AIOTI

ALLIANCE FOR INTERNET OF THINGS INNOVATION

Internet of Things Applications

AIOTI WG01 – IERC

Release 1.0

15th October 2015

2015

Introduction

The Internet of Things (IoT) value chains are today fragmented and many companies have developed innovative strategies and technology offerings, which have given rise to a number of submarkets such as M2M application platforms, M2M network security, connected device platforms, service cloud platforms, and industry specific vertical IoT platforms. In this context, the industry has challenges in defining the IoT business cases, the industry's IoT roadmap, IoT value chain analysis, deployment case studies, the vertical market ecosystem, vendor service/product strategies, strategic recommendations and comprehensive forecasts for the IoT market from 2015 until 2020, including an individual assessment of the submarkets.

IoT technology and applications are likely to be major drivers of investment and innovation in the communications sector, over the next years, delivering significant benefits to citizens, consumers and industrial end-users. These will lead to the introduction of many new and innovative services. It will allow data to be transmitted between many different types of devices, improving the safety of transportation, reducing the consumption of energy and improving our health.

The IoT technology is evolving and demonstrating the features in various applications require the integration of the highest, most generalized layer of intelligence and user interface that ties together connected devices and web services using interoperable platforms that deliver the functionality required by the end-users.

The IoT is bridging the virtual world with the physical world and the mobile networks need to scale to match the demands of 25-50 billion things while the processing capabilities require addressing the information provided by the "digital shadow" of these real things. In this context, there is a need to focus on the developments in the virtual world and the physical world for solving the challenges of IoT applications. In the virtual world, network virtualization, software-defined hardware/networks, device management platforms, edge computing and data processing/analytics are developing fast and urgency to be endeavoured as enabling technologies for IoT. The research and innovation in nanoelectronics, semiconductor, sensors/actuators technology, and cyber-physical systems are essential for the successful deployment of IoT applications.

In the physical world, the new wireless technologies for body/personal, home, local, neighbourhood and wide area networks all promise to deliver better economies of scale in terms of cost, energy and number of connections.

Bringing the IoT to life requires a comprehensive systems approach, inclusive of intelligent processing and sensing/actuating technology, connectivity (distributed intelligent gateways, communication cells, etc.), software and services, along with an ecosystem to address the smart environments applications.

In the last few years the European Commission's direct investment reached more than 100 Mill. Euro in the Internet of Things field and this has to be reflected by disseminating products and services developed through the EU FP7 projects and combining them with new products and services developed by industry.

Businesses and other organisations could benefit from new and improved IoT technologies developed in these projects. The increased productivity and enhanced ability of these organisations to offer new goods and services in turn supports the increase of Europe's output and GDP and the benefits from increased knowledge to enhance policy making and achieve its desired out- comes. These investments need to be mirrored in IoT commercial products and services which are developed with the help of EU funding, through research and development contracts, patents, use of EU funded facilities, technical assistance from EU, or data from EU projects research.

The IERC - IoT European Research Cluster – is bringing together EU funded projects with the aim of defining a common vision of IoT technology and addressing European research challenges. The rationale is to target the large potential for IoT-based capabilities; coordinate/encourage the convergence of ongoing work on to tackle the most important issues; and build a broadly based consensus for the realization and deployment of the IoT technology in Europe in order to keep the leadership and the competitive advantage on the world market.

The European Commission has adopted on May 2015 the Digital Single Market strategy and has opened the door for large-scale proposals to improve the future of industrial development. In this context, the future activities can mobilise the important research work delivered by the IERC projects in terms of IoT technology and societal analysis, and apply it in the market and in the EU policies. The launch of the Alliance for IoT Innovation (AIOTI) in order to develop and support the dialogue and interaction among the various IoT players should be seen as a signal in this direction.

The IoT research, development and deployment efforts will be fruitless if the EC and the Member States fail to continue to invest in the enabling technologies and factors that are required to accelerate the IoT that takes various implementation forms such as Industrial Internet of Things (IIoT) or Internet of Everything (IoE). The technology behind the IoT has to be combined with a number of larger and broader social, economic and political factors if Europe is to make the most of their productive and innovative potential. The problem for the IoT technology and application stakeholders is that these factors are complex, and often not under the control of the private sector.

EC and the Member States will need to make an even bigger investment in digital infrastructure if they are to support and facilitate the IoT deployment, as its success is critically dependent on the presence of robust infrastructures (anybody, anytime, anywhere, any device, any network and any business), such as ubiquitous connectivity, gateways and edge devices.

This will allow eliminating the "digital divide" and creating the basis for the implementation of the Digital Single Market.

Executive Summary

The IoT technological advancements and convergence within the IoT related technologies shape dynamically the emergence of new business models and IoT ecosystems. These ecosystems comprise of stakeholders representing the IoT application value-chain: components, chips, sensors, actuators, embedded processing and communication, system integration, middleware, architecture design, software, security, service provision, usage, test, etc. This new model allows integrating the future generations of applications, devices, embedded systems and network technologies and other evolving ICT advances, based on open platforms and standardised identifiers, protocols and architectures.

In this context, the deployment of IoT Large Scale Pilots (LSPs), to promote the market emergence of IoT and overcome the fragmentation of vertically oriented closed systems, architectures and application areas is the next important step in the IoT development. The LSPs can address the challenges in different application areas by bringing together the technology supply and the application demand sides in real-life settings to demonstrate and validate the IoT technology in real environments.

While human social and economic activities continue to gravitate towards urban centres, Smart Cities deploy digital and telecommunication technologies to increase administration efficiency and improve the quality of life of their inhabitants.

Cross-domain challenges in public safety, mobility, lighting and energy efficiency can be addressed by user-centric ecosystems of interoperable vertical sub-systems. The integration and compatibility of sensors and actuators of connected sub-systems that are often complementary in the public space, in turn, stimulates the development of novel data-driven value-added application domain services. Due to their high density and ubiquitous nature, connected systems offer the prospect of evolving into platforms acquiring domain-level contextual information and delivering application management functions to diverse domains' stakeholders.

The LSPs need to address challenges in the fields of standardization, cyber-security, open data governance and privacy, and validate the novel business models underlying the services provisioned by future domain infrastructures. These IoT LSPs have to address technology challenges across the industrial sector verticals and go beyond the M2M, IoT vertical applications developed in the recent years, in order to break the silos and to evaluate the real impact of IoT technology across industrial domains. The definition of themes need to have a broader perspective and go beyond the narrower use cases proposed until now since in the future that cross-vertical collaboration and integration will be among the primary benefits of IoT.

This document provide an overview of the research and developments results of the IERC projects and the key elements related to the IoT technology developments and deployments for the domains covered by the future IoT LSPs. The report provides information about IoT technological and deployment challenges, findings, and recommendations for action for the use of the results in the new LSPs.

Table of Contents

1 Mission Statement

"Imagination is not only the uniquely human capacity to envision that which is not, and, therefore, the foundation of all invention and innovation. In its arguably most transformative and revelatory capacity, it is the power that enables us to empathize with humans whose experiences we have never shared."

J.K. Rowling

IoT is a concept and a paradigm that considers pervasive presence in the environment of a variety of things/objects that through wireless and wired connections and unique addressing schemes are able to interact with each other and cooperate with other things/objects to create new applications/services and reach common goals.

The IoT is the network of physic al objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment. The confluence of efficient wireless protocols, improved sensors, cheaper processors, and a bevy of start-ups and established companies developing the necessary management and application software, has finally made the concept of the IoT mainstream.

The IoT makes use of synergies that are generated by the convergence of Consumer, Business and Industrial Internet Consumer, Business and Industrial Internet. The convergence creates the open, global network connecting people, data, and things. This convergence leverages the cloud to connect intelligent things that sense and transmit a broad array of data, helping creating services that would not be obvious without this level of connectivity and analytical intelligence. The use of platforms is being driven by transformative technologies such as cloud, things, and mobile.

The dynamics surrounding emerging IoT applications are very complex and issues such as enablement, network connectivity, systems integration, value-added services, and other management functions are all needs that generally must be addressed when the end-users seek to connect intelligent edge devices into complex IoT applications. From the end-user standpoint, open alliances between different stakeholders in the IoT value chain are the best available means to address these complexities.

The IoT LSPs require combining technologies from multiple domains and packaging them into a cohesive user driven experience that will help ensure all of the IoT application value that is being captured is being used and monetized.

The development of enabling technologies such as nanoelectronics, communications, sensors, smart phones, embedded systems, cloud networking, network virtualization and software will be essential to provide to things the capability to be connected all the time everywhere. This will also support important future IoT product innovations affecting many different industrial sectors.

Some of these technologies such as embedded or cyber-physical systems form the edges of the Internet of Things bridging the gap between cyber space and the physical world of real things, and are crucial in enabling the Internet of Things to deliver on its vision and become part of bigger systems in a world of "systems of systems".

The IERC definition states that IoT is "*A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.".*

The major objectives for IoT are the creation of smart environments/spaces and self-aware things (i.e. smart transport, products, cities, buildings, rural areas, energy, health, living, etc.) for climate, food, energy, mobility, digital society and health applications.

One challenge is receiving the data from the things in an interoperable format and in creating systems that break vertical silos and harvest the data across domains, thus unleashing truly useful IoT applications that

are user centred, context aware and create new services by communication across the verticals.

These exchange and processing capabilities are part of the concept of the Internet of Things (IoT) applied to applications such as Internet of Energy (IoE), Internet of Lighting (IoL), Internet of Buildings (IoB) and Internet of Vehicles (IoV) in the City context.

The aim is to create ecosystems of state-of-the-art, viable, technologies that apply the IoT, IoE and IoV concepts to increase the efficiency of the application domain by enabling unobtrusive, adaptable and highly usable services at the network-edge, gateway and cloud levels.

In this context, the IoT LSPs activities can mobilise the important research work delivered by the IERC in terms of IoT technology and societal analysis, and apply it in the market and in the EU policies.

1.1 AIOTI WG01 Objectives

1.1.1 Vision

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

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

The technological trend is a move from systems where there are multiple users/people per device, people in control loop of the system, and the system providing the ability for people to interact with people. The IoT brings a new paradigm where there are multiple devices per user; the devices are things that are connected and communicating with other things. The interaction will be with a heterogeneous continuum of users, things and real physical events (e.g., move left/right/up/down, change humidity/temperature/light/sound, etc.) and the Internet is the common convergence connectivity capability, replacing the previous independent systems.

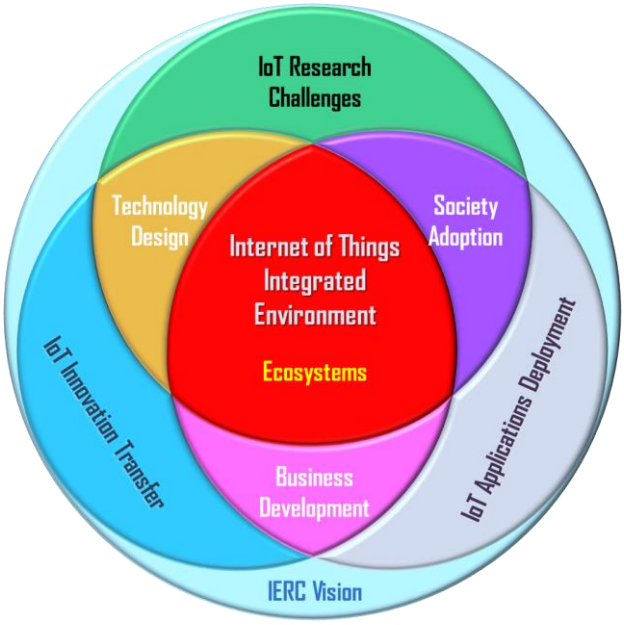

Figure 1.1: IERC Vison for IoT Integrated Environment and Ecosystems

The vison of the IERC is bringing together EU-funded projects with the aim of defining a common strategy of IoT technology, addressing European research challenges and supporting all the key phases in the research, innovation, development, deployment and adoption of new IoT technologies and

applications.

1.1.2 Objectives

The objectives of the IERC related to the IoT LSPs is to provide the information related to the important research work and results delivered by the IERC projects in terms of IoT technology and societal analysis, and apply it in the IoT LSPs and further into the market applications and in the EU policies. The final goal is to test and develop innovative and interoperable IoT solutions in areas of industrial and public interest.

The IERC objectives are addressed as an IoT continuum of research, innovation, development, deployment and adoption as presented in Figure 1.2.

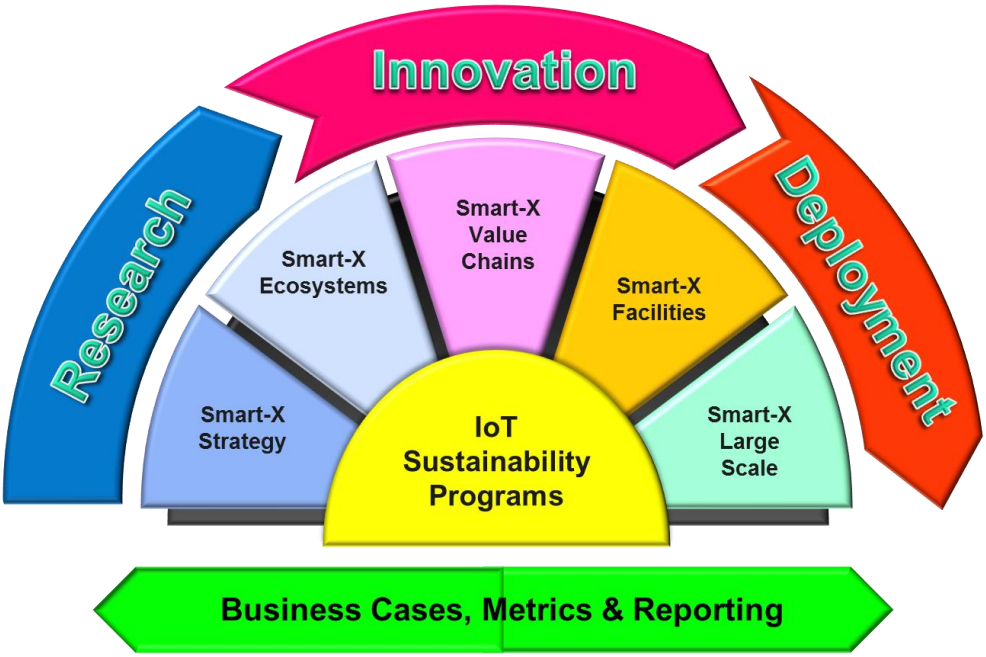

Figure 1.2: IoT Continuum – Research, Innovation, Deployment

The objectives are considering the use of the important research work and results delivered by the IERC projects to provide scalable proof-of-concepts so that IoT technology and applications can be mainstreamed in the industrial and public processes, products and services. IoT-based innovations emerged from the previous projects combined with the new ideas put forward in the IoT LSPs allow to test in real settings, demonstrate the genuine value, and prepare for the wider IoT adoption.

The Internet of Things European landscape is evolving and the IERC will focus on the creation of Internet of Things ecosystems in the context of smart environments and applications with links to other disciplines that provide the enabling technologies for IoT applications. Emphasis will be on on stronger combination of IoT with nanoelectronics, cyber-physical systems (CPS), smart system integration, edge computing, future Internet, network technologies, analytic, and new areas like nanotechnology, cognitive science, biotechnology, while supporting the policy and social dialogue is laying the foundation for the “digital society”.

IERC will take measures for supporting the development of ecosystems around the platforms addressed by the new projects under the IoT connected platforms programme emerged from the ICT30 Call and provide input to the future IoT LSPs.

The IERC is actively involved in the AIOTI that was initiated in cooperation with the European Commission in order to develop and support the dialogue and interaction among the various IoT players. The overall goal of the establishment of the AlOTI is the creation of a dynamic European IoT ecosystem to unleash the potentials of the IoT.

1.1.3 Research and Innovation Challenges

The new ICT technological developments will boost nanoelectronics, edge computing, connectivity, architectures and platforms, while IoT will become a strategic element to enable and drive the Digital Single Market (DSM) through new products and services. IoT is an emerging and disruptive technology that integrates devices, data, connections, processes and people and will affect the technological and economic development in the next years.

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

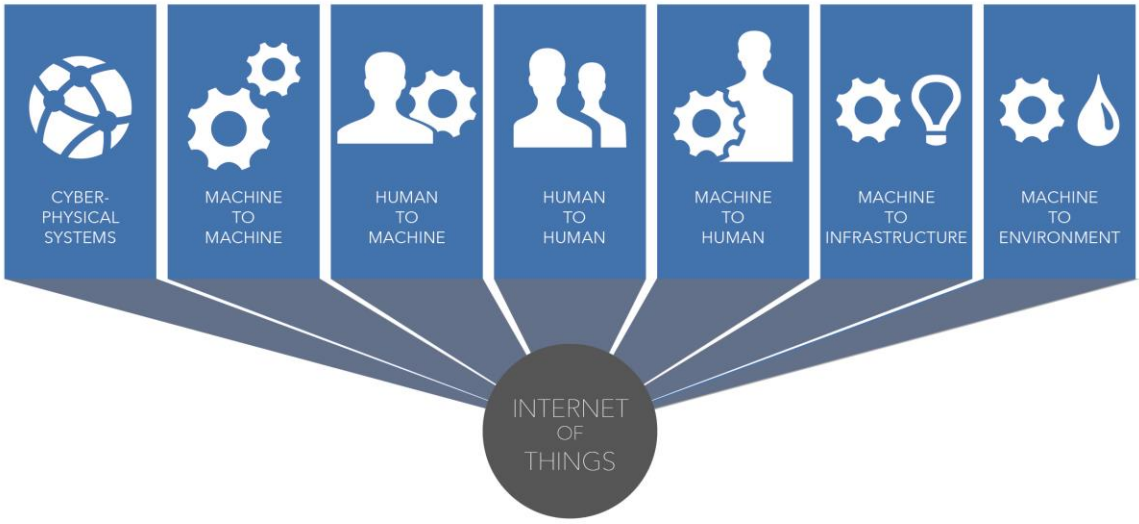

Figure 1.3: Internet of Things Environment

The systemic nature of innovation requires the need for coordination stakeholders, systems and services in interaction-intensive environments with a permanent and seamless mix of online and real-world experiences and offerings, as the IoT will consist of countless cyber-physical systems. The overlay of virtual and physical will be enabled by layered and augmented reality interfaces for interconnected things, smartphones, wearables, industrial equipment, which will exchange continuous data via edge sensor/actuator networks and context-aware applications using ubiquitous connectivity and computing by integrating technologies such as cloud edge cloud/fog and mobile. In this context, the IoT applications will have real time access to intelligence about virtual and physical processes and events by open, linked and smart data.

The future IoT developments will address highly distributed IoT applications involving a high degree of distribution, and processing at the edge of the network by using platforms that that provide compute, storage, and networking services between edge devices and computing data centres. These platforms will support emerging IoT applications that demand real-time latency (i.e. mobility/transport, industrial automation, safety critical wireless sensor networks, etc.). These developments will bring new challenges as presented in Figure 1.4.

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

The IoT architecture, like the Internet, will grow in evolutionary fashion from a variety of separate contributions and there are many current efforts regarding architecture models under development. The IERC was supported and encouraged the projects in the Cluster to use a common approach that is based on the Architectural Reference Model from the EU IoT-A project in order to assure interoperability among different implementations considering that in the future it is likely that several reference

architectures will co-exist in the Internet of Things. The challenges that the IERC considers for the IoT architecture are the complexity and cooperative work for developing, adopting and maintaining an effective cross-industry technology reference architecture that will allow for true interoperability and ease of deployment.

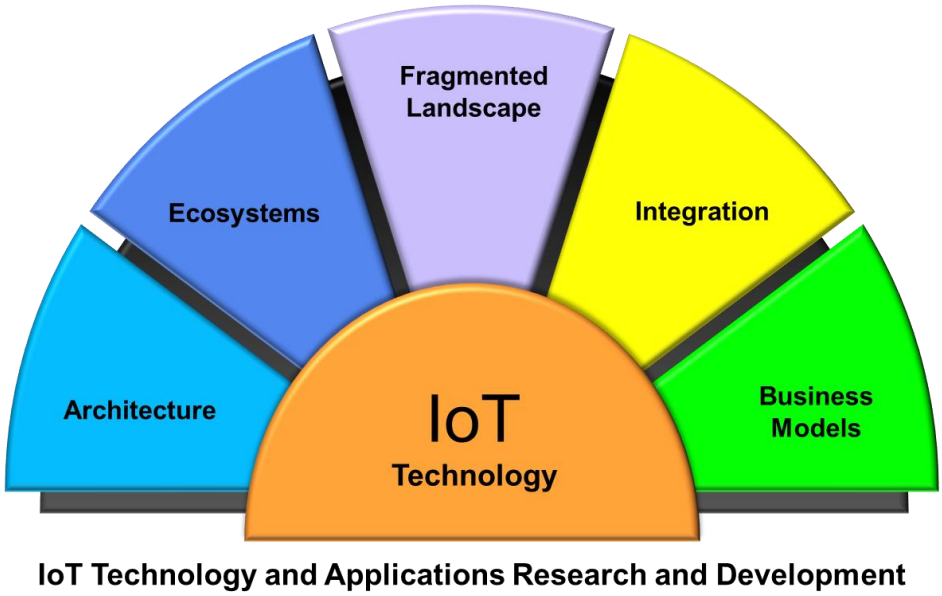

Figure 1.4: IoT Future Challenges

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

The IERC will cooperate with AIOTI WG03 to imitate a discussion with the SDOs working groups addressing the IoT reference architecture in order to provide a common framework convergence towards a common approach.

The horizontal character of the IoT requires the creation of IoT ecosystems as a pre-requisite for the development of innovation and IoT applications take up. In order to address the totality of interrelated technologies the IoT technology ecosystem is essential and the enabling technologies will have different roles such as components, products/applications, and support and infrastructure in these ecosystems. The technologies will interact through these roles and impact the IoT technological deployment.

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

The IoT requires alliances between multiple sectors and stakeholders to cover an increasingly complex value chain and open platforms that can integrate many different types of equipment and applications. The challenges are related to the complexity of services and solution delivery ecosystems. These IoT ecosystems are part of the technology disruption that could cause shifts across value chains where revenue and profits are generated. The emerging IoT ecosystems can evolve and contribute to the IoT LSPs and the IoT technology and applications can be combined with the activities driven by end-users and citizens, and involving existing and new communities at an early stage.

IoT applications have developed on multiple architectures, standards and platforms, resulting in a highly fragmented IoT landscape. The existing IoT applications show a multitude of solutions for edge devices with small installed bases that produce siloed data to which marketers have limited access. The vertical silos and fragmented Smart X landscape is not yet well aligned with the larger IT infrastructure and network services players.

The IoT technology will face a new challenge due to heterogeneous integration of various technologies that requires the technology convergence at various levels. This is mainly due to the anticipation and expectation of new IoT products, services and systems innovation modes that are not widely adopted today. The increased number of IoT edge devices and their "digital shadows" logically multiplies the total number of application infrastructure endpoints that consume or produce data and events, and which in "real-time" need to interoperate with other applications, business processes and operational business intelligence systems as presented in Figure 1.5.

IoT applications are using at the edge of the network sensors collecting data on a computing and communicating device and actuators to perform specific tasks controlled by these devices. A wave of innovation and experimentation is needed in developing these nodes by determine what sensors measure, actuators act, communication/computing is performed, how the nodes are embedded, packages, how they look like, and how much they cost.

The IoT edge devices will increase the overall complexity of distributed business processes, the volume of messages and data flowing across all ICT assets, and drive more demand for "real-time" interoperability with other applications and systems Data security and data protection is a challenge in the integration process for various IoT applications. The developed integrated software defined networking (SDN) and network virtualisation functions (NVF) features for IoT platforms require to implement event triggers which can isolate network components and operations in order to provide real-time security.

The rise of recurring revenue business models and the IoT could transform a wide range of industries, creating new opportunities for customer engagement and revenue growth. The challenge for IoT technology providers, and the stockholders in the IoT ecosystem, is to create value that will convince individuals or business to use it and pay for it. Today the companies are using various traditional business models and they are facing the challenge in adopting new and innovative business models and making the business case in different Smart X areas and across these areas to support investments.

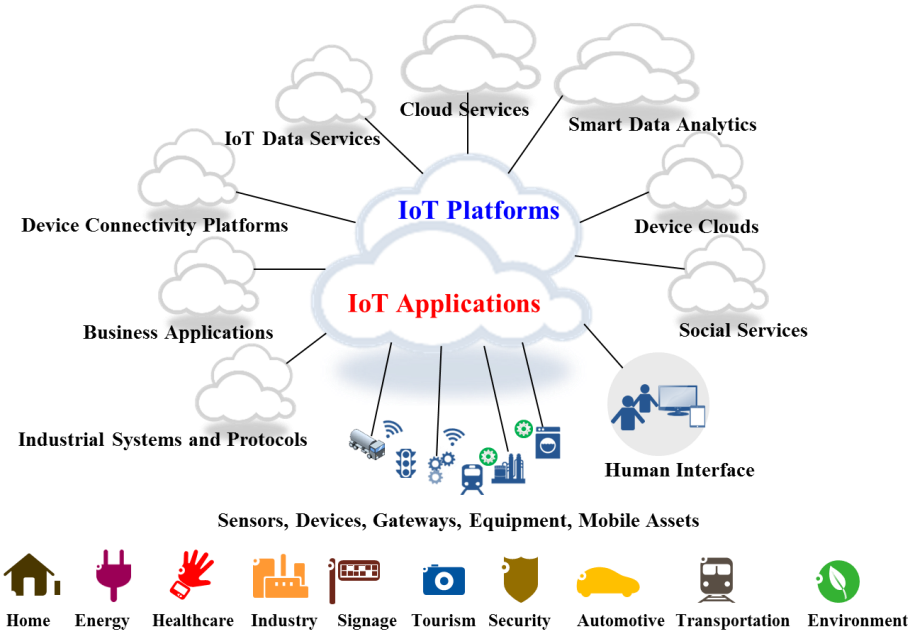

Figure 1.5: Internet of Things Integration of Platforms and Applications

2 Interoperability

To provide seamless communication and interaction between and with the real world objects, at anytime and anywhere in IoT applications, there is a need to address and efficiently solve the interoperability issues at different levels. Interoperability is defined as the ability of two or more systems or components to exchange data and use information this provides many challenges on how to get the information, to exchange data, and to understand and process the information. There are four basic IoT interoperability layers to be thoroughly tested and validated: technical, syntactical, semantic, and organizational. Interoperability is addressing the technical challenges, while composability (a system design principle that deals with the inter-relationships of components), is dealing with modelling issues.

- Technical Interoperability is usually associated with hardware/software components, systems and platforms that enable machine-to-machine communication to take place. This kind of interoperability is often centred on (communication) protocols and the infrastructure needed for those protocols to operate.
- Syntactical Interoperability is usually associated with data formats. Certainly, the messages transferred by communication protocols need to have well-defined syntax and encoding, even if it is only in the form of bit-tables. However, many protocols carry data or content, and this can be represented using high-level transfer syntaxes such as HTML, XML or ASN.1.
- Semantic Interoperability is usually associated with the meaning of content and concerns the human rather than machine interpretation of the content. Thus, interoperability on this level means that there is a common understanding between people of the meaning of the content (information) being exchanged.
- Organizational Interoperability is the ability of organizations to effectively communicate and transfer (meaningful) data (information) even though they may be using a variety of different information systems over widely different infrastructures, possibly across different geographic regions and cultures.

Organizational interoperability depends on the former three. Following the definitions and the trends on ICT sector about sensors and sensor data we can add two other dimensions: Static and dynamic interoperability.

- Dynamic interoperability: Two products cannot interoperate if they do not implement the same set of options (“services”). Therefore when specifications are including a broad range of options, this aspect could lead to serious interoperability problem. Solutions to overcome these aspects consist of definition clearly in a clear document the full list options with all conditions (e.g. defined as PICS in ISO 9646 [24]) as well as to define set of profiles. In the latter case, defining profile would help to truly check interoperability between two products in the same family or from different family if the feature checked belongs to the two groups.
- Static interoperability using approach of the well-known OSI overall test methodology ISO 9646 [24], where there is definition of static conformance review. Conformance testing consists of checking whether an Implementation Under Test (ITU) satisfies all static and dynamic conformance requirements. For the static conformance requirements this means a reviewing process of the options (PICS) delivered with the IUT. This is referred to as the static conformance review. This aspect could appear easy but that represent serious challenge in the IoT field due the broad range of applications.

The challenges for IoT interoperability are many and there is a need for an interoperability framework to address them in a consistent manner under the IoT architectural model. These challenges require addressing a number of research topics that are presented in the IERC position paper "The IoT Semantic Interoperability: Research Challenges, Best Practices, Recommendations and Next Steps" [12]. The report presents various parallel and inter-related interoperability challenges ensuring that technologies deliver information in a seamless manner while the information is understood whatever the context and can be efficiently processed to deliver the potential of innovative services that IoT is aiming for.

3 IoT Policy Issues

IoT presents new challenges to network and security architects. Specific and more evolved security solutions are required in order to cope with these challenges, which if not addressed may become barriers for the IoT deployment on a broad scale. Large-scale applications and services based on the IoT are increasingly vulnerable to disruption from attack or information theft. Vulnerability is the opportunity for a threat to cause loss and a threat is any potential danger to a resource, originating from anything and/or anyone that has the potential to cause a threat.

Many initiatives are addressing the IoT policy issues. One example is the Mauritius Declaration on the Internet of Things [26] that states the following:

- Self-determination is an inalienable right for all human beings.
- Data obtained from connected devices is "high in quantity, quality and sensitivity" and, as such, "should be regarded and treated as personal data."
- Those offering connected devices "should be clear about what data they collect, for what purposes and how long this data is retained."
- Privacy by design should become a key selling point of innovative technologies.
- Data should be processed locally, on the connected device itself. Where it is not possible to process data locally, companies should ensure end-to-end encryption.
- Data protection and privacy authorities should seek appropriate enforcement action when the law has been breached.
- All actors in the internet of things ecosystem "should engage in a strong, active and constructive debate" on the implications of the internet of things and the choices to be made.
- Implement privacy by design.
- Be transparent about what data is collected, how data is processed, for what purposes data will be used, and whether data will be distributed to third parties.
- Define the purpose of collection at the time of collection and, at all times, limit use of the data to the defined purpose.
- Obtain consent.
- Collect and store only the amount of data necessary for the intended lawful purpose.
- Allow individuals access to data maintained about them, information on the source of the data, key inputs into their profile, and any algorithms used to develop their profile.
- Allow individuals to correct and control their information.
- Conduct a privacy impact assessment.
- Consider data anonymization.
- Limit and carefully control access to personal data.
- Conduct regular reviews to verify if results from profiling are "responsible, fair and ethical and compatible with and proportionate to the purpose for which the profiles are being used."
- Allow for manual assessments of any algorithmic profiling outcomes with "significant effects to individuals."

The IoT policy issues is addressed in Europe by 2014 European Commission's Article 29 Working Party on Data Protection [27] setting forth its interpretation of how EU data protection laws apply to IoT and in US by the 2015 Report on the Internet of Things (IoT), from FTC [28] setting forth privacy and security best practices for IoT.

The WP 29 Report looks at IoT via EU data protection principles, highlighting these concerns for IoT manufacturers, developers and data collectors:

- Lack of control – Interconnectivity means a greater potential for automatic flow of data among devices (and vendors) without notice to users.
- Additional purposes – Interconnectivity also may lead to use of gathered data by third parties for other than the original intent.
- Consent – Because users lack full disclosure of data flow, their consent to initial data collection may be inadequate.

- Profiling – Fine-grained user monitoring and profiling could result from the type of information collectable from connected devices.
- Limiting anonymity – More use of connected devices suggests lower likelihood for maintaining anonymity.
- Security – Large volumes of data transferring over connected devices may lead to considerable security risks.

The WP 29 Report recommendations are the security and privacy concerns and recommends that IoT manufacturers, developers and data collectors:

- Conduct a privacy impact assessment before releasing a device.
- Delete raw data from the device as soon as it has been extracted.
- Follow privacy-by-design and privacy-by-default principles.
- In a user-friendly way, provide a privacy notice, and obtain consent or offer the right to refuse.
- Design devices to inform both users and people interacting with them (e.g., people being recorded by a camera in a wearable technology) of the data processing by the entity providing the device.
- Inform users of data that has been collected and enable them to access, review and edit that data before it is transferred.
- Give users granular choices on the type of processing as well as time and frequency of data gathering.

These principles apply whenever a connected device is used in the EU, even if the device did not originate in the EU. While the WP 29 Report is not binding law, it is persuasive to EU regulators, when deciding how to apply data protection law to the IoT. Once the new EU Data Protection Regulation takes effect, fines for violations of EU data protection law could be up to 5 percent of global turnover for a company. Thus, flouting the WP 29 Report principles, which are considered persuasive authority on the interpretation of EU data protection law, could result in very significant fines.

The FTC Report focuses on security (considered as harm to consumers from unauthorized access and misuse of personal information, attacks on other systems and safety risks) and privacy that are considered as following:

- Remote access to smart meters could enable thieves to determine when a house is empty, leaving it susceptible to robbery.
- A connected device could be used to gain control of a consumer's internal network and in turn, attack a third-party system.
- Remote access to stored financial data could enable fraud.
- Privacy-related concerns over the collection of sensitive information (geolocation, financial and health data), the sheer volume of data collected and the potential for misuse.

The FTC Report recommends best practices to IoT manufacturers, developers and data collectors, focusing on:

- Data security – The FTC recommends that device manufacturers adopt a privacy-by-design approach, including a privacy and security risk assessment made prior to release, use of "smart defaults" (e.g., forcing changes to default device passwords) and security and access control measures, and monitoring throughout the device's life cycle.
- Data minimization – While endorsing the necessity to limit collection and retention of users' data, the FTC calls for a "flexible approach," urging companies to "develop policies and practices that impose reasonable limits on the collection and retention of consumer data."
- Notice and choice – The FTC recognizes notice and choice play a "pivotal role," but – in contrast to the WP 29 view – acknowledges that notice and choice are not always necessary. Instead, the FTC calls for notice and choice where sensitive data is collected or where there is unexpected collection or sharing.

The OWASP Internet of Things (IoT) Top 10 [29] is a project designed to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or

assessing IoT technologies. The project defines the top ten security surface areas presented by IoT systems, and provides information on threat agents, attack vectors, vulnerabilities, and impacts associated with each. In addition, the project aims to provide practical security recommendations for builders, breakers, and users of IoT systems.

In order to fulfil the end-to-end security principles and IoT inherent requirements, a distributed approach seems to be the most suitable. With this approach, objects are becoming more intelligent, capable of making their own authorization decisions. The adoption of fine-grained authorization mechanisms allows for more flexible resources control and enables tolerance when fronting unknown-risks. In addition, IP security protocol variants for the IoT with public-key-based cryptographic primitives in their protocol design, such as Datagram TLS (DTLS), the HIP Diet EXchange (DEX), and minimal IKEv2, can fulfil the requirements of IoT regarding scalability and interoperability. End-to-end authentication, integrity confidentiality and privacy, are essential.

The variety of devices comprising the IoT applications is increasing and standardization of security protocols across that various application domains is lacking. Each IoT technology provider has historically taken its own approach to securing devices and addressing the end-to-end security in IoT applications. The digitalization and automation of millions of devices will create a completely new security landscape that has to be evaluated and tested in IoT LSPs. As the IoT environment develops, the main focus need be on adapting privacy and security laws and regulations to protect individuals without hindering IoT's growth, while fostering the huge potential of this market.

The end-user/consumer privacy will require new privacy by design scalable and context aware mechanisms for securing the personal data of individuals as the things they use become increasingly digitized. The IoT applications require a flexible standards-based framework that supports the implementation of privacy and security policies in these applications. The policies need to provide information practices and principles, while offering guidelines for developing operational solutions to privacy issues in various application domains.

In the area of IoT, Europe is addressing the competitiveness in the context of globalisation. The technological specialisations built up over decades are transforming rapidly. In the area of IoT, IERC is focusing on increasing the link of projects, companies, organizations, people and knowledge at European level as a way of making projects more innovative and competitive.

This is particularly challenging, as the information generated by IoT is a key to bringing better services and the management of such devices. Security will have to be integrated as part of IoT infrastructure.

IoT governance, security, privacy and trust are important policy issues that need to be addressed by the LSPs. Achieving the right governance framework is critical to IoT's success across all aspects from architecture, through standards to implementation. IoT embraces a breadth of established, emerging and evolving technologies across a variety of vertical domains that to achieve open interoperability and an environment for market driven application innovation IoT requires an inclusive governance framework, which is yet inexistent. The value of independent leadership, the development of multi-stakeholder supported criteria and backed by the EC would be in providing a suitable adequately resource backed initiative to establish a trusted environment for multi-stakeholder participation and support. This offers the best opportunity to minimize the persistent risk of IoT fragmentation between different stakeholders in the IoT value chain (i.e. ISPs, MNOs, Smart Cards/Embedded providers, ITS, Banking/payment, WSN, etc.) each with their own preferred agenda backed by their particular sector governance body.

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

The challenges and a number of recommendations are presented in the IERC position paper "IoT Governance, Privacy and Security Issues" [12]. The paper identifies relevant IoT challenges and describes solutions defined by the cluster projects, which can be used to address these challenges. IERC projects

have spent considerable effort in the definition of technical solutions and frameworks for the IoT domain. In some case, these solutions may overlap or they may leave gaps, which might become a basis for proposals for future IERC research activities and research programs.

Development of specific "Privacy and Security by Design" approach needs to be considered as required by the LSPs, reflecting the content of the AIOTI Privacy Knowledge base developed by WG04.

The scope of Working Group 4 (WG04), as per the AIOTI terms of reference, is to identify existing or potential market barriers that prevent the take-up of the Internet of Things in the context of the Digital Single Market, as well as from an Internal Market perspective, with a particular focus on trust, security, liability, privacy and net neutrality. In its policy document, WG4 highlights a number of key issues related to each of these areas. In so doing, WG04 also makes a number of recommendations to further inform both the policy debate and the activities of the Large Scale Pilots due to commence in 2016. WG4 also makes reference to other relevant stakeholders that are carrying out important activity in this field and which need to be linked to the work of WG04.

4 IoT Standardisation

IoT is a global concept, and is based on the idea that anything can be connected at any time from any place to any network, by preserving the security, privacy and safety. The concept of connecting any object to the Internet could be one of the biggest standardization challenges and the success of the IoT is dependent on the use/development of interoperable global standards.

Global standards are needed to achieve economy of scale and interworking. Interconnected edge devices are evolving to intelligent devices, which need networking capabilities for a large number of applications and these technologies are "edge" drivers towards the IoT, while the network identifiable devices will have an impact on telecommunications networks.

IERC focussed to identify the requirements and specifications from industry and the needs of IoT standards in different domains and to harmonize the efforts, avoid the duplication of efforts and identify the standardization areas that need focus in the future IoT LSPs.

The complexity with IoT comes from the fact that IoT intends to support a number of different applications covering a wide array of disciplines that are not part of the ICT domain.

Requirements in these different disciplines can often come from legislation or regulatory activities. As a result, such policymaking can have a direct requirement for supporting IoT standards to be developed. It would therefore be beneficial to develop a wider approach to standardization and include anticipation of emerging or on-going policy making in target application areas, and thus be prepared for its potential impact on IoT-related standardization.

IoT implementation costs are expected to follow Moore’s law and in this context, standardisation has to be in place in order to gain full deployment potential.

Standards are needed for interoperability both within and between domains. This is particularly important for the IoT LSPs. Within a domain, standards provide cost efficient realizations of solutions, and a domain can be even a specific organization or enterprise implementing an IoT application. Between domains, the interoperability ensures cooperation between the engaged domains, and is more oriented towards a proper IoT deployment. There is a need to consider the life cycle process in which standardization is one activity. Significant attention is given to the “pre-selection” of standards through collaborative research, but focus should also be given to regulation, legislation, interoperability and certification as other activities in the same life cycle.

Any IoT related standardization must pay attention to how regulatory measures in a particular applied sector will eventually drive the need for standardized efforts in the IoT domain. Agreed standards do not necessarily mean that the objective of interoperability is achieved.

The mobile communications industry has been successful not only because of its global standards, but also because interoperability can be assured via the certification of mobile devices. The emerging IoT dependant industries should also benefit from ensuring interoperability of devices via activities such as conformance testing and certification on a broader scale. The IoT LSPs could be a proper playground for conformance testing.

4.1 Examples of Mapping to Standardised Communication Protocols to Applications

The IoT applications in the LSPs are recommended to use open standards based on independent, international governance body/organization (e.g. ETSI, IEEE, IETF, W3C, OASIS, OMG, OneM2M, ITU-T; ISI, IEC, etc.). Many of these standards are horizontal and neutral and are applicable across vertical domains.

The IoT applications will use standard-defined gateways to connect the applications to other core protocols.

An example of mapping the different SDOs to the protocols provided for different layers in the ISO communication is given in Figure 4.1. The EAP-TLS transport layer security is one example of security mechanism. There could be different layers providing security and encryption (Layer 1, Layer 2, TLS and DTLS, Application layer security) depending on the application and implementation. In this example EAP- TLS run over DECT as an IP stack, but it can also use the MAC layer security mechanism.

TLS could not be included in each radio technology as it is part of the transport layer, and is used by each radio technology as in the provided example. 6loWPAN is a compression mechanism used for 802.15.4 MAC and can run on the IEEE 1901.2 (Power Line Communication) that uses the same MAC layer as the 802.15.4.

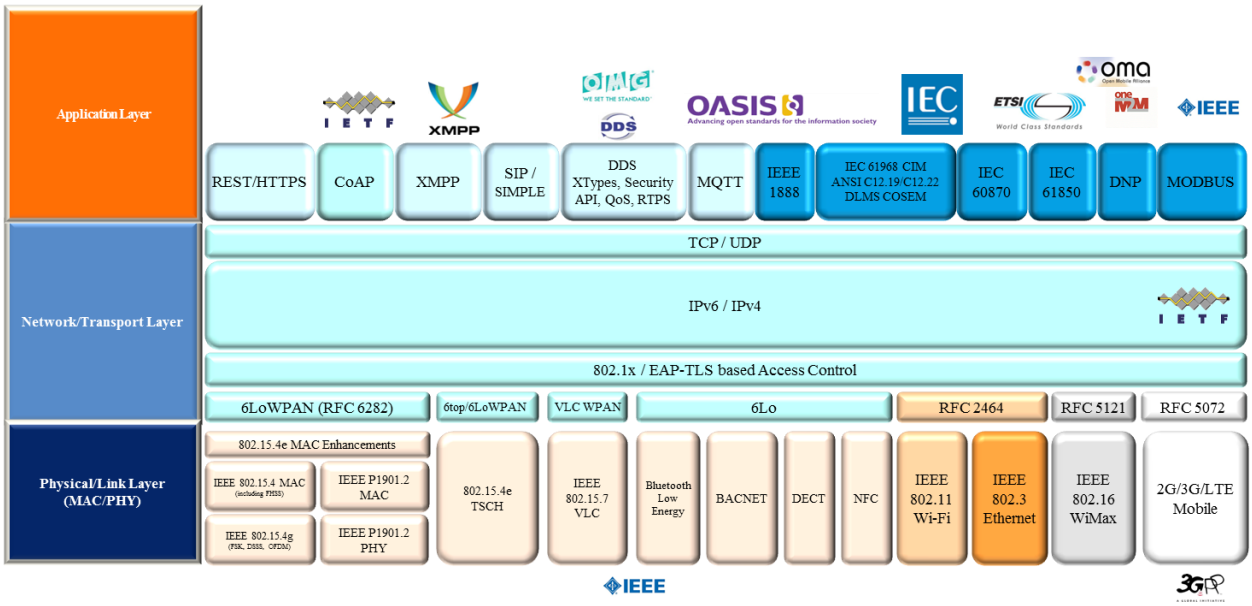

Figure 4.1: Generic Example of Mapping the Different SDOs to the Protocol Layer Stacks

6LoWPAN is not working on any other MAC layer and this is the reason why the working group 6lo has been formed to deal with IPv6-over-foo adaptation layer specifications using 6LoWPAN technologies (RFC4944, RFC6282, RFC6775).

The IETF documents are dealing with transmission of IPv6 Packets over Bluetooth Low Energy, transmission of IPv6 Packets over DECT Ultra Low Energy, transmission of IPv6 over MS/TP Networks, transmission of IPv6 packets over ITU-T G.9959 Networks, transmission of IPv6 Packets over IEEE 1901.2 Narrowband Powerline Communication Networks and transmission of IPv6 Packets over Near Field Communication (NFC). The example is generic and represents only one example of IP stack.

For the IoT applications there are several different types of area networks that will be used and these networks can be can be characterized by their size, their purpose, the coverage range and the data rate values. The spatial/geographic area they occupy and the number of devices that are part of the area network can express the size of an area network. The area networks can cover anything from few devices placed on the body or within a single room to millions of devices spread across a large geographic area.

Figure 4.2 illustrates an example of mapping different protocols to different area networks for IoT applications. There are 5 area networks represented and they are defined as:

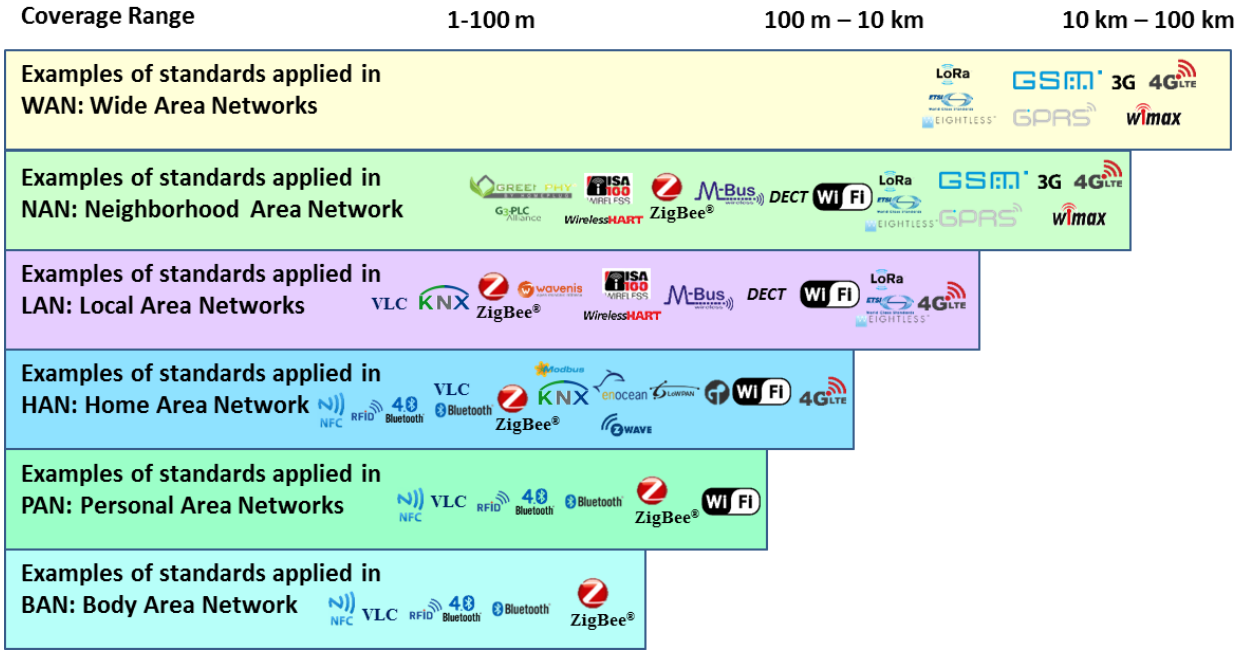

Figure 4.2: Example of Mapping the Different Protocols to Different Area Networks

In this example, there are 6 area networks represented and they are defined as:

- WAN: Wide Area Networks cover a broad area, communication links that cross metropolitan, regional, or national boundaries. Internet is an example of a WAN.
- NAN: Neighbourhood Area Network is defined as a utility access network that connects meters and distribution automation devices to WAN gateways such as RF collectors or data concentrators and field devices.
- LAN: Local Area Networks cover a small physical area, like a home, office, or a small group of buildings or facilities. WLAN: Wireless Local Area Networks cover wirelessly a larger area that is connected to the network.
- HAN: Home Area Network is the connection of network-enabled devices in a domestic home.
- PAN: Personal Area Networks are used for communication among various devices, such as phones, personal devices, fax, and printers, which are located close to a single user.
- BAN: Body Area Network comprises communication between sensors placed on the human body.

The wireless technologies or protocols have different benefits and drawbacks when it comes to the IoT and each can help connect devices to one another for IoT communication depending on the type of application and the requirements and specifications. The same apply for the different area networks.

Figure 4.3 gives an example of mapping different protocols to different area networks for specific applications (i.e. combination of healthcare monitoring, smart home, smart appliances, energy, electric mobility and Cloud integration) showing the multiple protocols that are available for implementation.

The example includes short, medium and long-range area networks with protocols ranging from NFC/RFID to Wi-Fi and cellular.

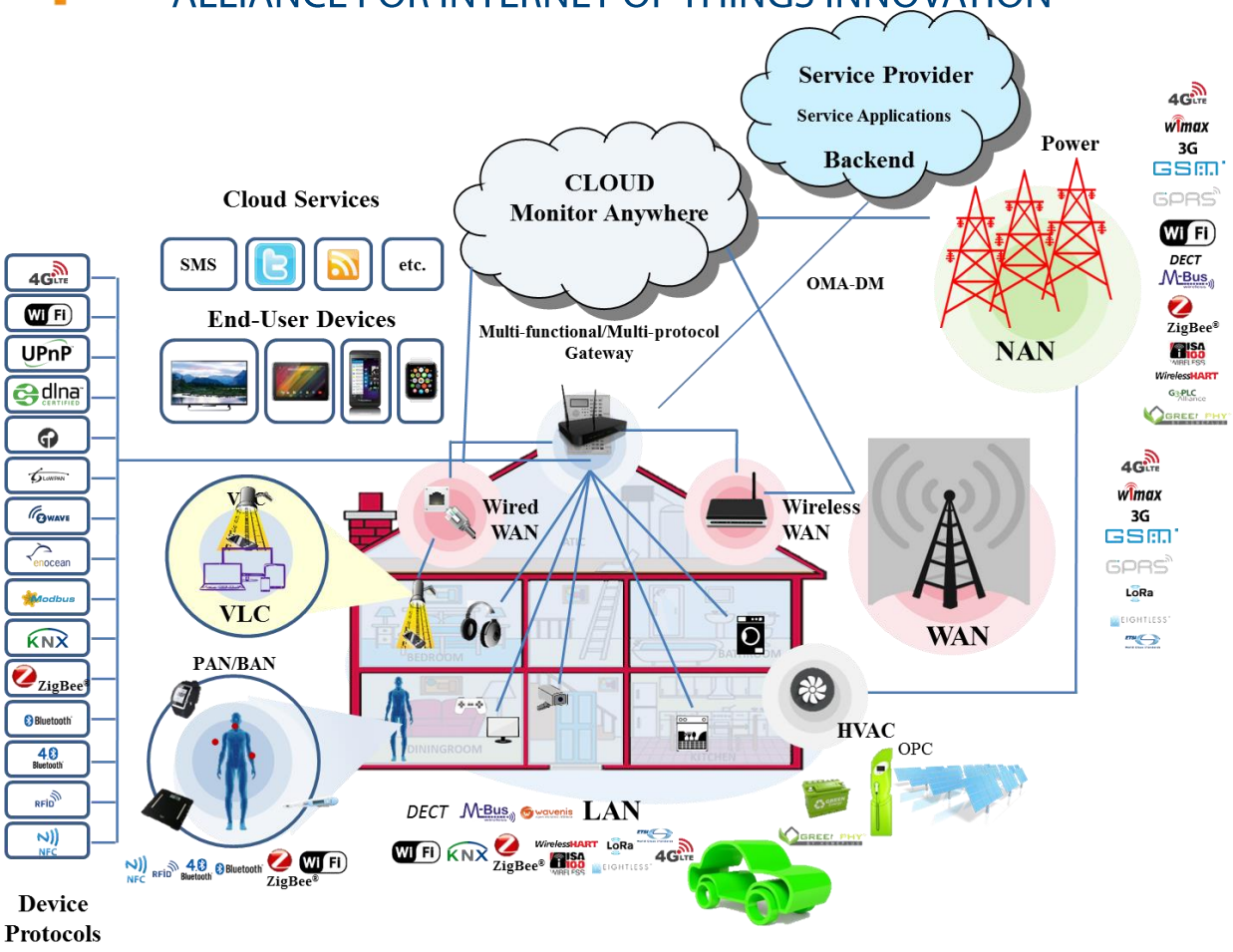

Figure 4.3: Example of Mapping Different Protocols to Different Area Networks for Specific Applications

An overview of the IoT standardisation landscape is presented in the IERC position paper "Standardization for IoT technologies" [12]. A discussion on IoT identifications mechanisms and possible solutions are presented in the IERC position paper "EU-China Joint White Paper on Internet-of-Things Identification" [12]. The work in the AIOTI WG01 is reflecting the views in "IoT LSP Standard Framework Concepts", "IoT High Level Architecture (HLA)", "Semantic interoperability for AIOTI LSPs" for IoT LSPs provided by WG03.

The AIOTI W03 has provided their views on the IoT standardisation that are covered in 3 documents (**): "IoT Landscape and IoT LSP Standard Framework Concepts", "IoT High Level Architecture (HLA)", "IoT Semantic interoperability" recommendations for IoT LSPs.

The documents delivered describe and summarise the outcomes of the discussions within the AIOTI WG03 and reflect the interaction with the other AIOTI WGs.

The work is seen as a reference for the AIOTI WGs in different domains in order to address the standardisation issues and to recommend the use of standard-based solutions for the deployment of IoT solutions in future projects. The documents offer an extensive overview of the IoT standardisation landscape and do not prescribe methods to achieve the implementation of the IoT solutions in different domains. This allows the stakeholders involved future projects to be flexible and innovative in their use of the information, while assuring that they provide standard-based and interoperable IoT implementations.

These documents could be used as a checklist for stakeholders and include information about the IoT Standardisation Landscape, how each SDO and Open Source initiative maps its activities. This is extremely useful information for stakeholders that will work to develop standard-based, interoperable IoT solutions that can demonstrate compliance with specific standards or other standard-based IoT solutions.

(**) AIOTI WG03 documents approved by 16 Oct AIOTI Steering Board meeting will be available at https://docbox.etsi.org/SmartM2M/Open/AIOTI/

5 IoT Applications

IoT technologies are expected to foster innovation in a number of core European industrial sectors, including healthcare and wellness, factory automation/smart manufacturing, sustainable energy, mobility, food production and distribution, environmental monitoring, buildings, living environments, wearables, smart cities, etc.

This section provides an overview of the application areas addressed, as well as technologies, components, demonstrators and pilots that are part of the results of IERC EU-funded research projects in the area of IoT. The Figure 5.1summarizes the application areas addressed by such projects.

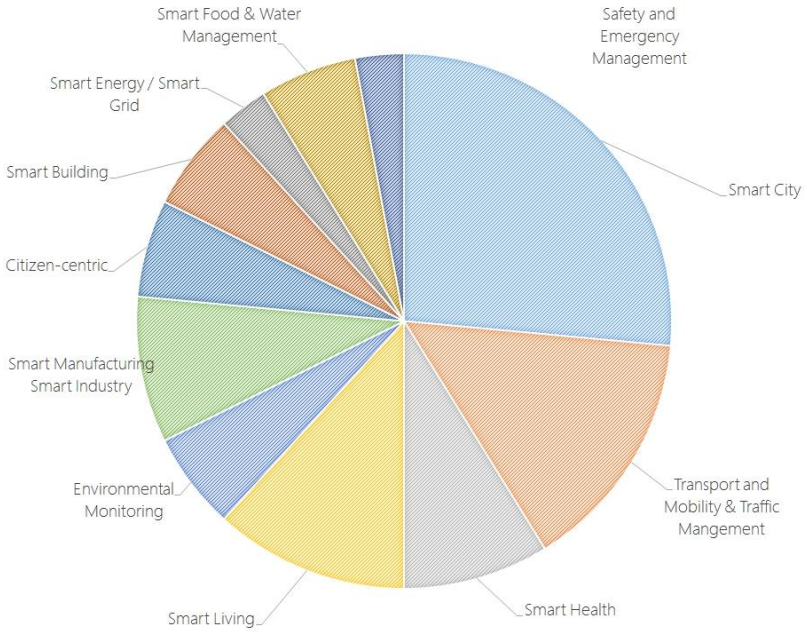

Figure 5.1: Application Areas Covered by IoT Projects

The information presented summarizes the exploitable results that can be used as reference input to the IoT LSPs implementations in different application areas. The goal is fostering commercial and industrial opportunities in the future IoT applications.

5.1 Healthcare and Wellness

Healthcare and wellness offer unique opportunities for comprehensive IoT implementation. Health care treatments, cost, and availability affect the society and the citizens striving for longer, healthier lives. IoT is an enabler to achieve improved care for patients and providers. It could drive better asset utilization, new revenues, and reduced costs. In addition, it has the potential to change how health care is delivered. The emergence of Internet of Health (IoH) applications dedicated to citizens health and wellness that spans care, monitoring, diagnostics, medication administration, fitness, etc. will allow the citizens to be more involved with their healthcare. The end-users could access medical records, track the vitals signals with wearable devices, get diagnostic lab tests conducted at home or at the office building, and monitor the health-related habits with Web-based applications on smart mobile devices. The application of IoT in healthcare can improve the access of care to people in remote locations or to those who are incapacitated to make frequent visits to the hospital. It can also enable the prompt diagnosis of medical conditions by measuring and analysing a person's parameters. The medical treatment administered to the person under care can be improved by studying the effect of a therapy and the medication on the patients' vitals.

The IoT healthcare applications require a careful balance between data access and sharing of health information vs. security and privacy concerns. Some information could be shared with a physician, while

other type of information, will be not accepted to be provided divulge. For these applications, there is a need to have paradigm shift in human behaviour in order for patients to evolve, adapt and ultimately embrace what the IoT technology can provide, a secure Internet domain that can host all health information and push important health data back to the patient and their healthcare providers.

BUTLER SmartHealth trial is involving IoT technologies at home for health monitoring with the aim of helping people to control certain diseases. Partners such as TECNALIA joined the BUTLER project to test the benefits of integrating some of their already existing healthcare products into BUTLER's horizontal IoT platform. TECNALIA has developed different devices and has integrated them in the BUTLER platform (e.g. fall detector, emotion detector, medication intake assistant, telecare reporting service, videoconference for medical and risk prevention service). The field trials performed with the healthcare products integrated into a BUTLER-enabled IoT world prove that any company with already-released services cannot only integrate them easily but also profit from the BUTLER platform. This demonstrated that there are several efficient ways to integrate products and services into BUTLER platform, which should allow any third party company to follow the lessons learnt and benefit from IoT integration. BUTLER provides a complete set of functionalities at all levels, and flexible and cost-effective integration points.

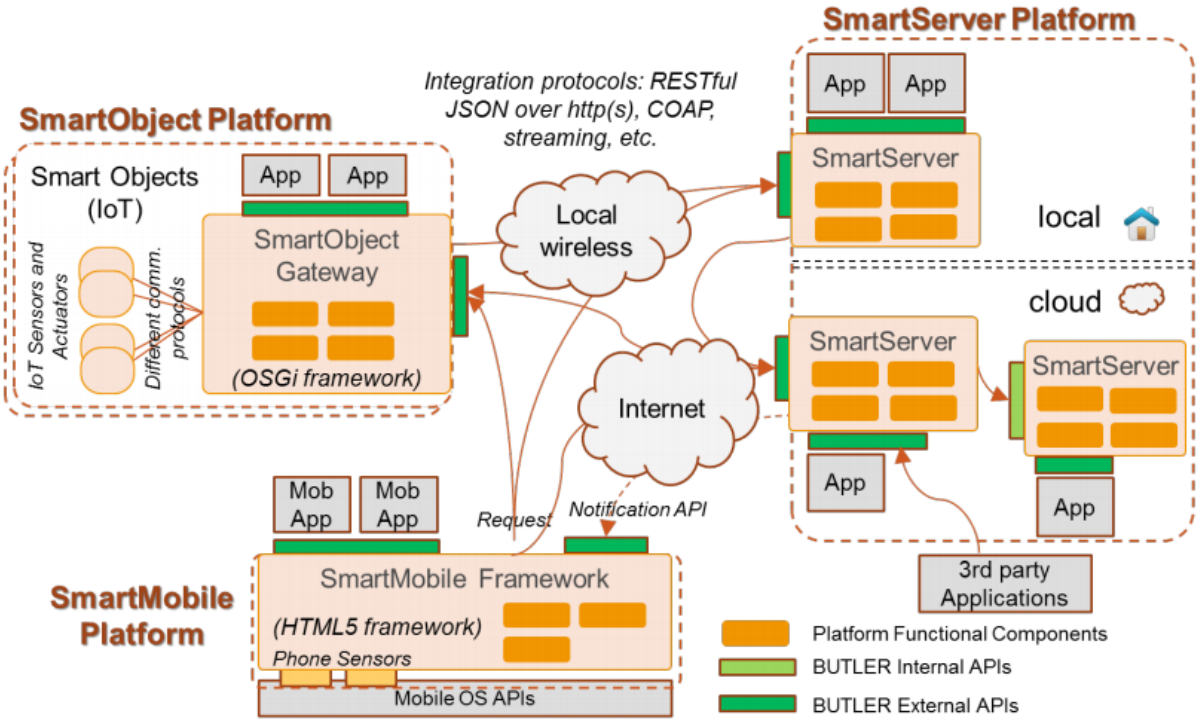

Figure 5.2: Main Components in BUTLER Architecture

The iCore project [11] addressed two key issues in the context of the Internet of Things: abstraction of the technological heterogeneity deriving from the vast amounts of objects, while enhancing reliability; and considering the views of different users/stakeholders (owners of objects & communication means) to ensure proper application provision, business integrity and, therefore, maximize exploitation opportunities. The iCore proposed solution is a cognitive framework reusable for various and diverse applications. Application areas are smart city, smart transport and mobility, smart health, smart living, smart manufacturing and smart buildings.

iCore pilot at Trento Hospital is setup at the department of neonatology of the central hospital of Trento, Italy. The pilot addresses tracking of portable medical equipment (in the range of few tens of items) inside the unit as well as from/to other relevant units, such as gynecology and emergency service. Information about usage and movement of devices will be used to produce predictive models about statistical usage and location of items to support both, end-users (doctors and nurses as well as hospital

procuring and maintenance departments) as well as indoor location developers for reducing energy consumption of their tracking system.

5.2 Living Environments

IoT could bring benefits to people's everyday living environments. The living environments are unique in that they can provide citizens with the greatest diversity of experiences. Citizens work and spend many hours of the day in these living environments. People exercise and engage in a wide variety of activities that can be designed for such activities as health and fitness experiences, work from home experiences, and energy usage experiences.

The ClouT project [4] has developed and deployed a mobile application called "Paw Collection" aiming the prevention of isolation of elderly people by encouraging them to go out and walk through suggested routes that match their interests and respect their health status. With an integrated Social Network Service (SNS), the application motivates elderly people to go out more frequently, take longer walks, thus promoting (physically and mentally) healthier lifestyle, and interacting within communities with common interests. A trial in Mitaka city in Japan has been organised with involvement of 30 senior citizens at their 50s, 60s and 70s (10 participants per each group). 70% of the participants answered that the application helped them indeed to create new communities, 53% confirmed that with the application they went out more frequently and 56% answered that the distance they walk increased. And finally, 77% confirmed that the application answered enjoyed going out more.

After the successful completion of this trial, the feedbacks have been used to release the next version of the application, called Sanpoki (http://sanpoki.ntt-rd.net/), which has been launched in September 26th 2015 for the purpose of health improvement, local community activation and newly introduced city attractiveness collection. The application is available at AppStore and Google Play. The participants can play "stamp rally" game with the distributed BLE beacons in 179 places, the deployed terminals automatically detect the participants' visit to those particular places. By the rule of the game, after visiting a place, participants are requested to take photo of attractive things nearest the place. As the result of this, many attractiveness of city can be collected, and this result will be utilized for the revise of Mitaka's long-term base plan. The field trials will continue until November 26th. Within 2 weeks, 400 users started to use the application and more than 6,000 pictures have already been posted.

The BUTLER project [3] aimed to design and demonstrate the first prototype of a comprehensive, pervasive and effective Context-Aware information system, operating transparently and seamlessly across various scenarios towards a unified smart urban environment. The application areas addressed smart city, health, transport and living.

BUTLER SmartOffice trial focus on deployment of IoT technologies based on the BUTLER platform in three of the offices of the project partners. The three trials shared common functional requirements (information sharing, office wellbeing), all three sites participated in a common PoC of IoT information sharing: coffee consumption data shared between the offices

BUTLER SmartShopping trial addresses the processing in real time of the city status for creating alerts for the merchants, to inform about potential presence of customers that fit with business profile. The system is able to alert merchants about the optimal moments for sending notifications to citizens based on an analysis of city context information: city agenda, parking information, banking information, environmental data. The system has been developed in close collaboration with the merchants of the city, through an iterative co-creation process. It lead to citywide development in Santander (Spain), involving over 250 businesses throughout the city.

iCore smart home trial addresses the IoT self-management aspects through cognitive functionalities in the scope of a Smart Home. The prototype comprises, apart from software components for the various functional components, Arduino platforms combined with various sensors and actuators such as temperature, humidity, luminosity, body pulse and motion detection sensors, accelerometer, lamp, fan/heating and buzzer. Software technologies used for the implementation include RESTful Web Services, JSON, RDF, SPARQL, Sesame API, etc.

iCore task-based Smart IoT testbed environment recommends appropriate tasks as a composition of IoT devices and their services. It is implemented in two rooms: a seminar room and a resting place. The seminar room has various smart objects like projector, screen, light, robot vacuum cleaner, flower pot, temperature/humidity/light sensor, and air conditioner (total 7 objects). The resting place includes smart board screen, smart fridge, and temperature/humidity/light sensor (total 3 objects). Basically the Task-based Smart IoT Prototype can interact with any user who has a smartphone installed with a client application. Based on scenarios including group tasks such as meeting, watching a movie, gaming, etc., the task-based Smart IoT Prototype properly supports up to 10 users.

iCore smart office trial demonstrates the capability of managing the whole lifecycle of a meeting, from its organization to its execution and wrap-up, while re-using already existing IoT devices (smartphones, tablets, smart panels). This is achieved through the development of appropriate Virtual Object (VO) containers for these devices that enable them to become part of an iCore ecosystem, while appropriate Composite VOs at the back-end are able to monitor the meeting and provide the required functionalities for supporting a variety of service requests, ranging from sending out the meeting invitations to supporting the indoor navigation of participants to the meeting venue, the recording of the meeting and the “attention-span” management (smart break) to the eventual wrap-up of the meeting with the uploading of the meeting recordings to a designated area and the notification of the participants for their offline availability.

OpenIoT Silver Angel - IoT Enabled Living and Communication in Smart Cities purpose is to help ageing citizens live independently in their own homes, and to facilitate meeting more often with friends and relatives. It offers three Silver Angel services namely Smart Meeting, Issue Reporting and Alarms.

OpenIoT IoT Enabled Smart campus guide is an application framework to support students, teachers and guest of a university. It offers features like information’s about buildings and rooms, reservations of meetings rooms and workplaces, and collaboration between people

5.3 Buildings

The IoT applications in the buildings are interacting with the intelligent Building Management Systems (BMS) that are overlaying of an IP network, connecting all the building services monitoring, analysing and controlling without the intervention of humans. The IoT applications are used by buildings' managers to manage energy use and energy procurement and to maintain buildings systems. The BMS is based on the infrastructure of the existing Intranets and the Internet, and therefore utilises the same standards as other IT devices. The value in IoT application is in both the data and the edge devices. Collecting data from more building services and equipment provides a more granular view of exactly how each building is performing. These will create the Internet of Buildings (IoB) applications. These IoT applications will reduce the need for human intervention to manage the complexity and the amount of date will increase exponentially. The IoB require interoperability and seamless data interchange between different sub-systems in a building, networks of buildings, various smart equipment, external utilities, (i.e. smart grids, smart cities, etc.) and increased interface with building stakeholders.

The IoE demonstrated a combined integration of EVSE, renewable energy and storage into a building or the power grid. Stability, quality and availability of an electric power grid with a substantial share of renewable energy generation and EVSE loads were demonstrated, confirming the reduction of energy consumption and costs. User-friendly, flexible and cost-effective handling of energy brokerage features and minimisation of external energy cost by efficient interaction with a DSO via energy consumption / production forecast, pricing signals and grid codes were implemented using the federation of several platforms.

The project has demonstrated the integration of partner systems in a residential environment, with electric vehicle and smart metering elements that combines automatic and manual data visualisation for optimized efficiency over a number of use cases. The project addressed the interoperability among the heterogeneous residential automation systems and provided environment friendly solutions through renewables, charging, energy storage, and real time monitoring. The implementation ensured the security, privacy and dependability in an ecosystem of many stakeholders.

The RERUM pilot for comfort quality monitoring utilizes sensors for measuring securely and reliably the indoor air quality within buildings and extract information so that guidelines for improving the air quality can be provided. In Heraklion the system will be installed in two pilot buildings of the municipality (one new and one old) for comparing the results and extract useful information for enabling the municipality to perform changes in order to improve the air quality in the offices. Pilot installation in homes of volunteers is also under discussion. In Tarragona the system will be installed at the municipal offices. Security of the system, reliable device connectivity, privacy of the user data and trust in the system are key RERUM advances in such an application.

The RERUM pilot for home energy management deals with the deployment of sensors for securely measuring the energy consumption of specific household appliances (e.g. air conditioning systems, PCs, lights, etc.) and extracting information and usage patterns so that guidelines for minimizing the energy consumption can be provided. In Heraklion the system will be installed in two buildings, one old and another new, "green" building. In Tarragona the system will be installed at municipal offices. This pilot deals with both improving the security of the system and preserving the privacy of the user data, ensuring that no external party can identify when the user is at home (office), who is at the office at any given time or usage patterns for the devices.

The exploitable results of the two aforementioned pilots, apart from the applications as a whole, include: (i) the powerful authorization framework that controls the access to the services provided by the RERUM system according to the user credentials, attributes, time and day of access, etc., (ii) the privacy protection framework (including anonymisation, pseudonymisation and other privacy enhancing technologies) for ensuring that no user data will be disclosed to unauthorised third parties or no linking between user data is possible is another exploitable result, (iii) the federation engine, that enables the forming of secure federations between trusted devices in order to provide advanced composed services to the users and (iv) the framework for the secure communications of the constrained devices to ensure that no unauthorized person/device can intercept the measurements.

The IoT.est project [15] demonstrates the whole service creation life cycle for IoT services. IoT services can be regarded as being, in principle, similar to any classical service with the marked distinction that part of the service instantiations relies on information obtained from IoT devices (sensor or other sources as well as actuation). Generation of test cases, testing, service-redefinition as well as monitoring will be automated (or at least semi-automated). The four phases of the IoT service life cycle are therefore enhanced with testing and monitoring facilities at different stages of the cycle. The application areas are in IoT service creation, testing and deployment with scenarios applied to Energy Efficient Buildings.

IoT.est IoT services testing scenario "EEBuildingSim" exposes four types of simulated IoT resources: temperature sensors, window actuators, AC units, as well as heaters, currently exposed as single atomic services. These services will be accompanied by a set of "smarter" atomic services, which will include some form of embedded logic combining sensing and actuation into a single service: basic temperature regulator, advanced temperature regulator and follow the fire service.

OpenIoT project [16] provides an open source platform supporting semantic interoperability between sensor data silos and for enabling Internet of Things semantically annotated services in the cloud. The OpenIot middleware platform and Virtual Development Kit was released and made available to the Open Source community for creating real time IoT services on demand and enable interoperability between vertical IoT solutions and interconnect data silos.

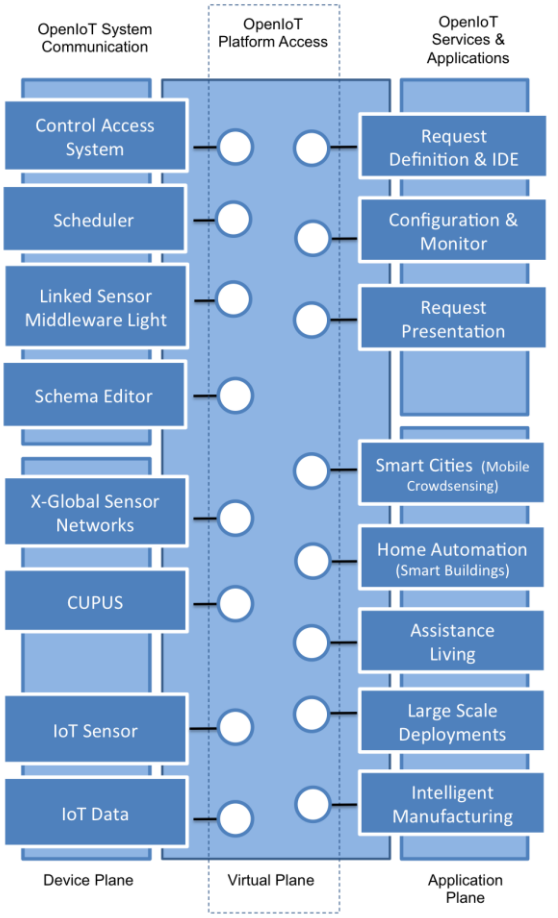

Figure 5.3: OpenIoT Project Architecture

The OpenIoT framework (BETA version v0.1.1) has been released via the github project management portal https://github.com/OpenIotOrg/openiot. The first version of the Virtual Development Kit – OpenIoT-VDK (running Linux) with the complete OpenIoT platform pre-installed and preconfigured for use/development has been released. It can be downloaded from the OpenIoT github wiki: https://github.com/OpenIotOrg/openiot/wiki/Downloads. The Virtual Development Kit (OpenIoT-VDK) developed and implemented, features the OpenIoT latest release i.e. v0.1.1 and it's size is 5,7 GB. The OpenIoT-VDK facilitates the learning and use of the OpenIoT framework for an easy adoption and it is industry friendly under LGPL licence and totally open for academic purposes. The OpenIoT-VDK instance deploys the IoT service delivery model facilitating the validation of use cases by using the OpenIoT platform. The application areas are smart city, smart transport and mobility, smart health, smart living, smart manufacturing and smart buildings.

5.4 Energy

The IoT allows connecting and monitoring assets from virtually anywhere for the smart grids and energy sector using the interconnected edge devices and the utilities and energy consumers/prosumers have the opportunity and accessibility to improve energy efficiency and energy use. The smart grid is drastically changing the way businesses operate. Using IoT technology, utilities are equipped to deliver power more efficiently, improve operations, reduce emissions and management costs, and restore power faster, while operators are able to immediately identify outages, allowing for improved efficiency to manage responses.

The Internet of Energy (IoE) [13] provides an innovative concept for power distribution, energy storage, grid monitoring and communication. It will allow units of energy to be transferred when and where it is needed. The IoE concept requires web based architectures to readily guarantee information delivery on demand and to change the traditional power system into a networked Smart Grid that is largely automated, by applying greater intelligence to operate, enforce policies, monitor and self-heal when

necessary. This requires the integration and interfacing of the power grid to the network of data represented by the Internet, embracing energy generation, transmission, delivery, substations, distribution control, metering and billing, diagnostics, and information systems to work seamlessly and consistently.

The concept enables the ability to produce, store and efficiently use energy, while balancing the supply/demand by using a cognitive Internet of Energy that harmonizes the energy grid by processing the data, information and knowledge via the Internet. The Internet of Energy concept leverages on the information highway provided by the Internet to link devices and services with the distributed smart energy grid that is the highway for renewable energy resources allowing stakeholders to use green technologies and sell excess energy back to the utility. The concept has the energy management element in the centre of the communication and exchange of data and energy.

The COSMOS project [6] targets a particular problem in the Energy industry, which is the issue of inefficient heating schedules. Research shows us that residents, for example in Camden housing, tend to adopt bad habits in terms of Energy efficiency when it comes to turning the heating on and off. In order to tackle this problem, COSMOS components are used to analyse both historical and real-time data. This way it is possible to create a system where Heating Schedules not only can be learnt for individual Virtual Entities (VEs), but also be automated depending on the status of certain sensors. Furthermore, COSMOS exploits Social Aspects to help VEs learn from each other and share their Heating Schedules when appropriate.

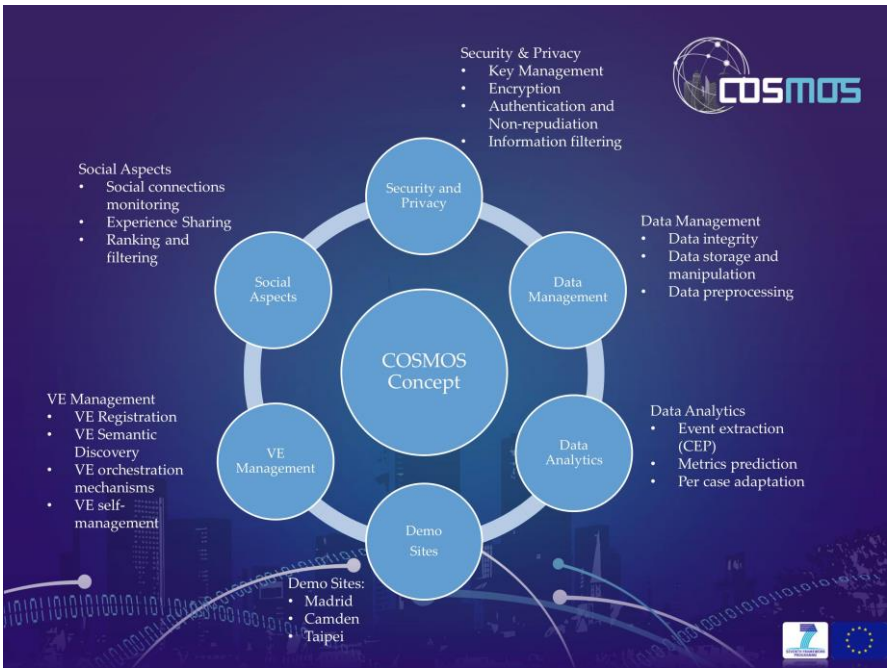

Figure 5.4: COSMOS Project Concept

The Internet of Energy for Electric Mobility (IoE) project [13] objective was to develop hardware, software and middleware for seamless, secure connectivity and interoperability achieved by connecting the Internet with the energy grids. The application of the IoE will be the infrastructure for the electric mobility. The underlying architecture is of distributed Embedded Systems (ESs), combining power electronics, integrated circuits, sensors, processing units, storage technologies, algorithms, and software. In this respect the "Internet of Energy" concept is defined as a network infrastructure based on standard and interoperable communication transceivers, gateways and protocols that allow a real time balance between the local plus the global generation and storage capability together with the energy demand, creating a high level of consumer awareness and involvement. The Internet of Energy converts the traditional power system into a network/grid that is largely automated, applying greater intelligence to operate, monitor and, heal itself when needed. By being Internet of Energy concept is a wider definition of Smart Grids, it includes a proactive role of DSO in deploying the needed field devices in the LV/MV grid to increase its observability.

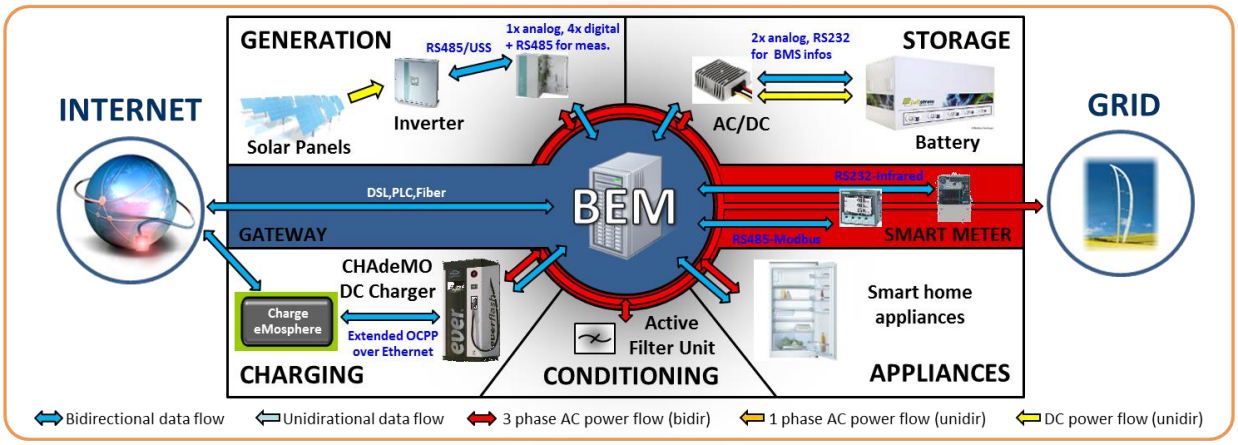

Figure 5.5: IoE Project Bidirectional Power and Communication Flow

This require the integration and interfacing between the power network represented by the grid and the data network represented by the Internet focusing on transmission, substation and distribution control, metering, substation monitoring and diagnostics and location information systems into seamless and coherent Internet of Energy implementation.

The project enabled the creation of value added services using both wired and wireless devices with access to the Internet by managing key topics: such as demand response, modelling/simulation, energy efficiency and conservation, usage monitoring, real time energy balance and billing. The project considers vertical integration and horizontal cooperation among energy utilities, OEMs, and hardware/software/silicon providers.

5.5 Farming and Food Security

IoT technology allows the monitoring and control of the plant and animal products during the whole life cycle from farm to fork. The challenge will be in the future to design architectures and implement algorithms that will support each object for optimal behaviour, according to its role in the Smart Farming system and in the food chain, lowering ecological footprint and economical costs and increasing food security.

iCore smart cold chain logistics domain implies high complexity and high risks because food and pharmaceutical goods are exposed to increasingly long and complex supply chains with many dangers of poor temperature control, delays and physical mishandling. The prototype improves the transportation process by monitoring the state of the products during transportation and by early warnings when the goods are not stored according to clients' requirements.

OpenIoT IoT-Large Scale Deployments – Phenonet trial describes the network of wireless sensor nodes collecting information over a field of experimental crops. The term “Phenomics” describes the study of how the genetic makeup of an organism determines its appearance, function, growth and performance. Plant phenomics is a cross-disciplinary approach, studying the connection from cell to leaf to whole plant and from crop to canopy.

The ebbits project [7] addressed food traceability as one of its important application domains - following the product through its complete lifecycle without interfering with existing stakeholder processes. The integration of the people manager covers the aspects of people in the Internet of Things, People & Services. During this period the project group started integration of the Digital Pen & Paper technology in the traceability scenario. ebbits promotes a paradigm shift towards the Internet of People, Things and Services (IoPTS), and allows a dynamic interconnection of smart objects, services and individuals. The

architecture can address "many2many" relationships between actors and sources of information, which compose a generic traceability chain.

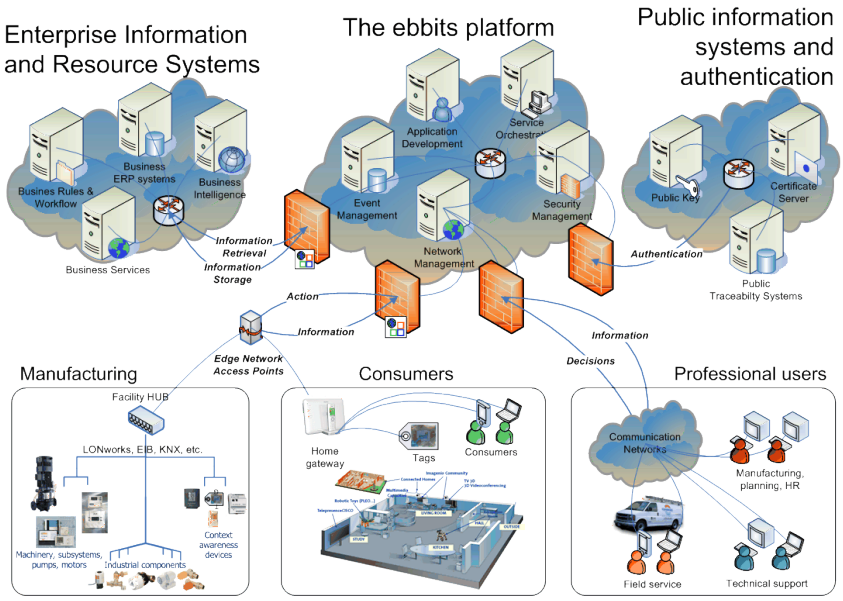

Figure 5.6: ebbits Project Concept

In food traceability ebbits allows to collect heterogeneous information about meat items along the different stages of the chain (farm, slaughterhouse, transportation, distribution and consumption), to integrate real time data from relevant monitoring and control systems and finally to include people in the loop. This has obvious benefits for farmers and all stakeholders across the distribution chain as well as for the end-users. It allows to face problems like the growing complexity of global supply chains, increasing user awareness, the management of food quality and food regulations e.g., about safety, ingredients, processes, packaging.

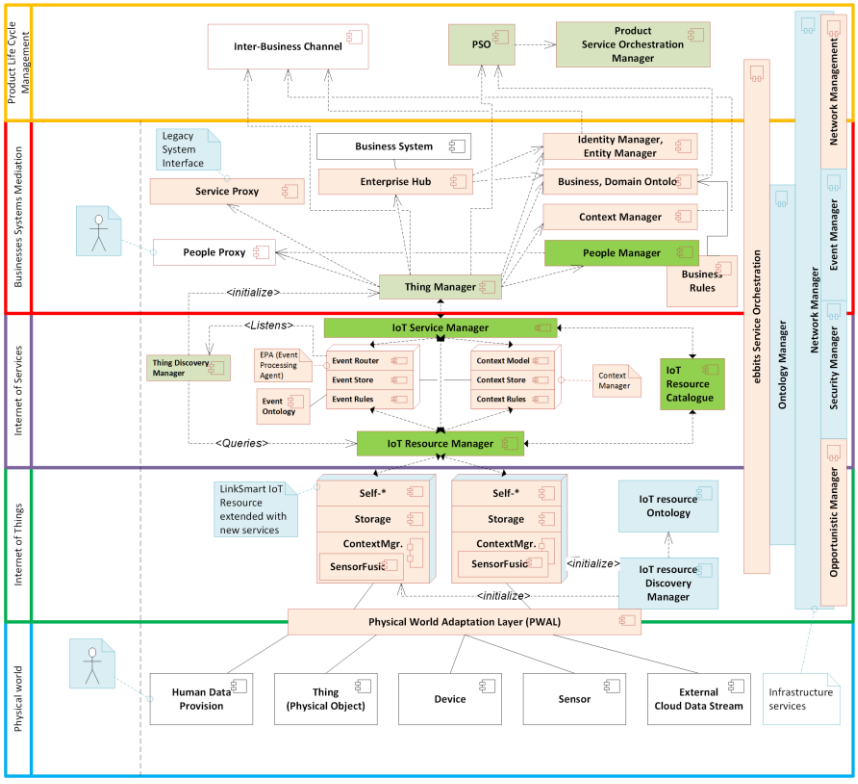

Figure 5.7: Overall Architecture

5.6 Wearables

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

5.7 Cities

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

The ALMANAC project [1] develops an IoT platform that promotes integrated smarter city processes for green, citizen-centric and sustainable urban ecosystems. The open software ALMANAC Smart City Platform (SCP) enables seamless integration of devices, services, and private and public data, as well as federation of existing services. This is achieved by using a set of basic building blocks that ease third-party application development. The SCP also enables interoperation of different communication networks and heterogeneous IoT technologies. Experimentation of selected Smart City services and applications will be carried in the city of Turin, Italy. The application areas for the project are the smart city, water management, waste management and provides a citizen centric solution to these application areas.

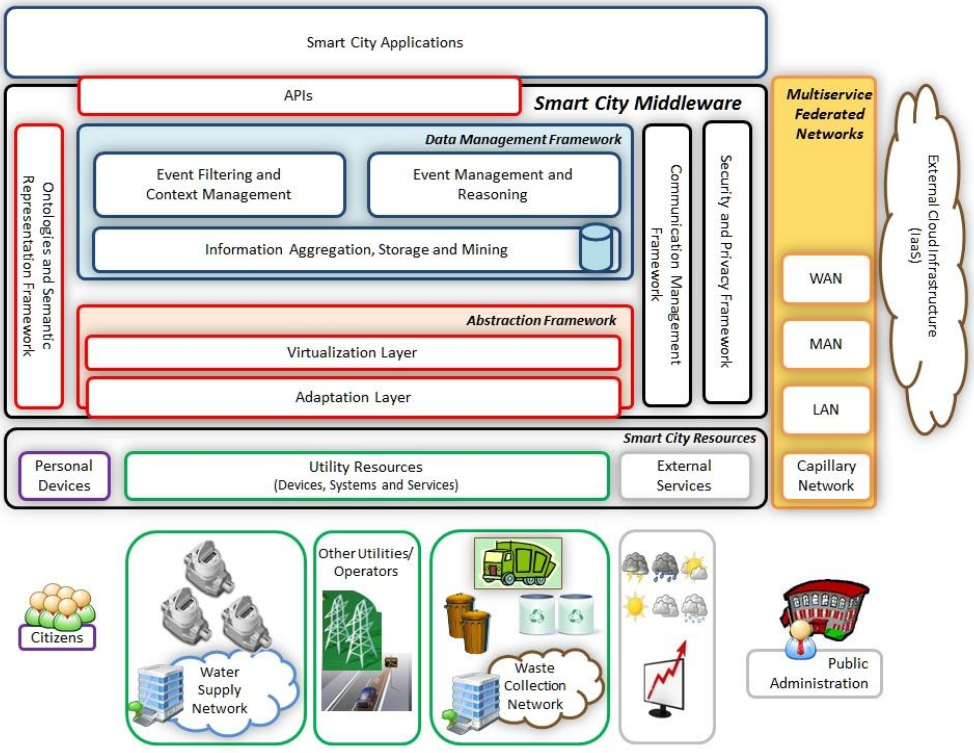

Figure 5.8: ALMANAC Project Concept

ALMANAC is currently developing a field trial in Turin, Italy, implementing an innovative waste collection system. The deployment foresees the installation of fill-level sensors in two selected Underground Ecological Islands (UEI), controlled access modules for a subset of the monitored waste bins in the selected UEIs, and weight sensors on-board of the waste collection trucks. The trial will involve the 350 private households and 50 commercial activities that use the UEIs selected.

The smart waste collection field trial integrates information from an issue reporting and management application developed by the project using the ALMANAC SCP, which enables citizens to report issues and irregularities in the waste management service. The same application provides a feature that, based on information from sensors deployed in the field and feedback from citizens, allows waste collection routes modification and can be used by the service operator to optimize the waste collection service.

The Smart Water Capillary Network provides the infrastructure to collect the data originated by different devices (sensors, meters, etc.) and ensures their collection in an ETSI M2M compliant service platform. The PoC consists of a smart water meter (flow meter and Ph sensor) sending data periodically using standard protocol - through a concentrator with IP connection - to the ALMANAC SCP, enabling both real-time and historical monitoring of water consumption data.

The Collaborative Citizen-centric application provides access to open public data and integrate third-party services relevant to the citizens with other services provided by the platform.

Throughout its execution, the ALMANAC project develops four main tangible assets that could be further exploited within the context of the Large Scale Pilots call. The first asset is the overall waste management trial described above, while the remaining three assets are specific technological components:

- The overall waste management trial described above could be further extended in the city of Turin as well as elsewhere. The trial already involves key stakeholders from the ALMANAC Consortium as well as technology and service companies that, even though they are not part of the ALMANAC Consortium, have been engaged to create an ecosystem and are participating in the trial.
- The ALMANAC SCP provides device abstraction, data management and virtualized access to heterogeneous resources in a Smart City. The platform enables easier, reliable and more scalable development of Smart City applications, with almost no coupling with real-devices. Access to all ALMANAC virtualization and processing features is enabled by a set of open cloud-based APIs that provide application developers with a unique interface to the SCP. This is seen, on one hand, as a way to foster adoption of the SCP and, on the other hand, as a vehicle to create a future Smart City Data and Applications marketplace, which can be shared among Smart Cities to exchange knowledge, practices and competences.
- As part of the Smart City platform, ALMANAC develops a Federated Cloud: an open federated architecture of cloud services to enable elasticity of storage services. The federation exposes software gateways to provide access to different logical parts of the smart city structure supporting efficient aggregation, processing, querying and analysis of smart city data.
- ALMANAC develops also an M2M platform that is a “lightweight” implementation of the ETSI standard, integrated with the higher functional layers of the ALMANAC Smart City Platform and using a scalable and multi-server architecture. It allows deploying the ETSI M2M in heterogeneous and complex Smart City ecosystems.

The ClouT joint European-Japanese project [4], is leveraging the Cloud Computing as an enabler to bridge the Internet of Things with Internet of People via Internet of Services, to establish an efficient communication and collaboration platform exploiting all information sources to make the cities smarter and to help them facing the emerging challenges such as efficient energy management, economic growth and development.

ClouT, which stands for “cloud of things”, is providing infrastructure, services, tools and applications that will be used by municipalities, citizens, service developers and application integrators to create, deploy and manage applications that take advantage of the latest advances in the Internet of Things (IoT) and Cloud domains.

The project aims at providing a reference Cloud + IoT architecture and developing its instances to be deployed in 4 pilot cities: Santander, Genova, Fujisawa and Mitaka. The applications areas are covering smart cities, safety and emergency management, smart transport and mobility, citizen centric and smart living.

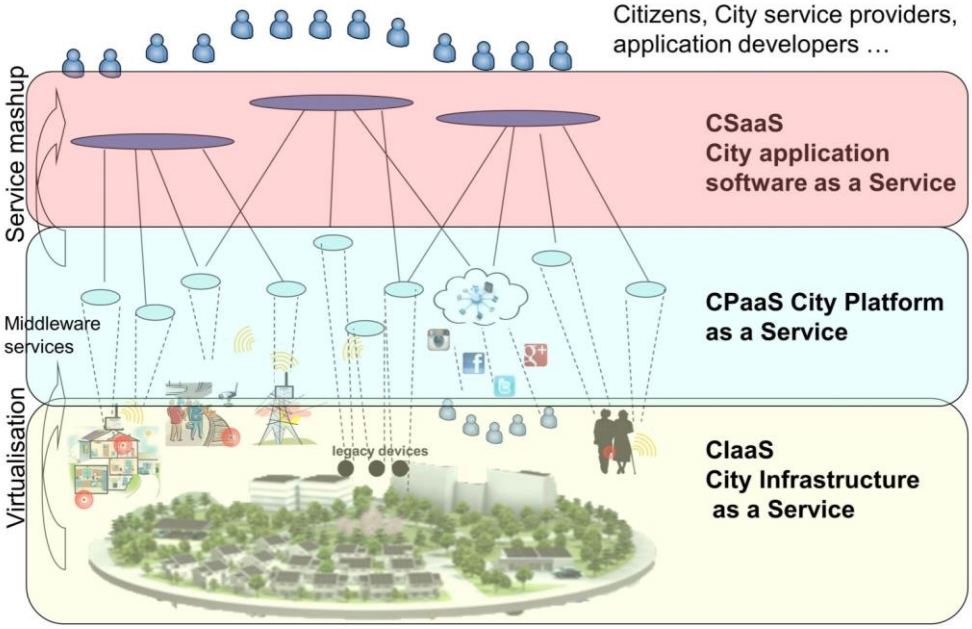

Figure 5.9: ClouT Project Concept

The CityPulse project [5] aims to design, develop and test a distributed framework for semantic discovery, processing and interpretation of large-scale real-time Internet of Things and relevant social data streams for knowledge extraction in a city environment. Project approach subjects like event detection for urban data streams, conflict resolution and fault recovery on IoT data based on semantic modelling and knowledge representation of IoT data streams leveraging advanced platform features such as knowledge extraction and events processing in IoT data streams or data mash-up and self-configuration.

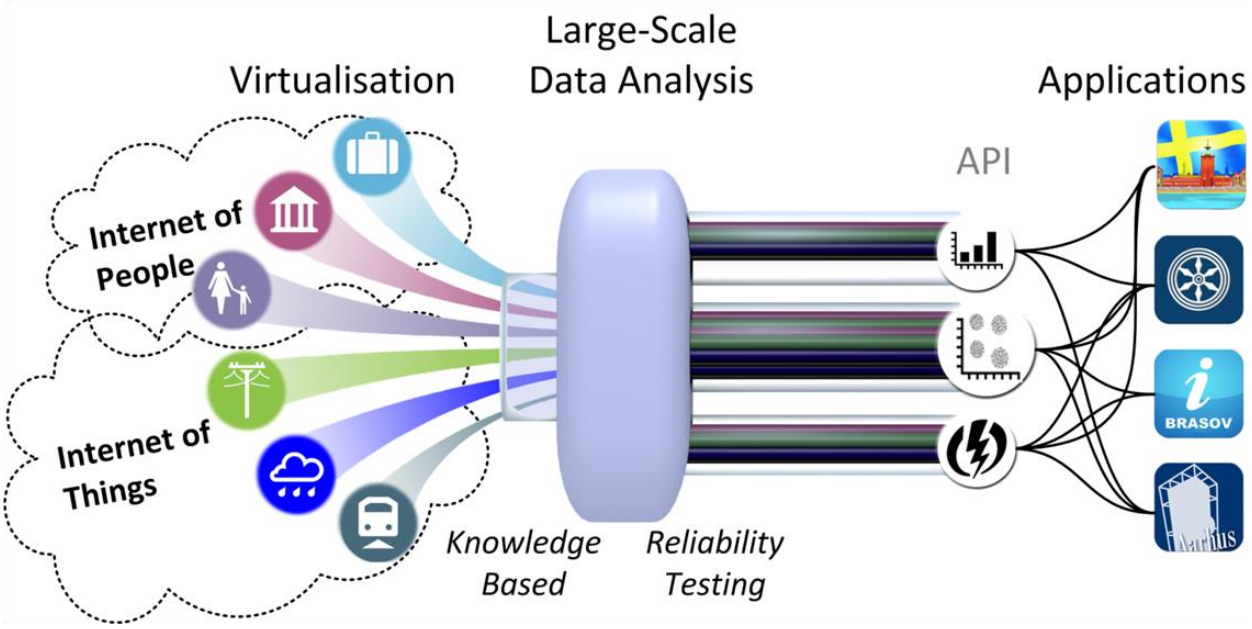

Figure 5.10: CityPulse Project Concept

Based on a public collection and selection of use case scenarios project implements in peer cities of Aarhus (Denmark) and Brasov (Romania) use cases like route planning optimization and parking places efficient usage aiming improvement in urban mobility and environment protection.

The FIEST project [8] goal is to open new horizons in the development and deployment of IoT applications and experiments at the EU and beyond boundaries (global scale), based on the interconnection and interoperability of diverse IoT platforms and testbeds.

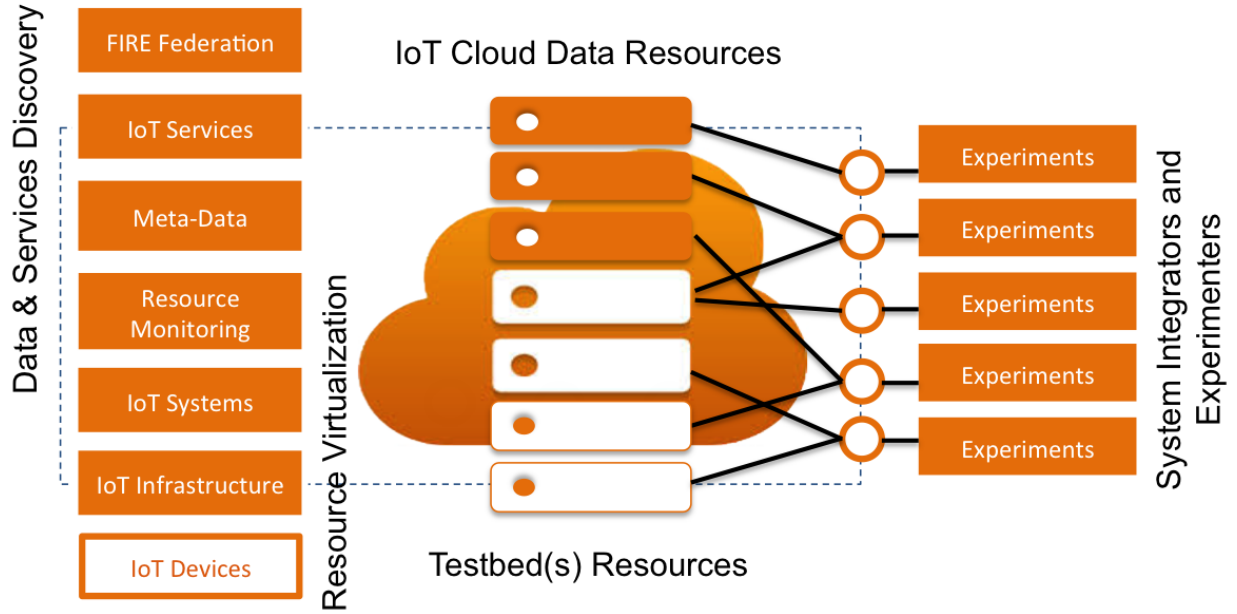

Figure 5.11: FIESTA Project Concept

The FIESTA project's experimental infrastructure will provide to the European experimenters in the IoT domain with the following unique capabilities: i) sccess to and sharing of IoT datasets in a testbed-agnostic way.

FIESTA aims to provide to researchers with tools for accessing IoT data resources (including Linked sensor data sets) independently of their source IoT platform/testbed; ii) enable execution of experiments across multiple IoT testbeds, based on a single API for submitting the experiment and a single set of credentials for the researcher, iii) portability of IoT experiments across different testbeds, through the provision of interoperable standards-based IoT/cloud interfaces over diverse IoT experimental facilities. capabilities from multiple testbeds. The FIESTA infrastructure will enable experimenters to use a single EaaS API (i.e. the FIESTA-IoT EaaS API) for executing experiments over multiple IoT federated testbeds in a testbed agnostic way i.e. like accessing a single large scale virtualized testbed.

iCore Smart urban security and VIP protection demonstrator is based on a surveillance system focused on VIP protection during a visit within a big and crowded exhibition area. Police Control and Command (C2) truck close to the area with dedicated surveillance applications is monitoring the VIP visit through a deployed wireless (video and chemical) sensors network also connected to exhibition area CCTV system and chemical sensors. When a dirty bomb explodes generating toxic cloud dispersal, VIP evacuation is triggered and managed up to a decided exit according to threats tracking (toxic cloud, crowds). iCore cognitive platform embedded in C2 truck manages in real time optimal selection of video streaming and use of available WSN bandwidth.

OpenIoT IoT-Smart City Crowdsensing Quality of Air Monitoring trial is realized through an opportunistic Mobile Crowdsensing application involving volunteers carrying smartphones and air quality sensors that contribute the sensed data to the OpenIoT platform.

The RERUM project [18] increases the trustworthiness of IoT providing an overall security, privacy, reliability and trust framework to address the citizens' requirements for advanced, reliable, resilient and secure smart city applications that respect their privacy improving both devices and middleware functionalities. ReMote is a hardware IoT platform fully designed and developed based on the requirements set by the RERUM project. It is both powerful and low power so that it can run the device-

embedded security, privacy and reliability RERUM mechanisms, while consuming very low energy. The application areas focus on smart cities exemplified through smart transport and mobility, smart environmental monitoring and smart building/ smart energy.

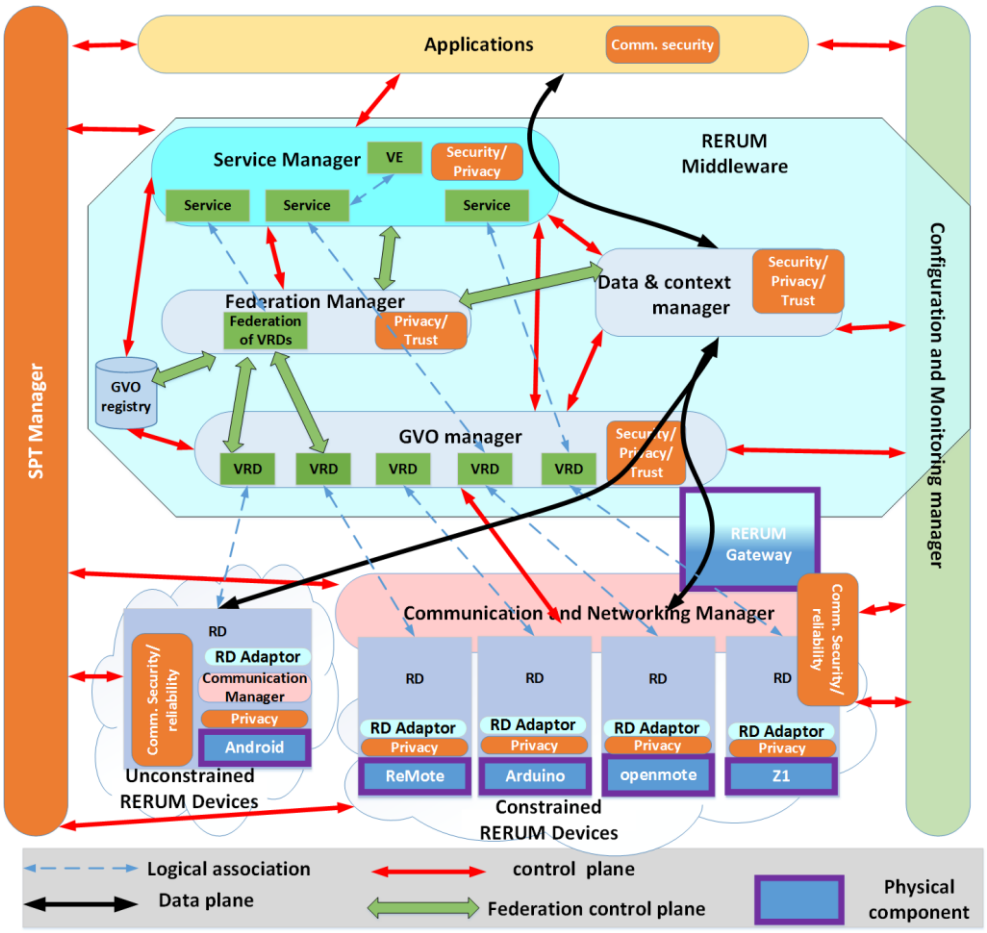

Figure 5.12: RERUM Project Concept

5.8 Mobility

The connection of vehicles to the Internet gives rise to a wealth of new possibilities and applications, which bring new functionalities to the individuals, and/or the making of transport easier and safer.

In this context, the concept of Internet of Vehicles (IoV) represents the future trend for smart transportation and mobility applications combining vehicle to vehicle and vehicle to infrastructure communication.

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

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

ClouT project has organised 2 mobility related trials in Fujisawa, Japan: “Eno-kama Info Surfboard” and “Smile Coupon”. These two applications are based on ClouT architecture and are deployed in Kamakura station in cooperation with Enoshima Electric Railway Co.,Ltd. While “Surfboard” is providing city context information for tourists in real-time, “Smile coupons” detects the degree of your smile and provides discounts at the local shops of your destination. The more you smile the more you have discount.

Figure 5.13: ClouT Smile Coupon Deployment in the Eno-Kama Station

ClouT Santander mobility field trial is designed to enable citizens and visitors to get access to enhanced urban mobility experience and to leverage city transportation resources efficiently. Through a single application, it is possible to obtain information related to public buses fleet, bikes, taxis, trains, traffic parameters as well as with environmental indicators.

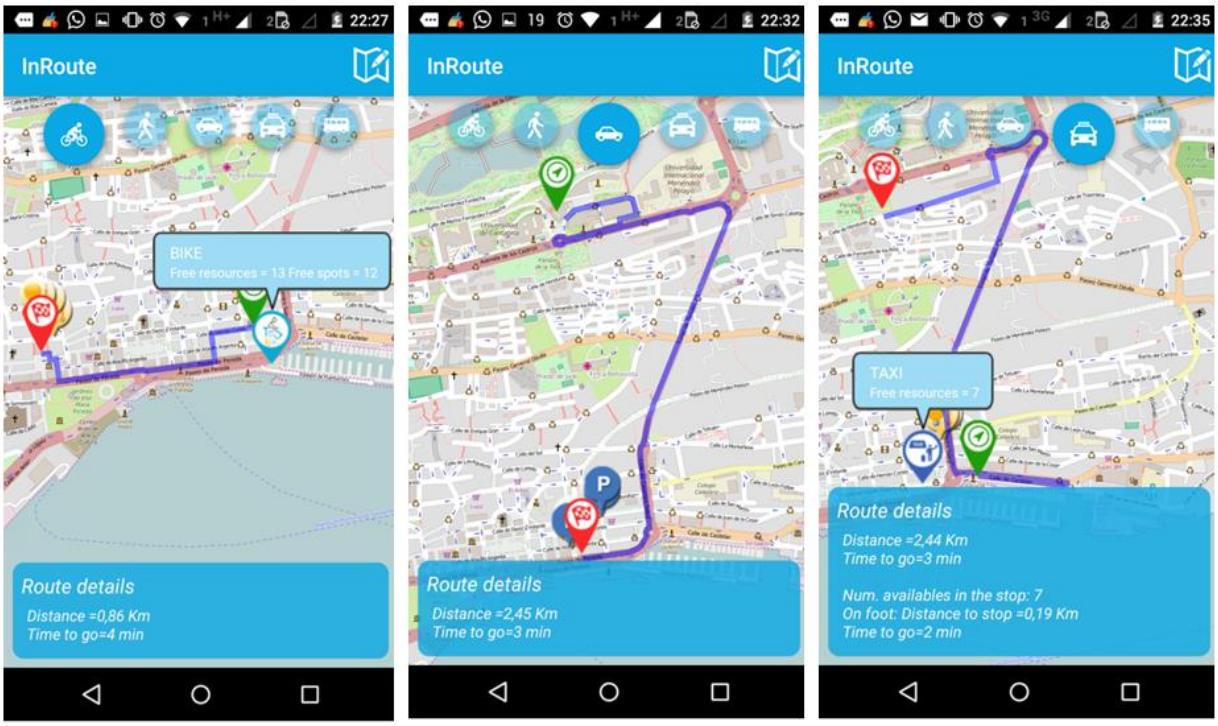

Figure 5.14: ClouT Santander Mobility Application

The IoE presented the end-to-end demonstration of electro mobility ecosystem and vehicle to grid (V2G) related technologies. Bidirectional power flow between vehicles and the grid the interaction between the different e-mobility actors and smart grid communication technologies and services were developed and demonstrated.

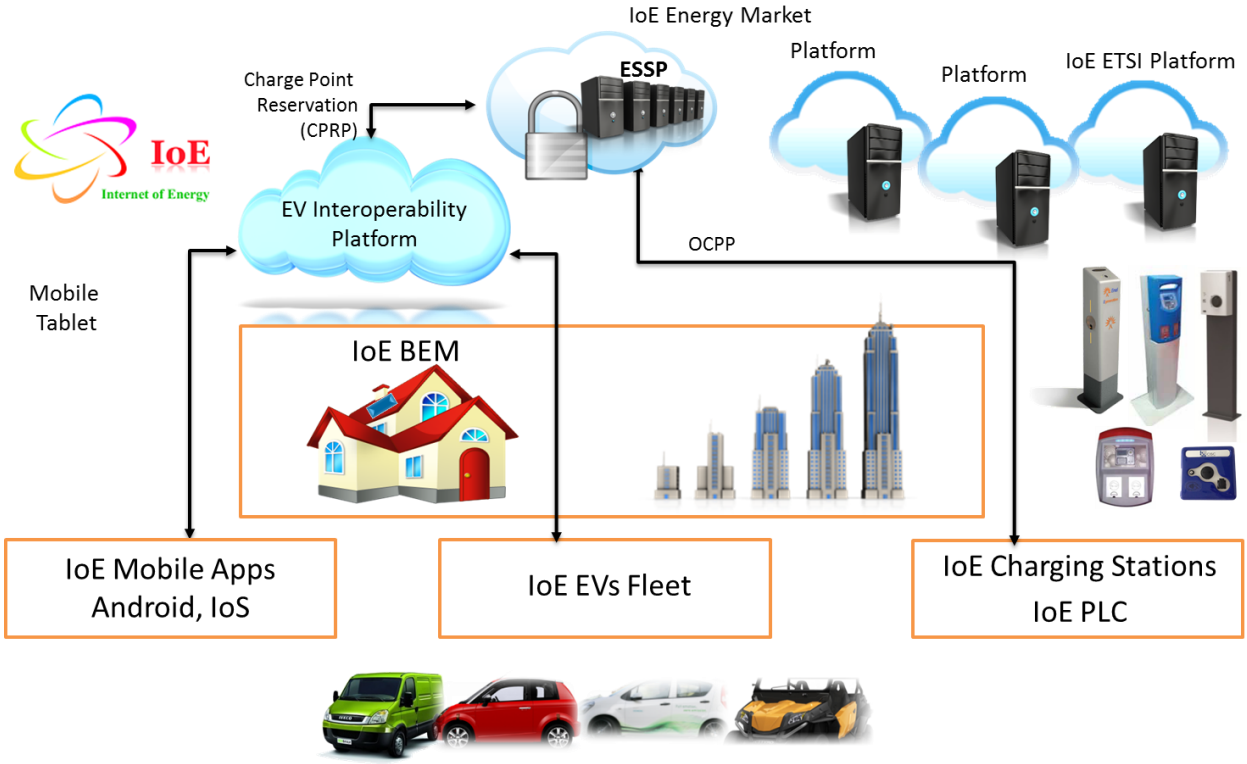

Figure 5.15: IoE Project Convergence of Platforms for Electric Mobility Applications

The SEAM4US project [19] objective was to develop advanced technologies for the optimal and scalable control of metro stations capable of producing energy savings of at least 5% in non-traction electricity consumption in one year. In other words, the equivalent of the electricity consumed in over 700 households in one year.

The main outcome of the project is the creation of systems for optimized integrated energy management and, the development of a decision support system for driving mid-term investments. SEAM4US integrated additional energy metering and sensor-actuator networks within existing systems by means of LinkSmart® middleware as abstraction layer, to acquire grounded user, environmental, and scheduling data. The data collected is used to update and enable a set of adaptive energy consumption and environmental models; models then used to proactively and optimally controlling metro stations.

Passeig de Gracia, one of the historic stations of the metro network in Barcelona, junction point of three underground railways, was used as the pilot station for testing and validating the systems. The result was an energy saving of at least 21% in the condition maximising passenger comfort and up to 38% in the strategy maximising energy savings in the controlled systems, leading to an overall energy saving of 13% in the maximum comfort condition and up to 23% in the maximum saving condition.

RERUM smart transportation pilot utilizes mobile devices to gather traffic information throughout city areas in a privacy-preserving way, without disclosing any type of personal information of the users from their mobile phones. The application includes mechanisms for geo-location privacy, data minimization, obfuscation of data, anonymisation, etc. to ensure that no personal user data are sent from the devices and that the RERUM Middleware transmits only statistical information to the application. For the pilot in Heraklion, the devices will be installed mainly on buses that traverse around the city area to measure the traffic at specific roads. Volunteer citizens will also be able to participate in the pilot by downloading the RERUM application and installing it on their devices as they move around in the city. A web server application has also been developed for the visualization of the traffic data in a privacy preserving way.

The SMARTIE project [20] works on security, privacy and trust for data exchange between IoT devices and consumers of their information. Results are demonstrated in smart cities in Germany, Serbia and Spain. The vision of SMARTIE is to create a distributed framework to share large volumes of

heterogeneous information for the use in smart-city applications, enabling end-to-end security and trust in information delivery for decision-making purposes following data owner's privacy requirements. The application areas addressed are smart cities and smart transport and mobility.

SMARTIE augmented reality based smart transport service demonstrator addresses the improving of the management of the public transportation network in the city of Novi Sad to promote and encourage the use of sustainable transport modes and to provide time and cost benefits to travellers. The demonstrator is implemented on two routes within a city public bus transport network operated by a local transport company JGSP. Bus stops are equipped with the Augmented Reality (AR) markers in the form of an image (e.g. logo or QR code). Devices to measure air pollution in the busses, an e-ticketing system and a mobile app providing touristic information and event suggestion, are expected to be integrated to the pilot.

The VITAL project [23] is developing a novel virtualization layer for the next generation of integrated and technology independent smart city operating systems in Europe. It offers semantic interoperability across IoT data and services stemming from different legacy IoT systems. In this way, VITAL facilitates the integration of the wide range of vertical (silo) smart city applications, which have been developed independently from each other. The project's application areas include smart working and urban mobility.

VITAL's IoT-supported pilot on smart working is hosted in London's first Business Improvement District (B.I.D), namely CTU, in the Camden Borough of London. CTU is providing an app, which enables (roaming) workers to locate appropriate workplaces within the city, taking into account the facilities available at the workplaces, along with a wide range of sensor-provided parameters.

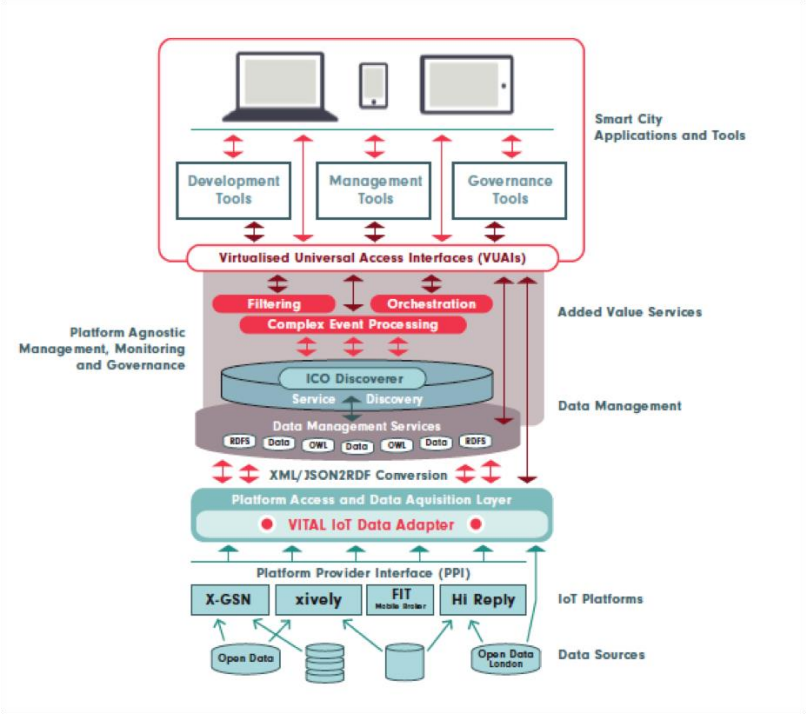

Figure 5.16: VITAL Project Architecture

VITAL's IoT-enabled smart traffic management pilot is addressing the development and validation in the city of Istanbul. Traffic management and analysis functionalities are based on multi-source data sets. They include functionalities for traffic prediction and incident detection (e.g., malfunctioning sensors/systems), based on IoT analytics over data streams stemming from the hundreds of sensors that are deployed in the city. End-users of the traffic management functionalities include citizens and the city authorities.

BUTLER SmartParking trial addresses a smart parking management system. A group of users tested during various days the SmartParking devices, the reservation system and the mobile app.

BUTLER SmartTransport trial is enabling public transportation systems use without taking care of pricing or ticketing leveraging on IoT solutions (i.e. e-ticketing, save child group monitor and tags). Real field trial took place in collaboration with TU Dresden ITVS and Fraunhofer IVI at AutoTRAM Extra Grand.

iCore transportation trial demonstrates the virtualization and use of ICT objects in Automotive industry, to create, configure and use mobility functions and services while driving and, in a seamless way, also in pre-trip and post-trip services, linking to smart home and smart meeting. Although the focus is on a single driver, data provision from several cars will also be addressed, for the mobility management in a smart city. Major aspects and challenges are the availability of objects within the vehicle and from the outside world, considering the vehicle as a complex and autonomous eco-system and not an always-connected environment. Another topic addressed is context awareness using cognitive technologies.

COSMOS will test how IoT technologies improve journey experience of passengers with special needs, while also simplify the work of caregivers. Passengers with special needs such as children, elderly, disabled, and the like, may choose using the bus transportation system if they get assistance from the beginning to the end of their journey. Assistance would come in the form of a caregiver helping passengers planning their journey, tracking passenger's progress, and even handing off to a new caregiver who would be waiting at their destination.

COSMOS enables this application by simplifying the communication schemes between the multiple components that are required for the decision-taking procedure that will help passengers with special needs to take the optimal route from their initial point to their destination. The COSMOS Message Bus, in collaboration with the µCEP Engine and the data efficient storage procedure defined in the project, supports the application of Machine Learning techniques to predict the evolution of city behaviour so to deliver events that are mapped into actions and orders for passengers and caregivers.

5.9 Environment

IoT solutions are built for many vertical applications such as environmental monitoring and control that use sensors to assist in environmental protection by monitoring air, water quality, atmospheric or soil conditions and noise pollution. IoT applications are addressing earthquake or tsunami early-warning solutions used by emergency services to provide more effective and rapid reaction.

ClouT Genova field trial, "I don't risk" aims informing citizens about good practices and general information about environmental risks and emergency situations, by using environmental data from weather sensors, hydrometers, webcams, etc. With additional features added in 2015, it has become the top mobile application of the Genova City with more than 4000 downloads and average rating of 4/5 based on 51 reviews.

Figure 5.17: Hydorlogical Risk Areas in Genova and a Screenshot of the ClouT Application

ClouT project has also deployed an environmental monitoring application by equipping garbage collection cars with environmental sensors (CO, O3, NO2, pollen, luminance, humidity, UV, temperature and ambient noise). By having equipped garbage collection cars, the Fujisawa municipality is able to provide citywide information of the atmosphere to citizens and visitors in Fujisawa city.

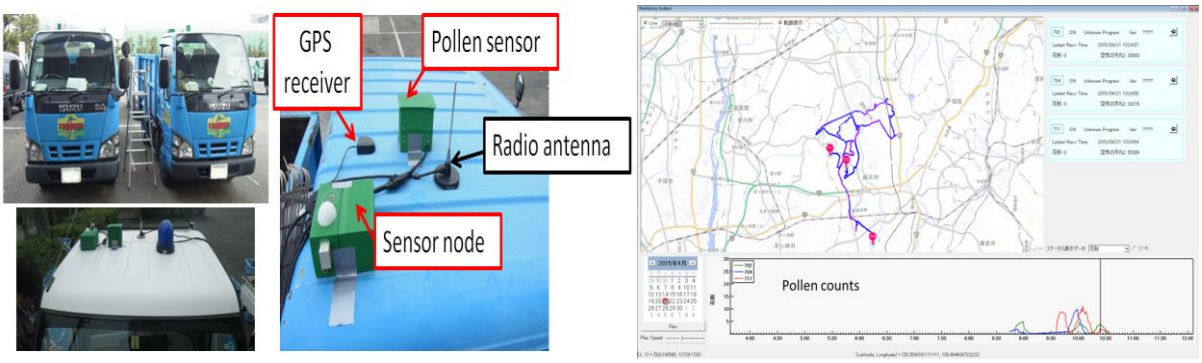

Figure 5.18: Sensor Equipped Garbage Collection Cars

RERUM's smart Environmental Monitoring pilot deals with the deployment of a secure and reliable system for gathering environmental pollution and weather related measurements throughout city areas. This is done in a secure and trustworthy way either by deploying sensor nodes at specific fixed locations or by installing sensors on top of buses and gathering the measurements at every bus stop. The goal is to ensure that no malicious users can intervene in the transmission of the measurements or gain unauthorized access to the system services. The pilot includes several mechanisms for secure communications, i.e. integrity protection to ensure that no intermediate node will alter the data (in multihop deployments), compressive sensing based data gathering and transmission for achieving both lightweight data encryption and compression for minimizing energy consumption, DTLS-based secure communication, etc. Furthermore, the trust framework ensures that no data from malicious or malfunctioning devices will be taken into account improving the trustworthiness and the reliability of the system. Finally, Cognitive-Radio inspired IoT gateways will be utilized for improving the spectrum efficiency of the deployments.

SocIoTal project [21] designs key enablers for a reliable secure and trusted IoT environment facilitating the creation of a socially aware citizen-centric Internet of Things. It takes a citizen-centric approach towards creation of large-scale IoT solutions of interest to the society. SocIoTal provides secure and trusted tools that increase user confidence in the IoT environment. The applications areas covers the smart city, smart living and citizen-centric services.

SocIoTal Santander and Novisad trials are enabling citizens and developers to develop new services using SocIoTal toolset. The initial set of trials is based on the output from co-creation workshops and the IoT meetups held in several cities. Examples are monitoring of lifts in the buildings, measuring happiness of a city as well as sharing data generated by citizen owned devices and navigating through the routes accessible to disabled people.

5.10 Manufacturing

The role of the IoT is becoming more prominent in enabling access to devices and machines, which in manufacturing systems, were hidden in well-designed silos. This evolution will allow the IT to penetrate further the digitized manufacturing systems. The industrial IoT will connect the factory to a completely new range of applications, which run around the production. This could range from connecting the factory to the smart grid, sharing the production facility as a service or allowing more agility and flexibility within the production systems themselves. In this sense, the production system could be considered one of the many IoTs, where a new ecosystem for smarter and more efficient production could be defined.

One key enabler to the IoT-driven smart and agile manufacturing lies in the way the applications manage and access the physical world, where the sensors, the actuators, and the production units operate. These devices provide their services in a structured manner, and can be managed and orchestrated for a multitude of applications running in parallel.

OSMOSE project [17] provides a roadmap and a technology platform that should support the transition and implementation of European SMEs of new business models and strategies in the digital world. The impact of OSMOSE is to provide already a middleware that is capable of addressing an increased asset

connectivity to a digital enterprise. Through sensing enterprise capabilities OSMOSE should unlock new business models opportunities. The application area is smart manufacturing.

OSMOSE applications for aerospace domain offers a proof of concept referred to a product operations monitoring and control use case using the flight simulators in AgustaWestland Italy. The goal of this PoC is to assure the training continuity and continuously improve the system reliability focusing on software snags faster assessment, resolution, and hardware faults prevention.

OSMOSE applications for manufacturing in automotive domain addresses an Engine Power Components (EPC) pilot in Spain as a proof of concept of OSMOSE. The proposed PoC is dedicated to manage the whole production process of camshafts, from its provisioning to its production, distribution and remanufacturing, if needed. The camshaft will be digitalized from its origin to its destination and all this information will be stored to keep the track of the whole life cycle of a camshaft, reducing the risk of delivering camshaft with defects and having more data available to make decisions in real time about the changes in the process.

OpenIoT IoT-Intelligent Manufacturing – Smart Industry trial addresses the means for dynamically selecting production process monitoring sensor information, as well as for structuring this information on KPIs and make them available in form of customized and created on the fly. Validated in the paper/ packaging industry in processes like printing, die cutting and gluing/folding.

The ebbits project [7] aimed to develop architecture, technologies and processes, allowing businesses to semantically integrate the Internet of Things into mainstream enterprise systems and support interoperable real-world, on-line end-to-end business applications.

ebbits provides semantic resolution to the Internet of Things and hence presents a new bridge between backend enterprise applications, people, services and the physical world, using information generated by tags, sensors, and other devices and performing actions on the real-world.

The ebbits platform allows efficient creation of innovative product services. During a product's life cycle phases ebbits collects real-world data from a variety of Internet of Things sources and feeds it into business systems for optimized production and increased consumer confidence in final product.

Starting from the set of measurements that tracks availability, performance and quality output of the plant equipment, it is possible to create a new overall KPI taking into account the energy consumption of the manufacturing process, named OEEE (Overall Equipment and Energy Efficiency). A business framework for online OEEE applications for production and energy optimization in real automotive manufacturing environments has been defined and OEEE metrics has been developed. The integration of recent products applied in the car body shops and powertrain assembly shops has been realized. Attention was put to the usability of the end-user applications with further analysis of SCADA/HMI integration and usability.

The BEMO-COFRA project [2] is an EU-Brazil Project that aimed to develop an innovative distributed framework, allowing networked monitoring and control of large-scale complex systems by integrating cooperating heterogeneous smart objects, legacy devices and sub-systems, to support holistic management and achieve overall systems' efficiency with respect to energy and raw materials.

The BEMO-COFRA framework supports the adoption of large-scale networks composed of heterogeneous smart objects provided with sensing and actuating capabilities and able to meet specific monitoring and control application requirements in terms of quasi-real time or real-time constraints. In the WSAN section of the framework, this is done by integrating devices adopting heterogeneous wireless communication technologies such as Wi-Fi, BlueTooth, and IEEE 802.15.4-based technologies. The WSAN developed by BEMO-COFRA features also the flexibility, reliability, availability and manageability characteristics that are of paramount importance to support dependable operations in harsh environments.

The achievements of the BEMO-COFRA project was demonstrated deploying the BEMOCOFRA framework in the challenging scenario represented by a manufacturing plant in Recife, Brazil where dependability of the system is of utmost importance and where a very large number of devices, systems,

WSAN devices interact and actively cooperate with each other to attain a very accurate observation of production processes

6 Recommendations

The Internet of Things is a new digital revolution and the applications of IoT can deliver benefits to key areas such as, healthcare, wearables, agriculture, water management, transport, buildings, energy manufacturing and smart cities.

The IERC has work on the last years with many projects that have developed IoT technology and applications. In this context the recommendations for the implementation of IoT LSPs is summarised as:

- Use as reference for the LSPs the results of the IERC projects that addressed IoT technologies and applications research, development and deployment.
- In order to fulfil the end-to-end security principles and IoT inherent requirements, a distributed approach seems to be the most suitable to be used for the different implementations in the IoT LSPs.
- Provide IoT technical solutions that minimizing the amount of data collected and encrypting the data that is collected, while allow the end-user to know what data is collected and how it is used.
- The end-user/consumer privacy solutions used in the IoT LSPs will require privacy by design scalable and context aware mechanisms for securing the personal data of individuals as the things they use become increasingly digitized.
- Development of specific "Privacy and Security by Design" approach needs to be considered as required by the LSPs, reflecting the content of the AIOTI Privacy Knowledge base developed by AIOTI WG04.
- Provide standard-based and interoperable IoT implementations for the LSPs in the different application domains and across the vertical domains.
- Create strong IoT ecosystems where the stakeholders will work together to develop standard-based, interoperable IoT solutions that can demonstrate compliance with specific standards or other standard-based IoT solutions. Align these activities with the work done in AIOTI WG03.
- Evaluate the opportunities, risks, and benefits of deploying IoT applications and solutions in the different LSPs by creating a cross-functional work package to identify, evaluate, and prioritize the most relevant IoT use-cases, scenarios and business value for the LSP in the specific domain. The selection should analyse the unique value proposition, regulatory environment, and IoT technology and the added value profitable opportunities across the value chain in the LSPs.
- Identify key technology components necessary for IoT solution deployment success. End-to-end solution implementation/deployment will require different technical elements, including sensors/actuators, intelligent edge devices/nodes, intelligent multi-functional gateways, network infrastructure, edge computing, security/privacy solutions, applications, and analytics services.
- Evaluate and test new disruptive technologies enabling seamless IoT solutions in the LSPs and cover the full scope of IoT systems creating strong IoT ecosystems for the LSPs.
- Sustainability of the LSPs.
- End-user involvement in the LSPs.

7 References

[1] ALMANAC EU Project, “ALMANAC Project Website,” online at http://www.almanac-project.eu/news.php.

[2] BEMO-COFRA EU-Brazil Project, “BEMO-COFRA website”, online at http://www.bemo-cofra.eu.

[3] BUTLER EU Project, “BUTLER Project Website,” online at http://www.iot-butler.eu/.

[4] ClouT EU Project, “ClouT project website,” online at http://clout-project.eu/.

[5] CityPulse EU Project, “CityPulse project website,” online at http://www.ict-citypulse.eu.

[6] COSMOS EU Project, “COSMOS project website,” online at http://iot-cosmos.eu/.

[7] ebbits EU Project, “ebbits Project Website,” online at http://www.ebbits-project.eu.
[8] FIESTA-IoT EU Project, “FIESTA-IoT project website,” online at http://www.fiesta-iot.eu.
[9] FITMAN EU Project, “FITMAN project website,” online at http://www.fitman-fi.eu.
[10] GAMBAS EU Project, “GAMBAS project website,” online at http://www.gambas-ict.eu/.
[11] iCore EU Project, “iCore Project Website,” online at http://www.iot-icore.eu/.
[12] IERC, "IERC Website,” online at http://www.internet-of-things-research.eu/.
[13] IoE ECSEL/ARTEMIS Project, “IoE Project Website,” online at http://www.artemis-ioe.eu/.
[14] IoT-A EU Project, “IoT-A Project Website,” online at http://www.iot-a.eu.
[15] IoT.est EU Project, “IoT.est Project Website,” online at http://ict-iotest.eu/iotest/.
[16] OpenIoT EU Project, “OpenIoT Project Website,” online at http://www.openiot.eu/.
[17] OSMOSE EU Project, “OSMOSE Project Website,” online at http://www.osmose-project.eu/.
[18] RERUM EU Project, “RERUM Project Website,” online at https://ict-rerum.eu/.
[19] SEAM4US EU Project, “SEAM4US Project Website”, online at http://seam4us.eu.
[20] SMARTIE EU Project, “SMARTIE Project Website,” online at http://www.smartie-project.eu/.
[21] SocIoTal EU Project, “SocIoTal Project Website,” online at http://sociotal.eu/.
[22] SMART-ACTION EU Project, “SMART-ACTION Project Website,” online at http://www.smart-action.eu.
[23] VITAL EU Project, “VITAL Project Website,” online at http://vital-iot.eu/.
[24] ISO 9646: “Conformance Testing Methodology and Framework”.
[25] Conceptual interoperability, online at https://en.wikipedia.org/wiki/Conceptual_interoperability.
[26] Mauritius Declaration on the Internet of Things, Balaclava, 14 October 2014, online at http://privacyconference2014.org/media/16596/Mauritius-Declaration.pdf.
[27] Opinion 8/2014 on the on Recent Developments on the Internet of Things, Article 29 Working Party on Data Protection, 14/EN, WP 223, 16 September 2014, online at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.
[28] Internet of Things – Privacy & Security in a Connected World, FTC Staff Report, January 2015, online at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
[29] OWASP Internet of Things Top Ten Project, online at https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project.

Editors:

Ovidiu Vermesan, SINTEF, Norway, Peter Friess, EC, Belgium

ContributingProjects:

ALMANAC, BUTLER, CityPulse, COSMOS, Com4innov, ebbits, FIESTA, FIESTA FITMAN, iCore, IoE, IoT.est, OpenIoT, OSMOSE, RERUM, SOCIOTAL, SMARTIE, VITAL,

Additional Contributing Experts:

Maurizio Spirito, ISMB, Italy
Claudio Pastrone, ISMB, Italy
Levent Gurgen, CEA-LETI, France
Jose Antonio Galache, Universidad de Cantabria, Spain
Sergio Gusmeroli, TXT e-solutions, Italy
Gabriella Monteleone, Piksel, Italy
Elias Tragos, ICS-FORTH, Greece
Klaus Moessner, Surrey University, UK
Srdjan Krco, DunavNet, Serbia
John Soldatos, Athens Information Technology, Greece
Martin Serrano, INSIGHT Centre, Ireland
Bertrand Copigneaux, Inno Group, France
Raffaele Giaffreda, CREATE-NET, Italy
Vera Stavroulaki, UPRC, Greece
Massimo Barozzi, TRILOGIS, Italy
Byoungoh Kim, KAIST, South Korea
Stephane Menoret, THALES, France
Andrea Parodi, M3S, Italy
Septimiu Nechifor, SIEMENS, Romania
Thomas Gilbert, Alexandra Instituttet, Danmark
Payam Barnaghi, Surrey University, UK
Markus Eisenhauer, FIT, Fraunhofer, Germany

Acknowledgements

The AIOTI would like to thank the European Commission services for their support in the planning and preparation of this document. The recommendations and opinions expressed in this document do not necessarily represent those of the European Commission. The views expressed herein do not commit the European Commission in any way.