with the IoT current developments at European and global level was materialised trough the success of Norwegian partners in the EU Calls that are participating in two of the nine projects accepted for funding. One of the partners Tinymesh™ presented its technology at the IoT Network Conference in Oslo, 2015 and now they are part, along with 14 others partners, in "VICINITY" Horizon 2020 Project funded by the EC and involving resources and expertise in 11 countries and the setting up of seven demo sites to showcase how to solve real world semantic interoperability. SINTEF as the largest independent research organisation in Scandinavia is leading several EU and National initiatives in the area of IoT.

The development of IoT technologies and applications requires a national strategy that includes policy considerations focusing on funding, convening and planning, Norwegian Research Council action, etc. Actions considered in the IoT developments are listed below:

- Funding local agencies and local communities' efforts to implement IoT connected technologies and services.
- Funding large-scale national pilot IoT projects for smart cities that focus on integrating multiple smart city applications with scalable and replicable solutions.
- Establishing national/city innovation challenges with prizes to encourage the development of IoT applications with high social or economic impact.
- Subsidizing key IoT connected devices for rapid deployment.
- Funding research, innovation and development for key underlying technological challenges relevant to the IoT, such as miniaturisation, multi-functional integration, intelligent edge computing, improving cyber security and reducing power consumption.
- Establishing government/city-backed venture capital funding for promising IoT connected technologies that could benefit public sector operations.
- Encouraging public-private partnerships for ambitious civic IoT technology projects.
- Facilitating local government smart city deployments, such as by providing best practices and financing guides and freely accessible software tools, free Wi-Fi, wireless sensor networks deployment for environment monitoring.
- Coordinating public sector deployments of IoT LPWA networks (NB-IoT, LoRa, Sigfox, etc.), and high-speed wireless networks, particularly for applications spanning multiple jurisdictions.
- Requiring interoperability and encouraging the development of industry-led voluntary standards and best practices around issues like privacy and security.
- Requiring relevant government agencies to develop and follow IoT action plans focused on improving mission delivery with IoT connected technologies.
- Procurement and grant policies to encourage deployment of IoT connected devices.
- Developing the label of "smart" by default for government operations, such as by requiring the use of IoT connected technologies for customs inspections, integrating smart technologies into government subsidized housing and agency buildings; and embedding sensor networks into infrastructure as part of modernization efforts.
- Supporting IoT, electronics, communications and data science skills in high school and higher education.

Some local industries within IoT technology development and their strategies are listed below:

- **Nordic Semiconductor ASA** is a RF specialist in ultra-low power wireless communications with their main offices in Trondheim and Oslo [59]. They are focusing on highly integrated

RF ICs, protocol stacks, development tools and reference designs within the 2.4 GHz RF, ANT, Bluetooth low energy (BLE), and Sub 1 GHz area.

- **Texas Instruments Norway** was established with the acquisition of Chipcon AS (1996 SINTEFs spin-off company) in 2006, a leading company in the design of short-range, low-power wireless RF (radio frequency) transceiver devices [60]. TI Norway is the worldwide headquarters, located in Oslo, for Low-Power Wireless group, which focus on RF solutions for a variety of short-range applications in the 315/433/868/915 MHz and 2.4 GHz frequency bands, and the ZigBee/IEEE 802.15.4 technology.
- **Atmel Norway AS** (Microchip Technology Norway AS) located in Trondheim, was acquired by Microchip Technology Inc. in 2016 [61]. Focus is design and manufacture of microcontrollers, capacitive touch solutions, advanced logic, mixed-signal, non-volatile memory and radio frequency (RF) components. They provide the electronics industry with intelligent and connected solutions on the industrial, automotive, consumer, communications, and computing markets. Atmel wireless technologies cover multiple in-demand wireless arenas to enable IoT communication: ZigBee, 6LoWPan (802.15.4), Bluetooth, and Wi-Fi.
- **Silicon Labs Norway** (former Energy Micro AS), located in Oslo, focus on ultra-low energy consumption microcontrollers (MCU), system on chip radios and RF Transceivers [62]. Their energy-friendly MCU and radio solutions are designed to enable a broad range of power-sensitive applications for the IoT, smart energy, home automation, security and portable electronics markets.

5.30 Iceland

The Icelandic Centre for Research (RANNIS) manages the national competitive funds and the participation in EU programmes [92]. Compared to its population, Iceland has the largest percentage of its population using the Internet [98].

According to the "Measuring the Information Society Report" launched during the World Telecommunication - ICT Indicators Symposium (WTIS) in 2016, Iceland has the most developed information and communication technology infrastructure in Europe, and the second most developed in the world [93][96]. The CEO of Reykjavik Fiber Network has even stated that Iceland is the best place to launch Internet of Things, Smart Cities and Smart Communities [97].

5.31 Switzerland

Switzerland is embracing IoT technology not just through the private sector via companies such as Deloitte, Nexiot, Swiss Post and Zühlke, but also through infrastructure and semi-public projects such as Cargo Sous Terrain and the Smart City of Carouge, Switzerland (participant of the H2020 project SynchroniCity).

In the private sector, for example, Swisscom - a leading telecommunications provider in Switzerland - is building a Low Power Network (LPN) designed to transmit small pieces of information independently of any external electrical network [46]. This will allow IoT technology to be easily deployable throughout the workplace, the home, and in the city streets themselves. The Swisscom LPN is based on the open LoRaWAN industry standard [47]. In August, Zürich holds a Street Parade and, recently, the Zürich police force used the LPN to track the “Love Mobiles” (moving music performance stages) [48]. In this way, they were able to coordinate the clean-up operation much more efficiently and reopen the streets to regular traffic sooner than was previously possible.

Another example of private-public partnership in IoT technology in Switzerland is Cargo Sous Terrain who will create a series of underground tunnels connecting major cities in Northern

Switzerland [49]. The system will allow easy transport of goods and is expected to reduce road congestion in Switzerland by as much as 40% within the next 20 years. IoT technology will be incorporated in the project by using sensors within the pallets and wagons which will then allow the system to perform automated, real-time route-planning and pre-emptive maintenance [50].

Swiss Post [83], the national postal service of Switzerland, is also striving to utilize IoT for its activities by establishing a network based on LoRaWAN (Long Range Wide Area Network) technology. By setting up a national LoRa network, Swiss Post intends to support its logistics and implement customer oriented application. Through this network Swiss Post was able to connect a range of objects and devices including delivery vehicles, packages and letter boxes at very low cost and limited energy consumption. Additionally, sensors in the LoRaWAN were programmed to trigger an automatic alarm in case sensitive consignments were subject to unauthorized access and theft. The networks could also adequately determine the exact location from where the package was accessed or stolen. The devices in LoRaWAN were approximately the size of a single 5 francs coin. These devices used within these networks are expected to become even smaller over time. This network and its services were first tested between Berne and Biel in March 2016.

At a municipal level, the city of Carouge in the canton of Geneva is pioneering Smart City technologies in Switzerland [51]. It is doing this as part of the H2020 project SynchroniCity who has 33 partners across 11 countries and 8 core cities of which Carouge is one [52]. These cities will work to develop the public benefit of IoT technologies in cities through, for example, 3D noise-mapping, optimisation of municipal service-management, and environmental concerns.

Not unexpectedly, Switzerland aims to improve the lives of its residents through the use of technology such as IoT. It chooses to do this through private companies that have the same goals and, with the presence of world-class technical schools like ETHZ in Zürich and EPFL in Lausanne, the start-up culture among engineers and technologists is competitive on a global scale. By setting out goals for the general improvement of Swiss society, Switzerland can allow IoT-technology companies to solve public problems their own way and then export their solutions to the world.

5.32 Liechtenstein

In 2017 Liechtenstein (and 31 other countries) signed a declaration (The Tallinn Declaration) on eGovernment jointly drawn up by the EU and EFTA [145]. The declaration is intended to create a common basis for the national and international digitalization of administration. The declaration on eGovernment contains five core principles and is intended to be a guide to advance the international digitalization of administration. The declaration is in line with Liechtenstein’s efforts to strengthen digital services in the country's administration, and states that service processes in administration should be conducted digitally as far as possible and be available to all. The data entry for citizens and companies should only have to be carried out once. In addition, efforts should be made for IT systems to be compatible nationally and internationally. A new central platform for digital innovation and networking for Liechtenstein are under construction [147].

In 2015 the Liechtensteinische Landesbank (LLB) Group presented a growth strategy, called the StepUp2020 strategy [146]. The LLB Group intends to embark on a new phase of corporate development and actively advance innovation while also defining its financial targets for 2020.The strategy, encompasses the four elements of growth, profitability, innovation and excellence. In terms of innovation, the LLB Group will invest around CHF 100 million by the end of 2020 into innovation and infrastructure projects as well as pioneering digital solutions.

5.33 Faroe Islands

The Faroe Islands is a self-governing territory of Denmark; hence we refer to Denmark in section 5.7 regarding the national strategies.

5.34 Israel

Israel is renowned for its Innovation ecosystem, sometimes called the "Startup Nation", after a famous American bestseller available in 20 languages [114]. It is also well known that the innovation ecosystem in Israel is based on the industry, and the government is mostly here to embrace and invest too where the private sector is committed. It seems Israel ecosystem has plenty of good reasons to be one of the top leaders in the IoT industry, mostly because they have leadership in the three core architectures of IoT (design, communications and chip technology), plus its world-wide strength in security. For example, the Mobileye acquisition at more than $15B in March 2017 has set how dynamic the IoT and security market is, and shows how motivated founders are now and will be in the following years [115].

Below we give an overview of IoT in Israel:

- The "Map of Israel's growing IoT landscape" by TLV, a venture capital firm, emphases three fields of excellence for IoT: Security, Analytics and Agritech [116].
- The white paper "The internet - everywhere, in everything" prepared by KPMG - emphases that the top Israel IoT excellence is security [117].
- Transportation field successes (Mobileye and others) show very good signs, even if not yet publicised in the reports. And few years back, Waze success & Better Place high-and-downs were part of this.
- In an overview of national IoT activities by Innovation Endeavors, the healthcare topic are added [118].

Israel Innovation Authority, is the public agency who embraces, synchronises and leverages with funds the private sector activities, including in IoT. Some examples are listed below:

- The technological innovation labs initiative program has been launched in 2017. Tender for five mini-incubators very IoT oriented [119]. Renault is one of the 5 winners and will set-up its second Innovation Centres in the world (following San Francisco).
- Creation of several new industry consortiums and the MAGNET program 2017 are including one Food IoT [120].

IoT R&D and Innovation Programs by Multinational companies are coming to Israel for talents and quick prototyping and development: Apple, Intel, GE, Cisco, Samsung, Motorola, PTC, IBM, SONY (following the acquisition of Altair), Harman (following the acquisition of Red Bend, Autodesk (following the investment in Jumper), ARM (following the acquisition of Sansa) and more.

Funding:

- Crowdfunding with national cooperation via Indiegogo and Kickstarter. They allow to begin to develop a field where Israel is being not strong to date (the B2C models).
- Equity crowdfunding some good successes too with the OurCrowd. Equity crowdfunding has good support with over ten IoT cooperation in the portfolio.
- The new VC fund "i3 Equity Partners" focused on IoT (funded by Microsoft, GE, Qualcomm, the Chinese HNA, the Indian Tata and more).

Start-ups and programs:

- Over a total of approximately 6,000 start-ups, almost 400 IoT registered start-ups in Israel [121].
- Some Incubators with IoT in their portfolio
  - MEDX Venture Group.
  - The Time Seed Fund.
  - Sanara Ventures (created by Teva & Phillips).
- Some IoT ventures recently in the news:
  - ForeScout that prepares its IPO at over $1B valuation
  - StoreDot that just raised $60M from Daimler with a valuation of estimated $500M
  - Argus Cyber Security, round B with valuation of about $150M

5.35 Albania

The e-Albania government portal is implemented and administered by the National Agency for Information Society (NAIS) [148]. This government interoperability platform interconnects the systems of the institutions with each other, and offer governmental services digitally. The portal is conceived as a one stop shop where the citizens can be registered only by using an Albanian ID card and is served by seeking and applying for the services needed. The platform include categories as e-Services, e-Payments, e-Property, and e-Consulate.

5.36 Bosnia and Herzegovina

In Bosnia, Agile Association [171] is organizing IoT events in which local communities and IoT experts from the region, including representatives of global companies, like Microsoft and Oracle, are taking part. Three years ago, Agency for environment monitoring of Republic of Srpska, has made an initial installation for environment monitoring.

5.37 FYR Macedonia

In FYR Macedonia, the leading institution is FEEIT [156]. Their involvement in IoT started with the FP7 PROSENSE project, and the group formed at that stage continues to evolve. They initiated several workshops addressing smart city domain and more generally the potential of IoT.

5.38 Moldova

Despite the size of the market Moldova is the house of a new generation of technology enthusiasts connected to global trends.

Most of local IT companies are labs of Romanian or Russian larger ones and are focused on outsourcing. Still, technological community starts to run own events like [94] or hosts own IoT oriented hub [95].

The purpose of the competitions is to increase young people's interest for IoT technology and to motivate them create a future career in this field. As a follow, up of the competition a community of young engineers passionate about IoT will be created, they will change their attitude from a passive observer to an active user who is able to create new things focused on IoT.

5.39 Montenegro

In Montenegro, IoT advancement is driven mainly by Bio-ICT centre of excellence [157] and is followed by University of Donja Gorica (UDG). The focus of their activities is on smart cities and smart agriculture. UDG has won one of the IOT-EPI open calls, and are now applying IOT technology to address problems with counterfeiting in wine-making industry. Public administrations, particularly on the coast, are keen on investing in services enhancing tourism.

5.40 Serbia

The seeds of IoT in Serbia and the region were planted in 2008/2009 by the FP7 PROSENSE project. The goal of the project was to help universities in Belgrade (Serbia) and Skopje (FYR Macedonia) to set up wireless sensor networking labs. These projects organized several workshops in the region, helped in education of the first group of young researchers interested in this domain and as such were the starting point of IoT activities in the region.

The first outdoors IoT installation in Serbia was done in 2011 in Belgrade as the ekoBUS pilot, in the context of the FP7 SENSEI project. On one of the public transport routes, GPS devices equipped with a set of air quality sensors, were installed on several buses, creating a mobile environment monitoring system on top of solution designed for improvement of public transport. Soon after the project, the same solution was expanded and deployed in the city of Pancevo across their complete bus network. This was a collaborative effort of the following companies: Ericsson, Telekom Serbia, and DunavNET. Later, the solution was short-listed for a Mobile World Congress award in the transport domain.

At this stage, M2M and later IoT activities were driven by Ericsson’s office in Serbia and were greatly supported by Telekom Serbia. The FP7 SENSEI project, the buzz it created together with the ekoBUS pilot, as well as several other FP7 projects where the two companies participated (EXALTED, IoT-I, SmartSantander, LoLa, OUTSMART etc.) with involvement of the two companies led to discussions with national government to set up a living lab in Belgrade. The goal of the living lab was to support validation of M2M technology and rapid introduction of smart city services. However, due to changes of the political structure in the country, this initiative has never materialized.

After several years of Ericson spearheading IoT activities in the country (and in the region), DunavNET [158] took over the leading role in promotion of IoT technology and applications as well as in the community creation. Public promotion and community engagement were strongly supported by the Centre for Promotion of Science, through organization of different events. Education of young researchers in the region has been greatly promoted and supported by senZations, an IoT summer school which runs since 2006. The summer school is held annually, and has been hosted in almost all the countries of the Balkan region, attracting several hundred young researchers. A large percentage of lecturers were representatives of relevant FP7 and H2020 projects. Around 2010/2011, Faculty of Organizational Sciences of the University of Belgrade introduced IoT course in the official undergraduate and postgraduate curricula, the first such undertaking in the region. In 2013, the first IoT meetup [159] was set up in the cities of Novi Sad and Belgrade as one of the activities of FP7 SOCIOTAL project. These gatherings were driven by DunavNET and were supported by the Chamber of Commerce of Belgrade. They served as the seed for establishment of a larger IOT community in the country. There are over 300 registered members of the meetup today. The first offspring of this activity were the setup of an extracurricular IoT course in “Jovan Jovanovic Zmaj” gymnasium in Novi Sad [160], and the initiation of the Makers’ movement [161]. With the establishment of several accelerators (e.g. StartIt), involvement of the start-up community has increased and with it the interest in applying

IOT in new business endeavours. A significant impact on general awareness and further enlargement of the IOT community in Serbia was the organization of IoT week in Belgrade in June 2016. This event, together with the prior events used to promote IoT week, gathered support from various institutional bodies and trade associations, resulting in a large turnout (500+).

Other organizations that contributed significantly to IoT activities in Serbia are Belit addressing energy efficiency domain [162], Bitgear addressing transport domain [163], Strawberry energy creating smart benches [164] and the Faculty of Technical Sciences in Novi Sad with its Biosense institute [165]addressing smart agriculture. Biosense institute is nowadays the leading research institution in the smart agriculture domain with strong collaboration links with the University of Wageningen (Netherlands).

While a few years ago, IoT activities were mainly driven by organizations participating in various FP7 and H2020 projects, over the last 2 years the number of active organizations have increased. Examples are market analyst companies like IDC [166], local technology oriented media like PC Press [172] and Internet Ogledalo [167] as well as trade exhibition venues in Novi Sad (novel technologies for agriculture as a part of the traditional international agriculture fair) and Belgrade (smart city extension of a security related fair planned for October 2017). PC Press, as the leading IT related magazine in the country is organizing event called Bizit [173] which regularly features IoT topics. Further to these initiatives, it is important to note activities of Microsoft. They are actively supporting start-up communities by providing cloud tools and mentorships, with specific focus on IoT. They are also organizing Sinergija [168], one of the largest IT technology events in the country gathering IT community and addressing IoT from both technical and business perspectives.

On the public administration side, the frontrunners in Serbia are the cities of Novi Sad and Belgrade. They are increasingly investing in development of relevant strategies as well as deployment of smart city services. Again, FP7 and H2020 projects (CLIPS, WeLive, MobiWallet) are playing an important role, particularly from the visionary point of view and sharing of experiences with other European cities. These two cities are now planning to join the OASC (Open and Agile Smart Cities) association. Several cities from the region are already members of this association [169]. If regional public administrations find a way to collaborate, the speed of the smart city development in the region can be greatly increased. The smaller administrations are also awakening. The efforts are mainly directed towards public lighting, environment monitoring and parking management (Belgrade started deployment of several thousands of parking sensors in the city centre) with a few occurrences of deployment of smart city furniture (benches).

5.41 Turkey

The Internet of Things (IoT) is moving slowly toward maturity in Turkey. But organizations still need to see clear, tangible returns on investment and evidence of how IoT can transform their businesses to commit seriously to a long-term project.

Only 30% or organizations foresee their IoT investment increasing by more than 20% in the coming 12-18 months and over 40% of organizations have no intention to increase their existing investment on IoT

IoT use cases in Turkey have mainly involved fleet tracking and vehicle monitoring. The development of Turkey’s public and network infrastructure, plus Smart City and Industry 4.0 initiatives, will lead to new IoT deployments

No dominant value proposition influences IoT investment or strategy, but the benefits include cost reduction, competitive differentiation, faster and better decision making, and improved customer experience.

A number of innovative companies in Turkey will soon start implementing IIoT by leveraging the intelligent connected devices in their factories. In fact, most multinational manufacturers in Turkey are looking to import smart manufacturing use cases that were previously tested in sites outside the country. In line with this goal, a few multinational manufacturers recently initiated pilot projects that include IIoT and other smart manufacturing enabler technologies (such as predictive maintenance, analytics, robotics, and cloud technologies). These pilot projects are expected to provide multinational organizations with greater efficiency, scalability, and cost savings in 2017. In the past, Turkish geothermal power plants — in partnership with GE — have also used IIoT to eliminate human error, reduce water wastage, and lower carbon dioxide emissions (and thereby improve their operations). This tactic as enabled these plants to save over $0.5 million annually. IDC expects similar use cases to be adopted in the future. With the wider adoption of IIoT, manufacturers in Turkey will break open data silos and connect all of their people, data, and processes from the factory floor to the corporate IT environment in order to enable faster decision making at the executive level. In 2017 and 2018, manufacturers will also focus on the integration of production-line components with internal IT systems. Combined with analytics, manufacturers will be able to optimize operations, diagnose problems, and rack inventory flows more effectively. Since IIoT will enable the faster and more efficient acquisition of greater amounts of data in the long run, business leaders will be able to get a fuller and more accurate view of their enterprises, which will allow them to make better decisions.

In 2016, IoT started to become an enabler of digital transformation across all verticals in Turkey, particularly across the manufacturing, transportation, and government verticals. For example, manufacturing giants reviewed their internal and external processes to optimize their supply chain operations through the use of IoT. Fleet management services and other IoT systems that monitor both vehicle conditions and driver behaviour also presented significant opportunities. However, despite these promising developments in the Turkish market, the local IoT landscape remained fragmented in 2016, with the disparate solutions, devices, and platforms offered by a range of vendors preventing the full value of IoT from being unlocked. Nevertheless, in 2017 and beyond, operators in Turkey will heavily invest in IoT platforms that enable centralized device monitoring, application development, and data management. These investments will allow them to build application services for various verticals such as banking, healthcare, and utilities on top of existing IoT systems and decrease the time to market for such services. In the past, telecom operators such as Turk Telekom also developed Smart City IoT platforms to provide various solutions such as smart home solutions, security systems, intelligent parking solutions, smart lighting solutions, and smart metering solutions. Even though IoT exists in a complex ecosystem and an end-to-end IoT application involves several technologies and entities, adopting platform approach will transform operators into collaborative partners for different types of organizations (such as vendors, platform providers, system integrators, app developers, and industry alliances, as well as niche technology companies and start-ups). This adoption trend will shape operator strategies in coming years and change the competitive dynamics in the whole Turkish IoT ecosystem.

6. European IoT Roadmap of Research and Innovation Priorities

6.1 IoT Focus Area Road Mapping Process

The IoT Focus road mapping process is to defining the framework for the development of IoT in Europe presenting next stages of IoT technologies and the evolution of IoT FA in the context of global societal and technological challenges trends foreseen for the next years. The process is the result of sharing ideas and concepts at European level, and alignment with activities at the national level and similar activities in countries and regions outside Europe and is developed in three steps as presented below: analyse, plan and implement. The work done in this delivery addresses the first step. The second step will be an integrated part of the delivery D01.05 IoT landscape and alignment with European IoT SRIA planned for m21. The IoT roadmap designed as a multi-layered time-based representation, bringing together various perspectives into a common high-level landscape that enables both 'demand' and 'supply' side views to be represented, balancing "market pull" and "technology push" will be implemented in the third step by future EU funded projects and initiatives.

6.1.1 Analyse

This is the first step of road mapping process for defining the framework for the development of IoT in Europe presenting next stages of IoT technologies and the evolution of IoT FA. Through this step the global societal and IoT technological challenges trends foreseen for the next years the are presented and the IoT developments/strategies in the European countries are analysed with the as basis for the road mapping methodological framework. The societal challenges are linked with the industrial domains/sectors and connected to relevant IoT technologies for their future development, as well as to the related the trends foreseen in the future.

The analysis supports the process of observing the dynamics of IoT technology development, including IoT technologies' life cycles, and the tendencies of the market, the tendencies of consumers' needs, and the tendencies of various industrial sectors, as their individual or combined dynamics can influence the rhythm of development of IoT technologies and applications.

The analysis considers that with time, IoT technologies can stick together or separate for generating different streams of IoT technological development (i.e. cognitive IoT, IoT of Robotic Things, artificial intelligence, machine learning, block chain, etc.).

The analysis employs a multi-faceted methodology covering more industry verticals across more metrics of measurement in different European countries and globally. The analysis is based on external and internal data sources from the project partners and IoT European Large-Scale Pilots Programme stakeholders by using a bottom-up approach to identifying global IoT technological challenges cutting across industry verticals, carefully analysing and quantifying these challenges through scenario analysis.

6.1.2 Plan

The planning is the second step of the process that will be an integrated part of the delivery D01.05 IoT landscape and alignment with European IoT SRIA planned for m21, step that will include priorities and timeline for research and development in medium and long term. In the development of the future scenarios for the road mapping of IoT technologies and the evolution of IoT FA several elements will be considered.

6.1.3 Implement

The implementation step considers the inclusion of IoT research priorities in funding programmes and research and innovation initiatives that have a relation to IoT technology and applications and contribute to the development of the new functions, product, services, platforms and digital industries.

6.2 IoT research and innovation priorities

Research efforts are still needed in areas of IoT architecture, communication, naming, discovery, programming models, data and network management, power and energy storage and harvesting, security, trust and privacy. The priorities are depicted by the European research community [26] and are based on the technological and societal trends identified during the last year.

The current approaches are not sufficient to solve these issues, and the technological challenges presented require to revise these research topics in order to address the complex requirements imposed by the convergence of industrial, business and consumer IoT. This opens the path for the development of intelligent artificial intelligence and cognitive algorithms, novel intelligent network paradigms and new seamless services.

The deployments of IoT technologies across industrial sectors require addressing topics such as knowledge-centric networks, context awareness, traffic characterisation, monitoring, optimisation, modelling and simulation of large-scale IoT scenarios for real-life full-scale testbeds, prototypes and practical systems.

The convergence of consumer-industrial-business Internet forms the basis for hyperconnected IoT environments, which require new IoT systems open architectures that are integrated with network architecture (a knowledge-centric network for IoT), horizontal interoperable open platforms that manage things that are physical/digital/virtual, automated and connected, functioning in real-time.

The shift toward contextual computing, where the intelligent nodes/devices can sense the objective and subjective aspects of a given situation, will augment the ability of edge intelligent "things" to perceive and act in the moment, based on where they are (context aware), who they are with, and accumulated experiences. The use of contextual computing in IoT space by combinations of hardware, software, networks, and services that use deep understanding of the intelligent "things" to create costumed, relevant actions that the "things" extend the development of IoT open platforms based on new distributed open architectures.

The contextual IoT is the integration of IoT with parallel and opportunistic computing capabilities, neuromorphic and contextual computing (combinations of hardware, software, networks and services) for creating new user experiences and generating tasks on the fly (such as opportunistic IoT applications using data sharing, forming opportunistic networks, on-demand community contextual formation, etc.). Research addressing the context awareness of IoT should include optimal solutions to create and facilitate decentralised opportunistic interactions among humans, IoT networks and the participatory mobile machines. Research should focus on the field of cross-sectorial IoT applications that anticipate human and machine (including human-machine and machine-machine interactions) behaviours and human emotions, absorb the social graph, interpret intentions, and provide guidance and support.

The Tactile Internet of Things is based on human-centric sensing/actuating, augmented reality and new IoT network capabilities, including the dynamic mobility of the IoT spatiotemporal systems and data management (personal data, which is consumer-driven, and process data, which is enterprise-driven in a pervasive way). Augmented reality includes 3D visualisation, software robots virtually embedded in things and back-end data systems that enable real-time info and

actions. Applications and web browsers are the preferred modes of communication between an IoT device and a smartphone and are challenged by a number of trends and emerging technologies. Messaging platforms for things and developments beyond application program interfaces (APIs) for virtual robots and virtual personal assistants (VPAs) are integrated with things for the post-app era that integrate algorithms at the edge.

The Internet of Mobile Things (IoMT), the Internet of Autonomous Things (IoAT) and the Internet of Robotic Things (IoRT) require research into the area of seamless platform integration, context-based cognitive network integration, new mobile sensor-actuator network paradigms, things identification (addressing and nomenclature in IoT) and dynamic-things discoverability. Research is needed on programmability and communication of multiple heterogeneous mobile, autonomous and robotic things for cooperation, coordination, configuration, exchange of information, security, safety and protection. In addition, research should focus on IoT heterogeneous parallel processing, communication and dynamic systems based on parallelism and concurrency, as well as dynamic maintainability, self-healing and self-repair of resources, changing the resource state, reconfiguration/configuration and context-based IoT systems for service implementation and integration with IoT network service composition.

IoT dynamic collaborative ecosystems are the extension beyond artificial intelligence and cognition, where every mobile thing in an IoT application is able to store and analyse its own usage data and then communicate that data smartly to other connected things and make collaborative networked decisions. When there is a collective networked artificial intelligence and IoT dynamic collaborative ecosystem, the things have the ability to sense, interpret, control, actuate, communicate and negotiate. Networked collaborative artificial intelligence uses natural language processing and integrated bots (software robots) to interact with users based on deep-learning pattern recognition (vison, speech, smell, sound, etc.), convolutional neural networks and brain-inspired neuromorphic algorithms for parallel processing and communication. This requires developments in the area of dynamic and mobile machine-to-machine learning (beyond basic machine learning) and real-time coordination among mobile-sensing and actuation platforms for coordinated planning. The integration of IoT operating systems and distributed event-stream processing for real-time data analysis is based on distributed stream-computing platforms.

Research onto IoT swarm-based cognition, intelligence and continuous active learning, could lead to the development of IoT programming models through digitisation and automation of the multitudes of heterogeneous things.

Research is needed on IoT horizontal open platform integration for providing edge device control and operations, communications, device monitoring and management, security, firmware updates, IoT data acquisition, transformation and management, IoT application development, event-driven logic, application programming, visualisation, analytics and adapters to connect to enterprise systems. Research should also focus on IoT virtual space, mapping and mobility prediction, and virtual deployment for optimising the kinds of mobile things with sensing/actuating capabilities to install, which protocols to use, which types of IoT platforms can send messages directly to each other and which messages need to be routed through gateways or other IoT platforms. Research is also needed on dynamic sensor/actuator fusion and virtual sensing/actuating.

IoT devices require integrated electronic component solutions that contain sensors/actuators, processing and communication capabilities. These IoT devices make sensing ubiquitous at a very low cost, resulting in extremely strong price pressure on electronic component manufacturers. The research and development in the area of electronic components covers the IoT layered architecture, and solutions are needed for dynamic context, traffic characterisation- and location-based data processing, storage, processing, virtualisation and visualisation for mobile-edge computing,

analytics at the edge (device and gateway level) considering optimal data capture, communication, storage and representation.

The development in the area of autonomous systems requires new concepts for mobile edge-distributed micro IoT clouds based on mobility patterns where data is sent from the same mobile thing to multiple micro IoT clouds. The data needs to be kept synchronised for the purpose of later retrieval and analysis.

A context-based end-to-end (E2E) security framework for heterogeneous devices should be explored for various environments (e.g. operational and information technology security convergence) and applications. Protecting IoT devices and platforms from information cyberattacks and physical tampering by encrypting the communications, as well as addressing new challenges, such as impersonating "things" or denial-of-sleep attacks for batteries requires new research efforts, considering that the security framework should be built on real-time business processes and include methods for protecting personal safety and privacy. New artificial intelligence IoT algorithms combined with machine-to-machine learning and swarm intelligence could provide new features to platforms in order to identify cyberattacks. Blockchain technology offers capabilities for tracking a vast number of connected devices. It can enable coordination and processing of transactions between devices. The decentralized approach provided by the technology eliminates single points of failure, and thus creates a more resilient device ecosystem.

Heterogeneous networks that combine diverse technical features and low operational cost could be used for various IoT applications offering a mix of low power short range and wide-area networks, offering combined coverage with both high and low bandwidth, achieving good battery life, utilizing lightweight hardware, requiring low operating cost, having high-connection density. Depending on applications request and the context, the heterogeneous networks should be able to offer high bandwidth, low-latency, high-data rates and a large volume of data, especially in safety and mission critical applications.

Standardisation and solutions are needed for designing products to support multiple IoT standards or ecosystems and research on new standards and related APIs.

Data protection in a future IoT landscape with millions of devices continuously monitoring the everyday lives of people is quite challenging. Various attempts have been performed for creating IoT architectures under the concept of privacy by design, and still research should be done on creating strong privacy enhancing techniques at the edge, enabling users to have full control over their data in a dynamic way. In that regard, the strategies are proposed using:

- **Traffic light metaphor to measure the trustworthiness of the IoT**.
- One idea could be to deploy a **solution, which measures the level of trustworthiness of a service using the traffic light metaphor**. Alternatively, a more elaborate dashboard could be used to give the user an overview of trust values and make adequate suggestions about which services to use [29].
- **Privacy Impact Assessment in Smart Cities** where users should be involved when carrying out **Privacy Impact Assessments** on the envisaged smart city initiative. In fact, According to Article 35 (9) of Regulation 679/2016 on the processing of personal data ("GDPR") "*Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations*". This can be done through:
    - **Open Consultation of users (citizens/data subjects)**
    - **Meetings or workshops with the data subjects' representatives**
- **Other measures** aimed at tackling trust and privacy issues of users could be:
    - Anonymizing as much as possible; alternatively, personal data should at least be pseudonymized;

- Setting a clear retention and portability policy for personal data processed by IoT services;
- Informing users on the envisaged data processing operations, as well as on the stakeholders involved, by means of dashboards.

To achieve the goal of a Trusted IoT (Label), the certification mechanisms envisaged by Article 42 of Regulation 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter the "GDPR"), are crucial to establish a Trusted and Secure IoT Label, either at European Union or Member State Level.

In this regard, it is therefore important to leverage on the certification models for IoT, which have or are being developed in the context of ongoing European research projects, such as:

H2020 Privacy Flag project, which is supporting the development of a new assessment methodology and certification model to assess the compliance with the GDPR. It is directly supporting the certification scheme [170]. H2020 ANASTACIA, which is researching an innovative model of Dynamic Security and Privacy Seal for IoT deployments. H2020 U4IoT project is developing guidelines on privacy for IoT deployments, as well as a serious game to educate data controller, IoT users and citizens on the risk and obligations related to personal data protection when deploying IoT. Coherently with the mentioned research activities, other initiatives have been launched, such as the creation of a European Centre for Certification and Privacy based in Luxembourg that is supported by several European partners, and is in the process of applying for the accreditation by the local competent Supervisory Authority, which could eventually make it an accredited certification body able to certify IoT deployments throughout Europe.

7. CONCLUSIONS

The document is the first step of road mapping process for defining the framework for the development of IoT in Europe presenting next stages of IoT technologies and the evolution of IoT FA.

In this context, the global societal and IoT technological challenges trends foreseen for the next years are presented and the IoT developments/strategies in the European countries are analysed and used as basis for the road mapping methodological framework.

Digitising industry requires a pervasive adoption of Information Technologies (IT) into Operations Technologies (OT) and IoT is considered to be one of the enablers of this adoption as is fuelled by the advancement of digital technologies, as well as dramatically changing how companies engage in business activities and people interact with their environment.

The IoT's disruptive nature requires the assessment of the requirements for its future deployment across the digital value chain in various industries and many application areas, which demand new business models and product-service-experience combinations to address and tackle the challenges in the Digital Single Market (DSM).

IoT is bridging the virtual, digital, physical worlds by combining, sensing/actuating, processing with augmented and virtual reality technologies which require mobile networks 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 in turn command focusing on the new technological challenges identified, while considering the security, privacy and trust issues across these new dimensions.

Connecting many heterogenous devices is on of the challenges of IoT, as the structure of communication models and the underlying technologies need to be changed as these are based on the centralized, server/client paradigm to authenticate, authorize and connect different nodes in a network.

As the networks scale to accommodate billions of devices, distributed, decentralized architectures using edge computing paradigms are needed where devices such as IoT gateways take care of processing and mission-critical operations and cloud computing platforms address the overall large processing tasks.

In this context, the analysis of the eleven technological and fifteen societal challenges brings new insights in future trends, while emphasising the potential that the IoT technologies and application can offer to create smart environment, based on IoT systems comprising of large heterogeneous platforms across the digital value chain in various industries and in various application areas considering even better exchange of data, the use of standardized interfaces, interoperability, security, privacy, safety, trust, and more integration in all areas of the Internet (consumer/business/industrial).

The technological challenges need to be address at the scientific level to produce the state of the art results and at the policy level in order to translate these results into general progress and well-being by introducing better laws and regulations that encourage the uptake and scaling of the technology. In the context of the new digital economy the regulations have to account for an increasing mixture of technologies across physical, biological and digital domains.

The technological and societal challenges will necessitate different and varied changes. Looking across the individual implications of the fifteen societal challenges, both in terms of what and how society may need to change, and how the IoT technology can support the change.

While the technological and societal challenges hold true globally, inevitably the European countries will need to determine the relevance of these changes at European level.

The IoT research and innovation priorities are depicted by the European research community [26] based on the technological and societal trends identified and used to develop IoT research roadmap that will be an integrated part of the delivery D01.05 IoT landscape and alignment with European IoT SRIA planned for m21.

8. REFERENCES

[1] O. Vermesan and P. Friess (Eds.). *Digitising the Industry - Internet of Things Connecting the Physical, Digital and Virtual Worlds*, ISBN: 978-87-93379-81-7, River Publishers, Gistrup, 2016.

[2] PwC, 2016, Industry 4.0: Building the digital enterprise Aerospace, defence and security key findings, Available at: https://www.pwc.com/gx/en/aerospace-defence-and-security/publications/assets/industry-4.0-aerospace-key-findings.pdf

[3] J. Daubert, A. Wiesmaier, and P. Kikiras. A View on Privacy and Trust in IoT. Tech. AGT International, Germany, Telecooperation Group, Technical University of Darmstadt, online at: https://www.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_TK/filesDownload/Published_Papers/joerg15privacytrust.pdf.

[4] The need for Privacy and its relation to Trust in the Internet of Things, online at: http://iot-epi.eu/2017/08/10/privacy-and-trust-in-iot/.

[5] J. Rifkin "The Zero Marginal Cost Society" McMillan, 2014.

[6] Assessing the size and Presence of the Collaborative Economy in Europe, PwC, April 2016

[7] IDC Market Forecast, Western Europe Digital Transformation Forecast, 2016–2020, Marta Muñoz Méndez-Villami, Jan van Vonno, Marianne Kolding, IDC August, 2017.

[8] IDC Market Perspective Analytics: Unlocking Value from IoT Data, Mike Cansfield, Philip Carnelley, Angela Salmeron, Helena Schwenk, IDC June 2017.

[9] The Hamburg Port Authority's Impressive IoT Project, online at: https://www.forbes.com/sites/stevebanker/2016/04/01/the-hamburg-port-authoritys-impressive-iot-project/#1488e7816c64

[10] Internet of Things in Logistics – DHL report, online at: http://www.dhl.com/en/about_us/logistics_insights/dhl_trend_research/internet_of_things.html

[11] DHL Smartsensor, online at: www.smartsensor-temperature.net

[12] IDC, Worldwide Semi-annual Internet of Things Spending Guide, 2017

[13] FAO, Food and Agriculture Organisation of the United Nations, online at: http://www.fao.org/home/en/

[14] FAO, The future of food and agriculture - Trends and challenges, ISBN 978-92-5-109551-5, Rome, 2017, online at: http://www.fao.org/3/a-i6583e.pdf

[15] J.R., Porter, et.al., Food security and food production systems. In IPCC. 2014. Climate Change 2014: Impacts, adaptation, and vulnerability. Part A: Global and sectoral aspects. Contribution of Working Group II to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change, pp. 485–533, Cambridge, UK and New York, USA, Cambridge University Press, 2014.

[16] Future Market Insights, online at: https://www.futuremarketinsights.com/

[17] Towards smart farming. Agriculture embracing the IoT vision, Beecham Research, online at: https://www.beechamresearch.com/files/BRL%20Smart%20Farming%20Executive%20Summary.pdf

[18] M2M Sector Map, online at: http://www.beechamresearch.com/

[19] OnFarm – Grow Informed, online at: http://www.onfarm.com/

[20] The power sector goes digital - Next generation data management for energy consumer- EURELECTRIC 2016

[21] Big Data in the Energy Industry, online at: https://www.wilmerhale.com/uploadedFiles/Shared_Content/PDFs/Services/WilmerHale-BigData-Energy.pdf

[22] The Future Belongs to Those Who Monetize and Maximize Their Data. Forrester 2017

[23] Digital DSO – A vision and the regulatory environment needed to enable it' published by EDSO for Smart Grids

[24] O. Vermesan, Internet of Energy, IoT Week Conference, Geneva, 6-9 June 2017, online at: https://iotweek.blob.core.windows.net/slides2017/WORKSHOPS/Energy%20and%20Home%20Comfort/O.%20Vermesan%20SINTEF%20DIGITAL.pdf

[25] S. Ravens and M. Lawrence, Defining the Digital Future of Utilities - Grid Intelligence for the Energy Cloud in 2030, Navigant Research White Paper, 2017, online at https://www.navigantresearch.com/research/defining-the-digital-future-of-utilities

[26] O. Vermesan and J. Bacquet (Eds.). *Cognitive Hyperconnected Digital Transformation Internet of Things Intelligence Evolution*, ISBN: 978-87-93609-10-5, River Publishers, Gistrup, 2017.

[27] Quality Matters Archive, The Commonwealth Fund, September 2011. http://www.commonwealthfund.org/publications/newsletters/quality-matters/2011/august-september-2011/in-focus?lipi=urn%3Ali%3Apage%3Ad_flagship3_pulse_read%3BWcyNAsjKT6ixVRg4aPAbxg%3D%3D

[28] mHealth and Home Monitoring, Berg Insight, 2017.

[29] W. Leister, and T. Schulz, Ideas for a Trust Indicator in the Internet of Things. Tech.IARIA, 27 May 2012, onlie at: https://www.thinkmind.org/index.php?view=article&articleid=smart_2012_2_10_40043

[30] http://www.dailymail.co.uk/sciencetech/article-2541306/Cyber-criminals-hack-REFRIGERATOR-send-malicious-emails-worlds-household-attack.html

[31] http://www.bbc.com/news/technology-36903274

[32] https://labs.bitdefender.com/2016/08/hackers-can-use-smart-sockets-to-shut-down-critical-systems/

[33] http://www.bbc.com/news/technology-36444586

[34] http://motherboard.vice.com/read/blame-the-internet-of-things-for-destroying-the-internet-today

[35] Are your company's IoT devices secure? Internet of Things Breaches are Common, Costly for U.S Firms, Altman Vilandrie & Company White Paper June 2017, online at: http://www.altvil.com/wp-content/uploads/2017/06/AVCo.-IoT-Security-White-Paper-June-2017.pdf

[36] GPEN's survey, online at: https://www.privacyenforcement.net/node/717/.

[37] JOIN(2017) 450 final JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Brussels, 13.9.2017.

[38] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), online at: https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_it

[39] IoT Austria - The Austrian Internet of Things Network, online at: https://www.iot-austria.at/

[40] Internet of Things Belgian, online at: http://www.iotbe.org/

[41] P. Nedeltchev, et. Al., Internet of Everything Opportunities for Bulgaria, CISCO, online at: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/iot-opportunities-for-bulgaria.pdf

[42] Review on the Implementation of the 2030 Agenda in Cyprus, 2017, online at: https://sustainabledevelopment.un.org/content/documents/15886Cyprus.pdf

[43] Yearly report on IoT of the Observatory on IoT of the University of Milan, School of Management, online at: https://www.osservatori.net/it_it/osservatori/executive-briefing/boom-del-mercato-iot-in-italia-2-8-miliardi-di-euro-40.

[44] Official website of the Ministry for the Economic Development, online at: http://www.sviluppoeconomico.gov.it/index.php/en/202-news-english/2036690-national-industry-4-0-plan.

[45] Law of 11 December 2016, nr.232, online at: http://www.governo.it/approfondimento/legge-di-bilancio-2017/6552

[46] SWISSCOM, online at: http://lpn.swisscom.ch/e

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

[48] M2M improves sense of rhythm at street parade, online at: http://lpn.swisscom.ch/wp-content/uploads/2016/06/ent-ss-stadtpolizei-zh-rgb-en.pdf

[49] Cargo sous terrain (CST), online at: http://www.cargosousterrain.ch/de/en.html

[50] Switzerland Builds Tunnel System Powered by The Sun And IoT To Reduce Cargo Traffic By 40 Percent, online at: https://www.forbes.com/sites/sap/2017/09/06/switzerland-builds-tunnel-system-powered-by-the-sun-and-iot-to-reduce-cargo-traffic-by-40-percent/#58ff42ca37fa

[51] Participation de Carouge dans l'open and agile smart city, online at: https://www.carouge.ch/sites/default/files/u1913/ville_de_carouge_communique_de_presse_open_and_agile_smart_city.pdf

[52] SINCRONICITY, online at: http://synchronicity-iot.eu/about/

[53] H. Etzkowitz and L. Leydesdorff, The dynamics of innovation: from National Systems and ''Mode 2'' to a Triple Helix of university–industry–government relations, Research Policy, Vol. 29, 2000, pp. 109-123, online at: http://www.oni.uerj.br/media/downloads/1-s2.0-S0048733399000554-main.pdf

[54] https://connectcentre.ie/pervasive-nation/

[55] http://www.idaireland.com/doing-business-here/industry-sectors/internet-of-things

[56] http://www.oascities.org

[57] IoT potential in Romania, online at: https://www.citiesdigest.com/2017/01/28/iot-potential-in-romania/

[58] Romanian Startups, online at: http://www.romanianstartups.com

[59] Nordic Semiconductor ASA, online at http://www.nordicsemi.com/eng

[60] Texas Instruments Norway, online at http://www.ti.com/europe/docs/sites/norway.htm

[61] Atmel Norway AS (Microchip Technology Norway AS), online at http://www.atmel.com

[62] Silicon Labs Norway, online at https://www.silabs.com

[63] https://www.tice.pt/en/grupos-de-trabalho/iot

[64] http://www.proteus-sensor.eu/

[65] http://tice.mobilidade.ipn.pt/

[66] https://futurecities.up.pt/site/

[67] http://centrofrutologiacompal.pt

[68] https://veniam.com/

[69] http://www.centi.pt/

[70] http://narrownet.iwork.pt/pt/pagina/3/tecnologia/

[71] iotsweden.se

[72] http://www.industriaconectada40.gob.es/Paginas/index.aspx#inicio

[73] https://hada.industriaconectada40.gob.es/es/register/0ff89de99d4a8f4b04cb162bcb5740cf/industria_conectada_40/

[74] The Internet of Things, Today and Tomorrow, HP Enterprise 2017

[75] COM:2017:228

[76] http://www.minetad.gob.es/telecomunicaciones/es-ES/Participacion/Paginas/consulta-estrategia digital.aspx
[77] Ciudades Inteligente, Agenda Digtal para España – Plan Nacional de Ciudades Inteligentes, 2015, Ministerio de Industria, Energía y Turismo.
[78] IAB Poland, online at: https://iab.org.pl/
[79] Figaro, online at https://www.fibaro.com/en/
[80] Estimote Inc., online at https://estimote.com/
[81] Polski Klaster Badań i Rozwoju Internetu Rzeczy, online at: www.iofthings.pl
[82] IoT North Poland, Regional Digital Innovation Hub related to Internet of Things, online at: http://i4ms.eu/regional_hubs/detail.php?id=126
[83] Swiss Post, online at: https://www.post.ch/en/about-us/company/media/press-releases/2016/swiss-post-is-developing-an-internet-of-things
[84] Digital Slovenia 2020 – Development Strategy for the Information Society untiL 2020, online at: http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/DID/Informacijska_druzba/pdf/DSI_2020_3-2016_pic1.pdf
[85] Touchit, online at: https://touchit.sk/
[86] National Agenda for the Internet of Things, Summary of the project IoT Sweden. ISBN 979-91-7439-989-9 (pdf), 2014.
[87] Internet of Things value Creation Network, online at http://internet-of-things.no/
[88] Modern rail modern Europe - Towards an integrated European railway area. EC Directorate-General for Energy and Transport, 2008. ISBN: 978-92-79-07608-4. Online at: https://ec.europa.eu/transport/sites/transport/files/media/publications/doc/modern_rail_en.pdf
[89] EC Mobility and Transport, online at https://ec.europa.eu/transport/
[90] Shift2Rail, online at https://shift2rail.org/
[91] Future of Rail 2016, Arup July 2014. Online at: https://www.arup.com/publications/research/section/future-of-rail-2050
[92] The Icelandic Centre for Research (RANNIS), online at: https://en.rannis.is/
[93] Iceland Has world's second most developed Information Society, according to UN agancy report. Iceland Magazine December 2016. Online at: http://icelandmag.visir.is/article/iceland-has-worlds-second-most-developed-information-society-according-un-agency-report
[94] http://www.hub.md/ro/event/hackathon-remix-iot-moldova-connect-your-city
[95] https://www.tekwill.md/news/primul-laborator-internet-of-things-iot-n-moldova-se-lanseaza-n-iunie
[96] The International Telecommunications Union (ITU), online at: http://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2016.aspx
[97] E. Gudmundsson. *Iceland, Internet of Things, Smart Cities*. TelDaC Resources, Online at: http://www.teldac.com/18982/weblog/iceland-internet-of-things-smart-cities
[98] *Which countries have the highest proportion of internet users?* World Economic Forum, 2013. Online at: https://www.weforum.org/agenda/2015/07/which-countries-have-the-highest-proportion-of-people-using-the-internet/
[99] *European strategies - Maritime Transport Strategy*, European Commission, September 2016. Online at: https://ec.europa.eu/transport/themes/strategies/2018_maritime_transport_strategy_en
[100] Commission staff working dokument on the implementation of the EU Maritime Transport Stragey 2009-2018. European Commission, Septembe 2016. Online at: https://ec.europa.eu/transport/sites/transport/files/swd2016_326.pdf
[101] *Shipping 4.0 presented at Singapore Maritime Week*. Online at: http://www.sintef.no/en/latest-news/shipping-4.0-presented-at-singapore-maritime-week/

[102] Marine Traffic, online at: http://www.marinetraffic.com/

[103] *Roadmap on standards for the Internet of Things (Danish: Roadmap om standarder for Internet of Things (IoT))*, Dansih Standards Foundation, January 2017. Online at: https://www.ds.dk/~/media/DS/Files/Downloads/iot/Roadmap-for-standarder-om-IoT_januar2017.ashx?la=da

[104] *Technologies for future ships and future shipping*, DNV-GL, July 2017. Online at: https://www.dnvgl.com/news/technologies-for-future-ships-and-future-shipping-96960

[105] S. Låg, B.-J. Vartdal, K. E. Knutsen, et.al. *Ship Connectivity*. DNV GL strategic research & Innovation position paper 04-2015.

[106] DNV-GL, Technology Outlook 2025.

[107] *Endorsment feature added to the Maritime Cloud*, EfficienSea, May 2017. Online at: http://efficiensea2.org/endorsement-feature-added-to-the-maritime-cloud/

[108] *Matitime Unmanned Navigation through Intelligence in Networks (MUNIN)*, online at: http://www.unmanned-ship.org/munin/

[109] *A new partnership will promote advanced production technology in SMEs (Danish: Et nyt partnerskab skal fremme avanceret produktionsteknologi i de små og mellemstore virksomheder)*, August 2016. Online at: http://www.lf.dk/aktuelt/nyheder/2016/august/et-nyt-partnerskab-skal-fremme-avanceret-produktionsteknologi-i-de-smaa-og-mellemstore-virksomheder#.Wc50VU0UlD_

[110] *Get help with the introduction of new technology to meet your business with a competitive future (Danish:* Få hjælp til indførelse af ny teknologi, så din virksomhed går en konkurrencedygtig fremtid i møde). Online at: http://www.erhvervspartnerskabet.dk/

[111] *Linked options - Analysis of Danish companies' use of Internet of Things (Danish: Forbundne muligheder - Analyse af danske virksomheders brug af Internet of Things*, IrisGroup. Online at: https://erhvervsstyrelsen.dk/sites/default/files/media/iot-rapport_og_10_cases.pdf

[112] Suomi – Teollisen Internetin Piilaakso, April 2015 (in Finnish)

[113] Huvio, E., Grönvall, J., Främling, K. Tracking and tracing parcels using a distributed computing approach. In: SOLEM, Olav (ed.) *Proceedings of the 14th Annual Conference for Nordic Researchers in Logistics (NOFOMA'2002)* , Trondheim, Norway, 12-14 June 2002. pp. 29-43.

[114] Senor, D., Singer, S. *Start-Up Nation - The story of Israel's Economic Miracle*. Start-Up Nation Book, 2017. Online at: http://startupnationbook.com/

[115] MobileEye (an intel Company). Online at https://www.mobileye.com/

[116] Bek, E., Leiser, R. *A Map of Israel's Growing IoT Landscape*, 2015. Online at: https://www.tlv.partners/a-map-of-israels-growing-iot-landscape

[117] *The internet - everywhere, in everything*. KPMG, 2016. Online at: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/everything-iot-data-security-forum-insights-march-2016.pdf

[118] *How Israel is Becoming a Global Leader in the Internet of Things*. Innovation Endeavors, 2015. Online at: http://www.innovationendeavors.com/thoughts/israeli-internet-of-things

[119] *The Technological Innovation Labs Incentive Program.* Online at: http://www.innovationlabs.org.il/en/index.html

[120] Isreal Ministry of Foregn Affairs. *Israel Innovation Authority begins selection process for MAGNET Consortiums*. Online at: http://mfa.gov.il/MFA/InnovativeIsrael/Economy/Pages/IIA-begins-selection-process-for-MAGNET-Consortiums-2-August-2017.aspx

[121] Start-up national central. Internet og Things. Online at: http://finder.startupnationcentral.org/tag/iot

[122] European Commission, Digital Single Market. Europe's Digital Progress Report 2017 - EDPR country profile. Online at: https://ec.europa.eu/digital-single-market/en/news/europes-digital-progress-report-2017
[123] European Bank for reconstruction and development. *Strategy for Hungary*. March 2016. Online at: http://www.ebrd.com/documents/strategy-and-policy-coordination/strategy-for-hungary.pdf
[124] Euraxess Hungary. Research in Hungary. Online at: https://www.euraxess.hu/hungary/essential-information/research-hungary
[125] Hungarian IoT Creativity Meetup. Online at: https://www.meetup.com/Hungarian-IoT-Creativity-Meetup/?_cookie-check=gNds1SymHJSkK0Xe
[126] T-Systems Hungary - Partner in transformation: Comprehensive industry solutions from T-Systems Hungary. Online at: http://www.t-systems.hu/about-t-systems/introduction/about-t-systems
[127] *Telenor Hungary appoints new sales and marketing director*. Budapest Business Journal, July 2017. Online at: https://bbj.hu/whosnews/telenor-hungary-appoints-new-sales-and-marketing-director_135629
[128] *First Greek NB-IoT smart city pilot introduced in Patras*. Deutsche Telekom 2017. Online at: https://www.telekom.com/en/company/details/first-greek-nb-iot-smart-city-pilot-introduced-in-patras-491858
[129] J. Twentyman. *Athens International Airport turns to IoT for environmental monitoring*. Intnernet of Business, September 2017. Online at: https://internetofbusiness.com/athens-international-airport-turns-to-iot-for-environmental-monitoring/
[130] MiT Enterprise Forum Greece. Online at: http://www.mitefgreece.org/
[131] A. Tsakanikas, S. Danchev, I. Giotopoulos, E. Korra, G. Pavlou. *ICT Adoption and Digital Growth in Greece*. Foundation for Economic & Industrial Research, December 2014.
[132] National Security Authority National Cyber Security Centre. *National cyber security strategy of the Czech Republic for the period from 2015 to 2020*. Online at: https://www.govcert.cz/en/
[133] *Science and Technology in the Czech Republic*. Ministry of foreign Affairs of the Czech Republic, 2014. Online at: http://www.mzv.cz/jnp/en/foreign_relations/science_and_technology/sience_and_technology_in_the_czech.html
[134] *RIS3 Strategy*. Section of deputy prime minister for the science, research and innovation. Online at: http://www.vyzkum.cz/FrontClanek.aspx?idsekce=753765
[135] *National Research and Innovation Strategy for Smart Specialisation of the Czech Republic (National RIS3 Strategy)*. Government of the Czech Republic Department for Analysis and Coordination of Science, Research and Innovation, June 2016.
[136] *Digital agenda 2020 for Estonia*. Ministry of Economic Affairs and Communications. Online at: https://www.mkm.ee/sites/default/files/digital_agenda_2020_estonia_engf.pdf
[137] *Information Society Development Guidelines 2014 - 2020 (Informative part)*. Cabinet of Ministers, October 2013. Online at: http://www.varam.gov.lv/eng/darbibas_veidi/e_gov/?doc=13317
[138] *Resolution No 244 on Approval of Information Society Programme for 2014 - 2020 'Digital Agenda for the Republic of Lithuania'*. Vilnius March 2014, (Consolidated version October 2015).
[139] *Digital Catapult, IoTUK, Online at: https://iotuk.org.uk/*
[140] *British government launches IoTUK program to coordinate Internet of Things development. Online at*: https://www.postscapes.com/british-government-launches-iotuk-program-to-coordinate-internet-of-things-development/
[141] Digital Luxembourg. Online at: http://www.digital-luxembourg.public.lu/en/index.html

[142] Digital Malta. *National Digital Strategy 2014 - 2020*. Online at: https://digitalmalta.org.mt/en/Pages/Home.aspx
[143] *Digital Strategy 2025*. German Federal Ministry for Economic Affairs and Energy. Online at: http://www.de.digital/DIGITAL/Navigation/EN/Strategy/strategy.html and http://www.bmwi.de/Redaktion/EN/Publikationen/digitale-strategie-2025.html
[144] *Twelve points on the digital future*. German Federal Ministry for Economic Affairs and Energy. Online at: http://www.de.digital/DIGITAL/Navigation/EN/Action-Programme/action-programme.html
[145] *Liechtenstein to advance digitalization of administration, October 2017*. Online at: https://www.liechtenstein.li/en/news-detail/article/liechtenstein-to-advance-digitalization-of-administration/
[146] *LLB Group presents growth strategy*, October 2015. Online at: https://www.liechtenstein.li/en/news-detail/article/llb-group-presents-growth-strategy/
[147] *Digital platform Liechtenstein*. Online at: http://digital-liechtenstein.li/
[148] eAlbania. Online at: https://www.e-albania.al/english/
[149] *Monetizing the Internet of Things: Extracting Value from the Connectivity Opportunity*. Capgemini Consulting, October 2014. Online at: https://www.capgemini-consulting.com/internet-of-things-monetization-models
[150] Sensolus NV. Online at: www.sensolus.com
[151] University of Zagreb, Faculty of Electrical Engineering and Computing. Online at: https://www.fer.unizg.hr/
[152] Finnish Industrial Internet Forum (FIIF). Online at: www.fiif.fi
[153] CityPulse: Real-Time IoT Stream Processing and Large-scale Data Analytics for Smart City Applications. Online at: www.ict-citypulse.eu
[154] DevTalks - Enjoy great talks. Online at: http://www.devtalks.ro/
[155] Living bits and things. Online at: http://www.livingbitsandthings.com/
[156] Faculty of Electrical Engineering and Information Technologies (FEEIT, Skopje). Online at: http://www.feit.ukim.edu.mk/
[157] BIO-ICT Centre of Excellence Montenegro. Online at: http://www.bio-ict.ac.me/
[158] DunavNET. Online at: www.dunavnet.eu
[159] MeetUp. Online at: https://www.meetup.com/This-group-is-part-of-the-sociotal-eu-project/
[160] Facebook group. https://www.facebook.com/groups/1023742737676567/?ref=br_rs
[161] MeetUp. https://www.meetup.com/makers-ns/
[162] Belit d.o.o. Online at: http://belit.co.rs/
[163] Bitgear. Online at: http://www.bitgear.rs/
[164] Strawberry energy. Online at: http://senergy.rs
[165] Faculty of Technical Sciences, Biosense institute, Novi Sad. Online at: http://biosens.rs.
[166] IDC. Online at: https://www.idc.com/
[167] Internet Ogledalo. Online at: http://www.ogledalo.rs/
[168] Sinergija. Online at: https://www.mssinergija.net/sr/sinergija17/Pages/Home.aspx
[169] Open and Agile Smart Cities. Online at: http://www.oascities.org/
[170] Euro Privacy. Online at: www.europrivacy.org
[171] Bosnia Agile. *Internet of Things Summit 2017 - Image Create Connect*. Online at: http://agile.ba/en/
[172] PC Press Online at: https://pcpress.rs/
[173] BIZIT. Online at: http://bizit.rs/