River Publishers Series in Communication

Internet of Things – From Research and Innovation to Market Deployment

Editors

Ovidiu Vermesan

Peter Friess

River Publishers

Contents

3

Internet of Things Strategic Research and Innovation Agenda

Ovidiu Vermesan[1], Peter Friess[2], Patrick Guillemin[3], Harald Sundmaeker[4], Markus Eisenhauer[5], Klaus Moessner[6], Marilyn Arndt[7], Maurizio Spirito[8], Paolo Medagliani[9], Raffaele Giaffreda[10], Sergio Gusmeroli[11], Latif Ladid[12], Martin Serrano[13], Manfred Hauswirth[13], Gianmarco Baldini[14]

[1] *SINTEF, Norway*
[2] *European Commission, Belgium*
[3] *ETSI, France*
[4] *ATB GmbH, Germany*
[5] *Fraunofer FIT, Germany*
[6] *University of Surrey, UK*
[7] *Orange, France*
[8] *ISMB, Italy*
[9] *Thales Communications & Security, France*
[10] *CREATE-NET, Italy*
[11] *TXT e-solutions, Italy*
[12] *University of Luxembourg, Luxembourg*
[13] *Digital Enterprise Research Institute, Galway, Ireland*
[14] *Joint Research Centre, European Commission, Italy*

"Whatever you can do, or dream you can, begin it. Boldness has genius, power and magic in it."

Johann Wolfgang von Goethe

"If you want something new, you have to stop doing something old."

Peter F. Drucker

"Vision is the art of seeing things invisible."

Jonathan Swift

3.1 Internet of Things Vision

Internet of Things (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. In this context the research and development challenges to create a smart world are enormous. A world where the real, digital and the virtual are converging to create smart environments that make energy, transport, cities and many other areas more intelligent. The goal of the Internet of Things is to enable things to be connected anytime, anyplace, with anything and anyone ideally using any path/network and any service. Internet of Things is a new revolution of the Internet. Objects make themselves recognizable and they obtain intelligence by making or enabling context related decisions thanks to the fact that they can communicate information about themselves and they can access information that has been aggregated by other things, or they can be components of complex services [69].

The Internet of Things is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment and 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 Internet of Things mainstream. The number of Internet-connected devices surpassed the number of human beings on the planet in 2011, and by 2020, Internet-connected devices are expected to number between 26 billion and 50 billion. For every Internet-connected PC or handset there will be 5–10 other types of devices sold with native Internet connectivity [43].

According to industry analyst firm IDC, the installed base for the Internet of Things will grow to approximately 212 billion devices by 2020, a number that includes 30 billion connected devices. IDC sees this growth driven largely by intelligent systems that will be installed and collecting data - across both consumer and enterprise applications [44].

These types of applications can involve the electric vehicle and the smart house, in which appliances and services that provide notifications, security, energy-saving, automation, telecommunication, computers and entertainment will be integrated into a single ecosystem with a shared user interface. IoT is providing access to information, media and services, through wired and

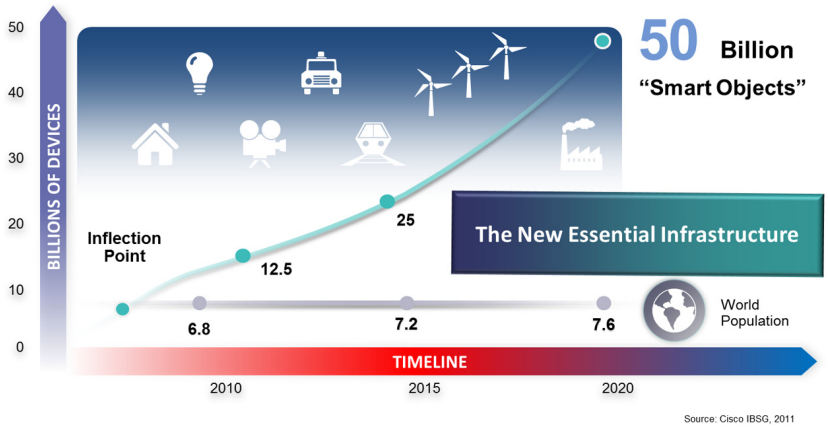

Figure 3.1 Internet-connected devices and the future evolution (Source: Cisco, 2011)

wireless broadband connections. The Internet of Things 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 Internet of Things and Services makes it possible to create networks incorporating the entire manufacturing process that convert factories into a smart environment. The cloud enables a global infrastructure to generate new services, allowing anyone to create content and applications for global users. Networks of things connect things globally and maintain their identity online. Mobile allows connection to this global infrastructure anytime, anywhere. The result is a globally accessible network of things, users, and consumers, who are available to create businesses, contribute content, generate and purchase new services.

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

The European Commission while recognizing the potential of Converging Sciences and Technologies Converging Sciences and Technologies to advance

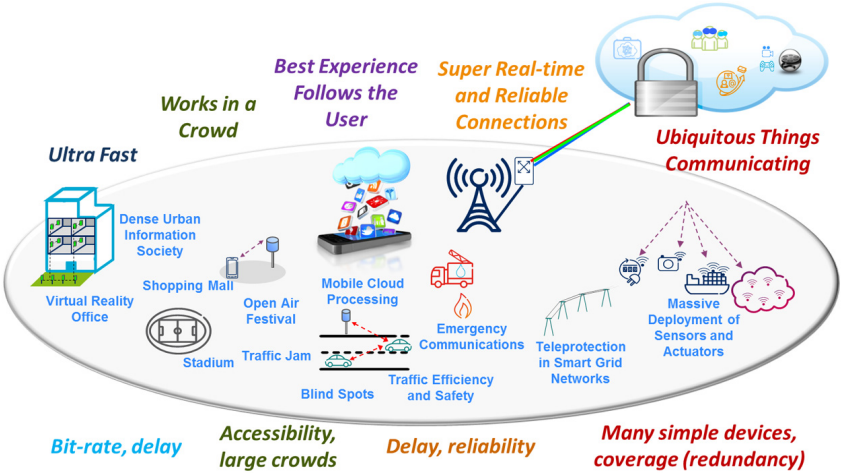

Figure 3.2 Future Communication Challenges – 5G scenarios [2]

the Lisbon Agenda, proposes a bottom-up approach to prioritize the setting of a particular goal for convergence of science and technology research; meet challenges and opportunities for research and governance and allow for integration of technological potential as well as recognition of limits, European needs, economic opportunities, and scientific interests.

Enabling technologies for the Internet of Things considered in [36] can be grouped into three categories: *i*) technologies that enable "things" to acquire contextual information, *ii*) technologies that enable "things" to process contextual information, and *iii*) technologies to improve security and privacy. The first two categories can be jointly understood as functional building blocks required building "intelligence" into "things", which are indeed the features that differentiate the IoT from the usual Internet. The third category is not a *functional* but rather a *de facto* requirement, without which the penetration of the IoT would be severely reduced. Internet of Things developments implies that the environments, cities, buildings, vehicles, clothing, portable devices and other objects have more and more information associated with them and/or the ability to sense, communicate, network and produce new information. In addition the network technologies have to cope with the new challenges such as very high data rates, dense crowds of users, low latency, low energy, low cost and a massive number of devices, The 5G scenarios that reflect the future challenges and will serve as guidance for further work are outlined by the EC funded METIS project [2].

As the Internet of Things becomes established in smart factories, both the volume and the level of detail of the corporate data generated will increase. Moreover, business models will no longer involve just one company, but will instead comprise highly dynamic networks of companies and completely new value chains. Data will be generated and transmitted autonomously by smart machines and these data will inevitably cross company boundaries. A number of specific dangers are associated with this new context – for example, data that were initially generated and exchanged in order to coordinate manufacturing and logistics activities between different companies could, if read in conjunction with other data, suddenly provide third parties with highly sensitive information about one of the partner companies that might, for example, give them an insight into its business strategies. New instruments will be required if companies wish to pursue the conventional strategy of keeping such knowledge secret in order to protect their competitive advantage. New, regulated business models will also be necessary – the raw data that are generated may contain information that is valuable to third parties and companies may therefore wish to make a charge for sharing them. Innovative business models like this will also require legal safeguards (predominantly in the shape of contracts) in order to ensure that the value added created is shared out fairly, e.g. through the use of dynamic pricing models [55].

3.1.1 Internet of Things Common Definition

Ten "critical" trends and technologies impacting IT for the next five years were laid out by Gartner and among them the Internet of Things. All of these things have an IP address and can be tracked. The Internet is expanding into enterprise assets and consumer items such as cars and televisions. The problem is that most enterprises and technology vendors have yet to explore the possibilities of an expanded Internet and are not operationally or organizationally ready. Gartner [54] identifies four basic usage models that are emerging:

- Manage
- Monetize
- Operate
- Extend.

These can be applied to people, things, information, and places, and therefore the so called "Internet of Things" will be succeeded by the "Internet of Everything."

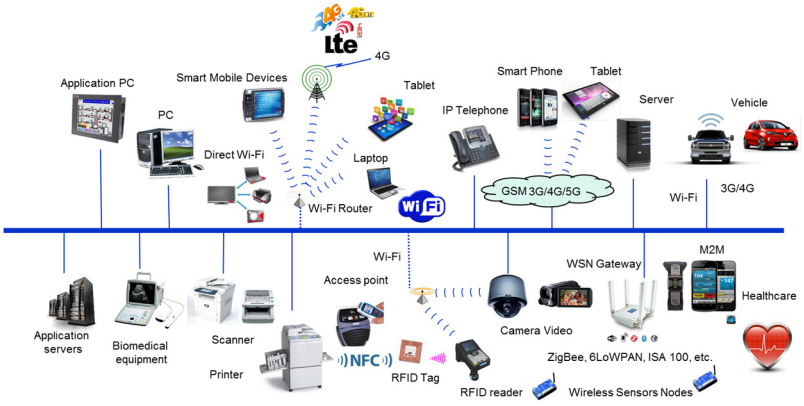

Figure 3.3 IP Convergence

In this context the notion of network convergence using IP is fundamental and relies on the use of a common multi-service IP network supporting a wide range of applications and services.

The use of IP to communicate with and control small devices and sensors opens the way for the convergence of large, IT-oriented networks with real time and specialized networked applications.

The fundamental characteristics of the IoT are as follows [65]:

- Interconnectivity: With regard to the IoT, anything can be interconnected with the global information and communication infrastructure.
- Things-related services: The IoT is capable of providing thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual things. In order to provide thing-related services within the constraints of things, both the technologies in physical world and information world will change.
- Heterogeneity: The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks.
- Dynamic changes: The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically.
- Enormous scale: The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude

larger than the devices connected to the current Internet. The ratio of communication triggered by devices as compared to communication triggered by humans will noticeably shift towards device-triggered communication. Even more critical will be the management of the data generated and their interpretation for application purposes. This relates to semantics of data, as well as efficient data handling.

The Internet of Things is not a single technology, it's a concept in which most new things are connected and enabled such as street lights being networked and things like embedded sensors, image recognition functionality, augmented reality, near field communication are integrated into situational decision support, asset management and new services. These bring many business opportunities and add to the complexity of IT [52].

To accommodate the diversity of the IoT, there is a heterogeneous mix of communication technologies, which need to be adapted in order to address the needs of IoT applications such as energy efficiency, security, and reliability. In this context, it is possible that the level of diversity will be scaled to a number a manageable connectivity technologies that address the needs of the IoT applications, are adopted by the market, they have already proved to be serviceable, supported by a strong technology alliance. Examples of standards in these categories include wired and wireless technologies like Ethernet, Wi-Fi, Bluetooth, ZigBee, and Z-Wave.

Distribution, transportation, logistics, reverse logistics, field service, etc. are areas where the coupling of information and "things" may create new business processes or may make the existing ones highly efficient and more profitable.

The Internet of Things provides solutions based on the integration of information technology, which refers to hardware and software used to store, retrieve, and process data and communications technology which includes electronic systems used for communication between individuals or groups. The rapid convergence of information and communications technology is taking place at three layers of technology innovation: the cloud, data and communication pipes/networks and device [46].

The synergy of the access and potential data exchange opens huge new possibilities for IoT applications. Already over 50% of Internet connections are between or with things. In 2011 there were over 15 billion things on the Web, with 50 billion+ intermittent connections.

By 2020, over 30 billion connected things, with over 200 billion with intermittent connections are forecast. Key technologies here include

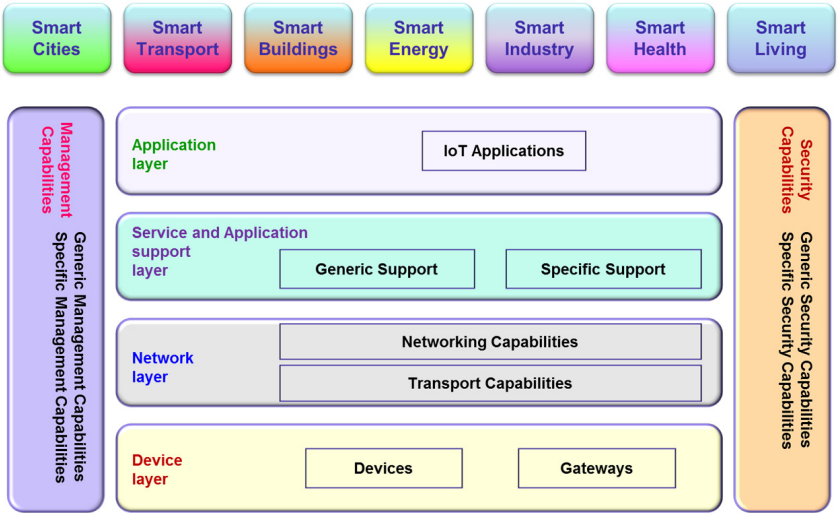

Figure 3.4 IoT Layered Architecture (Source: ITU-T)

embedded sensors, image recognition and NFC. By 2015, in more than 70% of enterprises, a single executable will oversee all Internet connected things. This becomes the Internet of Everything [53].

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

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

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

The Internet of Things had until recently different means at different levels of abstractions through the value chain, from lower level semiconductor through the service providers.

The Internet of Things is a “global concept” and requires a common definition. Considering the wide background and required technologies,

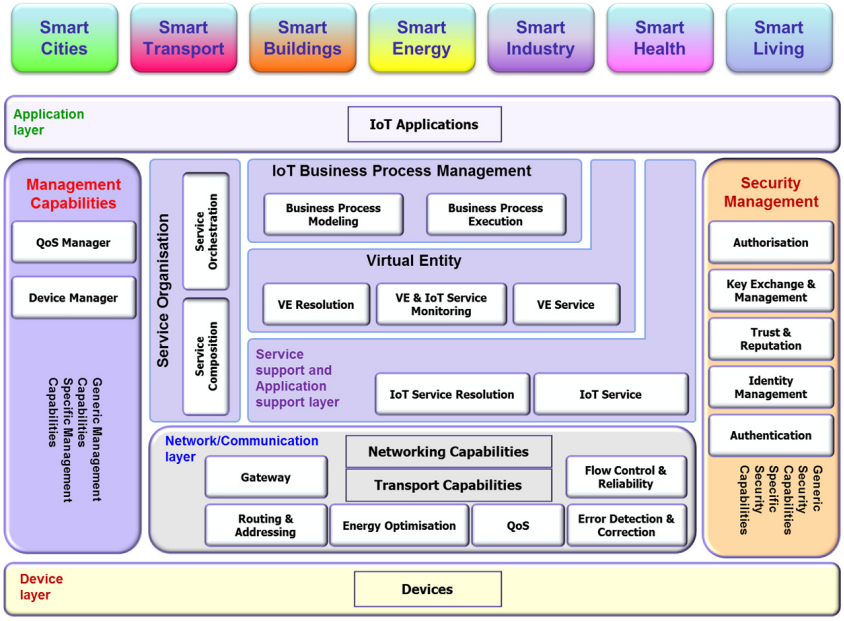

Figure 3.5 Detailed IoT Layered Architecture (Source: IERC)

from sensing device, communication subsystem, data aggregation and pre-processing to the object instantiation and finally service provision, generating an unambiguous definition of the "Internet of Things" is non-trivial.

The IERC is actively involved in ITU-T Study Group 13, which leads the work of the International Telecommunications Union (ITU) on standards for next generation networks (NGN) and future networks and has been part of the team which has formulated the following definition [65]: *"**Internet of things (IoT)**: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled. NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications."*

The IERC definition [67] states that IoT is "*A dynamic global network infrastructure with self-configuring capabilities based on standard and inter-operable communication protocols where physical and virtual "things" have*

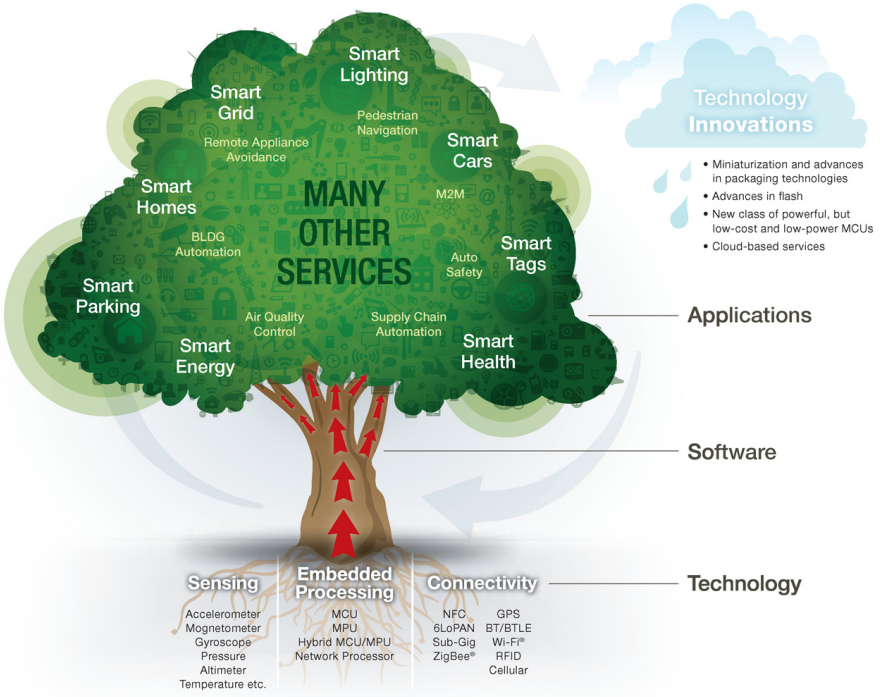

Figure 3.6 The IoT: Different Services, Technologies, Meanings for Everyone [77]

identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.".

3.2 IoT Strategic Research and Innovation Directions

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".

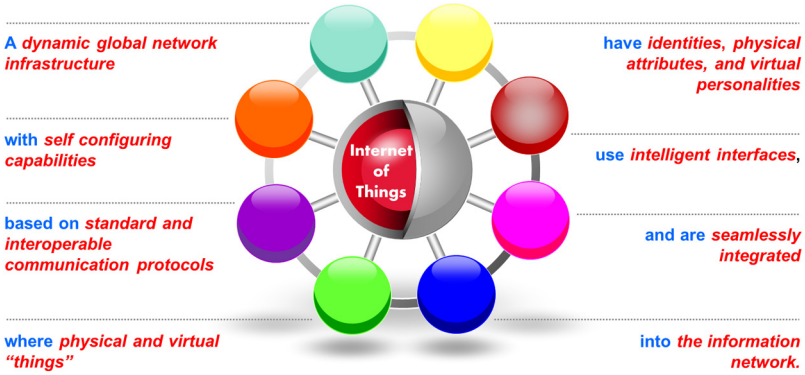

Figure 3.7 IoT Definition [68]

The final report of the Key Enabling Technologies (KET), of the High-Level Expert Group [47] identified the enabling technologies, crucial to many of the existing and future value chains of the European economy:

- Nanotechnologies.
- Micro and Nano electronics
- Photonics
- Biotechnology
- Advanced Materials
- Advanced Manufacturing Systems.

As such, IoT creates intelligent applications that are based on the supporting KETs identified, as IoT applications address smart environments either physical or at cyber-space level, and in real time.

To this list of key enablers, we can add the global deployment of IPv6 across the World enabling a global and ubiquitous addressing of any communicating smart thing.

From a technology perspective, the continuous increase in the integration density proposed by Moore's Law was made possible by a dimensional scaling: in reducing the critical dimensions while keeping the electrical field constant, one obtained at the same time a higher speed and a reduced power consumption of a digital MOS circuit: these two parameters became driving forces of the microelectronics industry along with the integration density.

The International Technology Roadmap for Semiconductors has emphasized in its early editions the "miniaturization" and its associated benefits in terms of performances, the traditional parameters in Moore's Law. This trend for increased performances will continue, while performance can always

be traded against power depending on the individual application, sustained by the incorporation into devices of new materials, and the application of new transistor concepts. This direction for further progress is labelled "More Moore".

The second trend is characterized by functional diversification of semiconductor-based devices. These non-digital functionalities do contribute to the miniaturization of electronic systems, although they do not necessarily scale at the same rate as the one that describes the development of digital functionality. Consequently, in view of added functionality, this trend may be designated "More-than-Moore" [50].

Mobile data traffic is projected to double each year between now and 2015 and mobile operators will find it increasingly difficult to provide the bandwidth requested by customers. In many countries there is no additional spectrum that can be assigned and the spectral efficiency of mobile networks is reaching its physical limits. Proposed solutions are the seamless integration of existing Wi-Fi networks into the mobile ecosystem. This will have a direct impact on Internet of Things ecosystems.

The chips designed to accomplish this integration are known as "multi-com" chips. Wi-Fi and baseband communications are expected to converge and the architecture of mobile devices is likely to change and the baseband chip is expected to take control of the routing so the connectivity components are connected to the baseband or integrated in a single silicon package. As a result of this architecture change, an increasing share of the integration work is likely done by baseband manufacturers (ultra -low power solutions) rather than by handset producers.

The market for wireless communications is one of the fastest-growing segments in the integrated circuit industry. Breath takingly fast innovation, rapid changes in communications standards, the entry of new players, and the evolution of new market sub segments will lead to disruptions across the industry. LTE and multicom solutions increase the pressure for industry consolidation, while the choice between the ARM and x86 architectures forces players to make big bets that may or may not pay off [63].

Integrated networking, information processing, sensing and actuation capabilities allow physical devices to operate in changing environments. Tightly coupled cyber and physical systems that exhibit high level of integrated intelligence are referred to as cyber-physical systems. These systems are part of the enabling technologies for Internet of Things applications where computational and physical processes of such systems are tightly interconnected and coordinated to work together effectively, with or without the humans in the

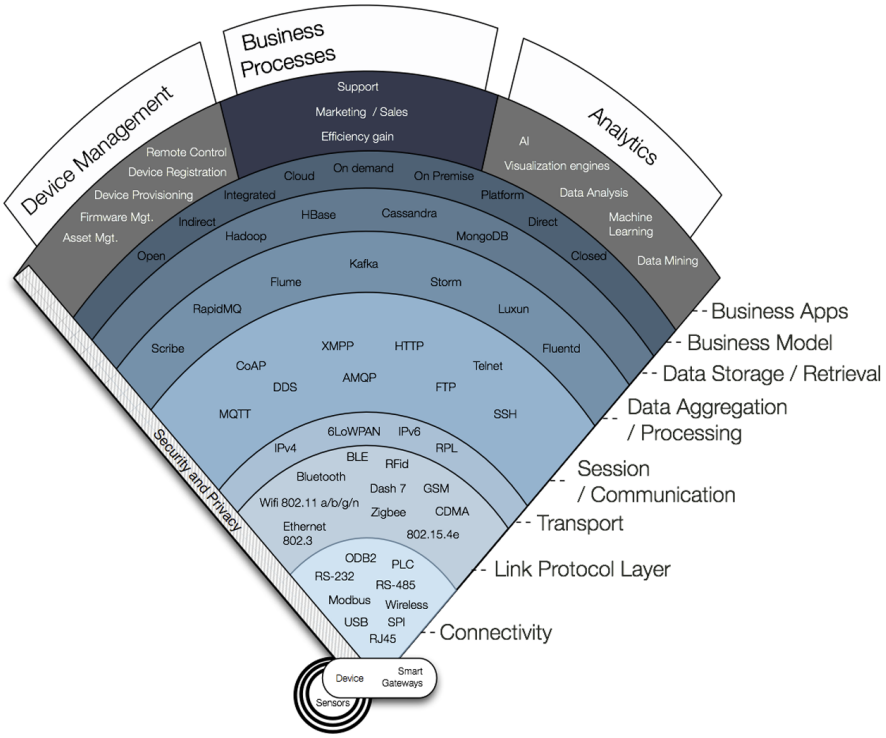

Figure 3.8 IoT landscape [21]

loop. Robots, intelligent buildings, implantable medical devices, vehicles that drive themselves or planes that automatically fly in a controlled airspace, are examples of cyber-physical systems that could be part of Internet of Things ecosystems.

Today many European projects and initiatives address Internet of Things technologies and knowledge. Given the fact that these topics can be highly diverse and specialized, there is a strong need for integration of the individual results. Knowledge integration, in this context is conceptualized as the process through which disparate, specialized knowledge located in multiple projects across Europe is combined, applied and assimilated.

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

Figure 3.9 Internet of Things — Enabling Technologies

IERC Strategic Research and Innovation Agenda covers the important issues and challenges for the Internet of Things technology. It provides the vision and the roadmap for coordinating and rationalizing current and future research and development efforts in this field, by addressing the different enabling technologies covered by the Internet of Things concept and paradigm.

Many other technologies are converging to support and enable IoT applications. These technologies are summarised as:

- IoT architecture
- Identification
- Communication
- Networks technology
- Network discovery
- Software and algorithms
- Hardware technology
- Data and signal processing
- Discovery and search engine
- Network management
- Power and energy storage
- Security, trust, dependability and privacy

- Interoperability
- Standardization

The Strategic Research and Innovation Agenda is developed with the support of a European-led community of interrelated projects and their stakeholders, dedicated to the innovation, creation, development and use of the Internet of Things technology.

Since the release of the first version of the Strategic Research and Innovation Agenda, we have witnessed active research on several IoT topics. On the one hand this research filled several of the gaps originally identified in the Strategic Research and Innovation Agenda, whilst on the other it created new challenges and research questions. Recent advances in areas such as cloud computing, cyber-physical systems, autonomic computing, and social networks have changed the scope of the Internet of Thing's convergence even more so. The Cluster has a goal to provide an updated document each year that records the relevant changes and illustrates emerging challenges. The updated release of this Strategic Research and Innovation Agenda builds incrementally on previous versions [68], [69], [84], [85], [85] and highlights the main research topics that are associated with the development of IoT enabling technologies, infrastructures and applications with an outlook towards 2020 [73].

The research items introduced will pave the way for innovative applications and services that address the major economic and societal challenges underlined in the EU 2020 Digital Agenda [74].

Figure 3.10 Internet of Things - Smart Environments and Smart Spaces Creation

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

The timeline of the Internet of Things Strategic Research and Innovation Agenda covers the current decade with respect to research and the following years with respect to implementation of the research results. Of course, as the Internet and its current key applications show, we anticipate unexpected trends will emerge leading to unforeseen and unexpected development paths.

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

The IoT Strategic Research and Innovation Agenda covers in a logical manner the vision, the technological trends, the applications, the technology enablers, the research agenda, timelines, priorities, and finally summarises in two tables the future technological developments and research needs.

Advances in embedded sensors, processing and wireless connectivity are bringing the power of the digital world to objects and places in the physical world. IoT Strategic Research and Innovation Agenda is aligned with the findings of the 2011 Hype Cycle developed by Gartner [76], which includes the broad trend of the Internet of Things, called the "real-world Web" in earlier Gartner research.

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

3.2.1 IoT Applications and Use Case Scenarios

The IERC vision is that "the major objectives for IoT are the creation of smart environments/spaces and self-aware things (for example: smart transport, products, cities, buildings, rural areas, energy, health, living, etc.) for climate, food, energy, mobility, digital society and health applications"[68].

The outlook for the future is the emerging of a network of interconnected uniquely identifiable objects and their virtual representations in an Internet alike structure that is positioned over a network of interconnected computers allowing for the creation of a new platform for economic growth.

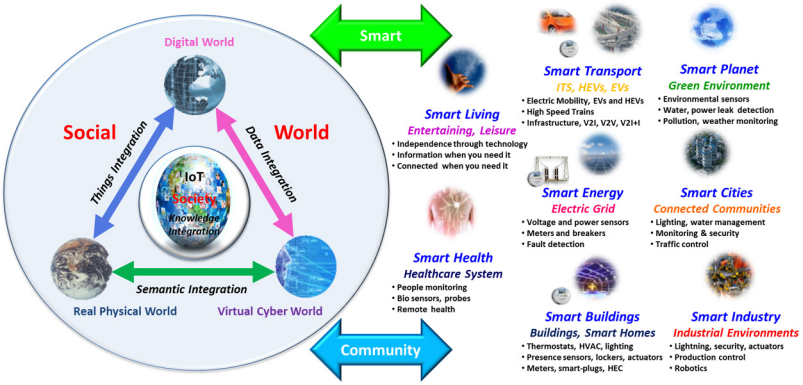

Figure 3.11 Internet of Things in the context of Smart Environments and Applications [84]

Smart is the new green as defined by Frost & Sullivan [51] and the green products and services will be replaced by smart products and services. Smart products have a real business case, can typically provide energy and efficiency savings of up to 30 per cent, and generally deliver a two- to three-year return on investment. This trend will help the deployment of Internet of Things applications and the creation of smart environments and spaces.

At the city level, the integration of technology and quicker data analysis will lead to a more coordinated and effective civil response to security and safety (law enforcement and blue light services); higher demand for outsourcing security capabilities.

At the building level, security technology will be integrated into systems and deliver a return on investment to the end-user through leveraging the technology in multiple applications (HR and time and attendance, customer behaviour in retail applications etc.).

There will be an increase in the development of "Smart" vehicles which have low (and possibly zero) emissions. They will also be connected to infrastructure. Additionally, auto manufacturers will adopt more use of "Smart" materials.

The key focus will be to make the city smarter by optimizing resources, feeding its inhabitants by urban farming, reducing traffic congestion, providing more services to allow for faster travel between home and various destinations, and increasing accessibility for essential services. It will become essential to have intelligent security systems to be implemented at key junctions in the city. Various types of sensors will have to be used to make this a reality. Sensors are moving from "smart" to "intelligent". Biometrics is already integrated in

the smart mobile phones and is expected to be used together with CCTV at highly sensitive locations around the city. National identification cards will also become an essential tool for the identification of an individual. In addition, smart cities in 2020 will require real time auto identification security systems.

The IoT brings about a paradigm were everything is connected and will redefine the way humans and machines interface and the way they interact with the world around them.

Fleet Management is used to track vehicle location, hard stops, rapid acceleration, and sudden turns using sophisticated analysis of the data in order to implement new policies (e.g., no right/left turns) that result in cost savings for the business.

Today there are billions of connected sensors already deployed with smart phones and many other sensors are connected to these smart mobile network using different communication protocols.

The challenges is in getting the data from them 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.

Wastewater treatment plants will evolve into bio-refineries. New, innovative wastewater treatment processes will enable water recovery to help close the growing gap between water supply and demand.

Self-sensing controls and devices will mark new innovations in the Building Technologies space. Customers will demand more automated, self-controlled solutions with built in fault detection and diagnostic capabilities.

Development of smart implantable chips that can monitor and report individual health status periodically will see rapid growth.

Smart pumps and smart appliances/devices are expected to be significant contributors towards efficiency improvement. Process equipment with in built "smartness" to self-assess and generate reports on their performance, enabling efficient asset management, will be adopted.

Test and measurement equipment is expected to become smarter in the future in response to the demand for modular instruments having lower power consumption. Furthermore, electronics manufacturing factories will become more sustainable with renewable energy and sell unused energy back to the grid, improved water conservation with rain harvesting and implement other smart building technologies, thus making their sites "Intelligent Manufacturing Facilities".

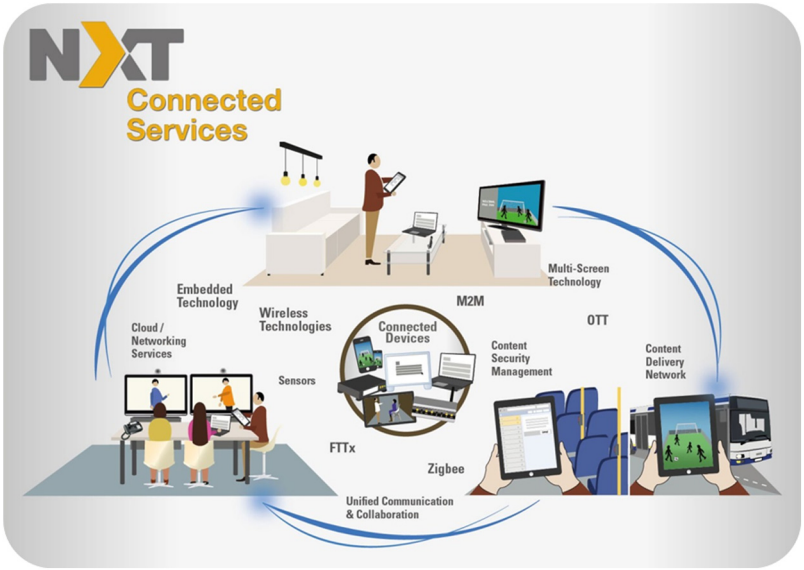

Figure 3.12 Connected Devices Illustration [62]

General Electric Co. considers that this is taking place through the convergence of the global industrial system with the power of advanced computing, analytics, low-cost sensing and new levels of connectivity permitted by the Internet. The deeper meshing of the digital world with the world of machines holds the potential to bring about profound transformation to global industry, and in turn to many aspects of daily life [58].

The Industrial Internet starts with embedding sensors and other advanced instrumentation in an array of machines from the simple to the highly complex. This allows the collection and analysis of an enormous amount of data, which can be used to improve machine performance, and inevitably the efficiency of the systems and networks that link them. Even the data itself can become "intelligent," instantly knowing which users it needs to reach.

Consumer IoT is essentially wireless, while the industrial IoT has to deal with an installed base of millions of devices that could potentially become part of this network (many legacy systems installed before IP deployment). These industrial objects are linked by wires that provides the reliable communications needed. The industrial IoT has to consider the legacy using specialised protocols, including Lonworks, DeviceNet, Profibus and CAN and they will be connected into this new netwoek of networks through gateways.

The automation and management of asset-intensive enterprises will be transformed by the rise of the IoT, Industry 4.0, or simply Industrial Internet. Compared with the Internet revolution, many product and asset management solutions have labored under high costs and poor connectivity and performance. This is now changing. New high-performance systems that can support both Internet and Cloud connectivity as well as predictive asset management are reaching the market. New cloud computing models, analytics, and aggregation technologies enable broader and low cost application of analytics across these much more transparent assets. These developments have the potential to radically transform products, channels, and company business models. This will create disruptions in the business and opportunities for all types of organizations - OEMs, technology suppliers, system integrators, and global consultancies. There may be the opportunity to overturn established business models, with a view toward answering customer pain points and also growing the market in segments that cannot be served economically with today's offerings. Mobility, local diagnostics, and remote asset monitoring are important components of these new solutions, as all market participants need ubiquitous access to their assets, applications, and customers. Real-time mobile applications support EAM, MRO, inventory management, inspections, workforce management, shop floor interactions, facilities management, field service automation, fleet management, sales and marketing, machine-to-machine (M2M), and many others [56]

In this context the new concept of Internet of Energy 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.

This concept would enable 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 as presented in Figure 3.14 [35] will leverage 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

Figure 3.13 Industrial Internet of Things [56]

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 Internet of Energy applications are connected through the Future Internet and "Internet of Things" enabling seamless and secure interactions and cooperation of intelligent embedded systems over heterogeneous communication infrastructures.

It is expected that this "development of smart entities will encourage development of the novel technologies needed to address the emerging challenges of public health, aging population, environmental protection and climate change, conservation of energy and scarce materials, enhancements to safety and security and the continuation and growth of economic prosperity." The IoT applications are further linked with Green ICT, as the IoT will drive energy-efficient applications such as smart grid, connected electric cars, energy-efficient buildings, thus eventually helping in building green intelligent cities.

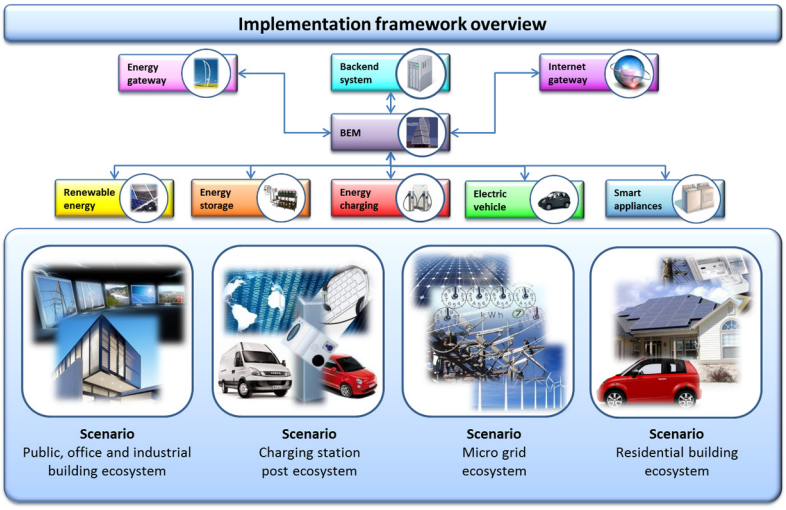

Figure 3.14 Internet of Energy Implementation Framework (Source:[35])

3.2.2 IoT Functional View

The Internet of Things concept refers to uniquely identifiable things with their virtual representations in an Internet-like structure and IoT solutions comprising a number of components such as:

- Module for interaction with local IoT devices (for example embedded in a mobile phone or located in the immediate vicinity of the user and thus contactable via a short range wireless interface). This module is responsible for acquisition of observations and their forwarding to remote servers for analysis and permanent storage.
- Module for local analysis and processing of observations acquired by IoT devices.
- Module for interaction with remote IoT devices, directly over the Internet or more likely via a proxy. This module is responsible for acquisition of observations and their forwarding to remote servers for analysis and permanent storage.
- Module for application specific data analysis and processing. This module is running on an application server serving all clients. It is taking requests from mobile and web clients and relevant IoT observations as input, executes appropriate data processing algorithms and generates output in terms of knowledge that is later presented to users.

- Module for integration of IoT-generated information into the business processes of an enterprise. This module will be gaining importance with the increased use of IoT data by enterprises as one of the important factors in day-to-day business or business strategy definition.
- User interface (web or mobile): visual representation of measurements in a given context (for example on a map) and interaction with the user, i.e. definition of user queries.

It is important to highlight that one of the crucial factors for the success of IoT is stepping away from vertically-oriented, closed systems towards open systems, based on open APIs and standardized protocols at various system levels.

In this context innovative architecture and platforms are needed to support highly complex and inter-connected IoT applications. A key consideration is how to enable development and application of comprehensive architectural frameworks that include both the physical and cyber elements based on enabling technologies. In addition considering the technology convergence trend new platforms will be needed for communication and to effectively extract actionable information from vast amounts of raw data, while providing a robust timing and systems framework to support the real-time control and synchronization requirements of complex, networked, engineered physical/cyber/virtual systems.

A large number of applications made available through application markets have significantly helped the success of the smart phone industry. The development of such a huge number of smart phone applications is primarily due to involvement of the developers' community at large. Developers leveraged smart phone open platforms and the corresponding development tools, to create a variety of applications and to easily offer them to a growing number of users through the application markets.

Similarly, an IoT ecosystem has to be established, defining open APIs for developers and offering appropriate channels for delivery of new applications. Such open APIs are of particular importance on the level of the module for application specific data analysis and processing, thus allowing application developers to leverage the underlying communication infrastructure and use and combine information generated by various IoT devices to produce new, added value.

Although this might be the most obvious level at which it is important to have open APIs, it is equally important to aim towards having such APIs defined on all levels in the system. At the same time one should have in mind the heterogeneity and diversity of the IoT application space. This will truly

support the development of an IoT ecosystem that encourages development of new applications and new business models.

The complete system will have to include supporting tools providing security and business mechanisms to enable interaction between a numbers of different business entities that might exist [86].

Research challenges:

- Design of open APIs on all levels of the IoT ecosystem
- Design of standardized formats for description of data generated by IoT devices to allow mashups of data coming from different domains and/or providers.

3.2.3 Application Areas

In the last few years the evolution of markets and applications, and therefore their economic potential and their impact in addressing societal trends and challenges for the next decades has changed dramatically. Societal trends are grouped as: health and wellness, transport and mobility, security and safety, energy and environment, communication and e-society. These trends create significant opportunities in the markets of consumer electronics, automotive electronics, medical applications, communication, etc. The applications in in these areas benefit directly by the More-Moore and More-than-Moore semiconductor technologies, communications, networks and software developments.

Potential applications of the IoT are numerous and diverse, permeating into practically all areas of every-day life of individuals, enterprises, and society as a whole. The IERC [68–69], [84–85] has identified and described the main Internet of Things applications, which span numerous applications domains: smart energy, smart health, smart buildings, smart transport, smart industry and smart city. The vision of a pervasive IoT requires the integration of the various domains into a single, unified, domain and addresses the enabling technologies needed for these domains while taking into account the elements that form the third dimension like security, privacy, trust, safety.

The IoT application domains identified by IERC [68], [85] are based on inputs from experts, surveys [86] and reports [87]. The IoT application covers "smart" environments/spaces in domains such as: Transportation, Building, City, Lifestyle, Retail, Agriculture, Factory, Supply chain, Emergency, Health care, User interaction, Culture and tourism, Environment and Energy.

The applications areas include as well the domain of Industrial Internet [58] where intelligent devices, intelligent systems, and intelligent decision-making

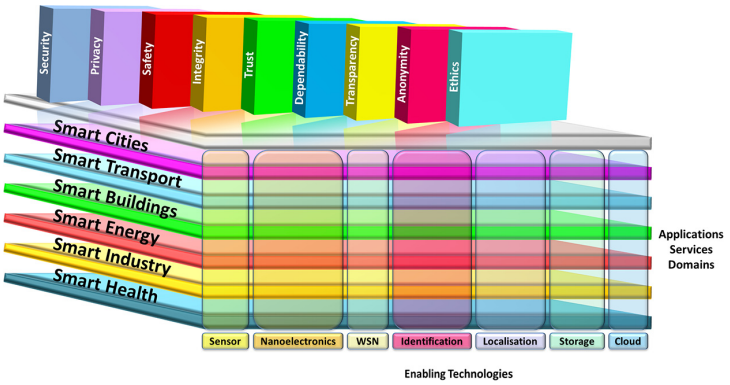

Figure 3.15 IoT 3D Matrix

represent the primary ways in which the physical world of machines, facilities, fleets and networks can more deeply merge with the connectivity, big data and analytics of the digital world. Manufacturing and industrial automation are under pressure from shortened product life-cycles and the demand for a shorter time to market in many areas. The next generation of manufacturing systems will therefore be built with flexibility and reconfiguration as a fundamental objective.

This change is eminent in the transition from traditional, centralized control applications to an interconnected, cooperative "Internet of Things" model. Strong hierarchies are broken in favour of meshed, networks and formerly passive devices are replaced with "smart objects" that are network enabled and can perform compute operations. The software side has to match and leverage the changes in the hardware. Service Oriented Architectures (SOAs) are a well-known concept from business computing to deal with flexibility and reconfiguration requirements in a loosely coupled manner. However, the common concepts of SOAs cannot be directly mapped to embedded networks and industrial control applications, because of the hard boundary conditions, such as limited resources and real-time requirements [57].

The updated list of IoT applications presented below, includes examples of IoT applications in different domains, which is showing why the Internet of Things is one of the strategic technology trends for the next 5 years.

Smart Food/Water Monitoring

Water Quality: Study of water suitability in rivers and the sea for fauna and eligibility for drinkable use.

Water Leakages: Detection of liquid presence outside tanks and pressure variations along pipes.

River Floods: Monitoring of water level variations in rivers, dams and reservoirs.

Water Management: Real-time information about water usage and the status of waterlines could be collected by connecting residential water meters to an Internet protocol (IP) network. As a consequence could be reductions in labour and maintenance costs, improved accuracy and lower costs in meter readings, and possibly water consumption reductions.

Supply Chain Control: Monitoring of storage conditions along the supply chain and product tracking for traceability purposes.

Wine Quality Enhancing: Monitoring soil moisture and trunk diameter in vineyards to control the amount of sugar in grapes and grapevine health.

Green Houses: Control micro-climate conditions to maximize the production of fruits and vegetables and its quality.

Golf Courses: Selective irrigation in dry zones to reduce the water resources required in the green.

In-field Monitoring: Reducing spoilage and food waste with better monitoring, statistic handling, accurate ongoing data obtaining, and management of the agriculture fields, including better control of fertilizing, electricity and watering.

Smart Health

Fall Detection: Assistance for elderly or disabled people living independent.

Physical Activity Monitoring for Aging People: Body sensors network measures motion, vital signs, unobtrusiveness and a mobile unit collects, visualizes and records activity data.

Medical Fridges: Control of conditions inside freezers storing vaccines, medicines and organic elements.

Sportsmen Care: Vital signs monitoring in high performance centres and fields. Health and fitness products for these purposes exist, that measure exercise, steps, sleep, weight, blood pressure, and other statistics.

Patients Surveillance: Monitoring of conditions of patients inside hospitals and in old people's home.

Chronic Disease Management: Patient-monitoring systems with comprehensive patient statistics could be available for remote residential monitoring of patients with chronic diseases such as pulmonary and heart diseases

and diabetes. The reduced medical center admissions, lower costs, and shorter hospital stays would be some of the benefits.

Ultraviolet Radiation: Measurement of UV sun rays to warn people not to be exposed in certain hours.

Hygienic hand control: RFID-based monitoring system of wrist bands in combination of Bluetooth LE tags on a patient's doorway controlling hand hygiene in hospitals, where vibration notifications is sent out to inform about time for hand wash; and all the data collected produce analytics which can be used to potentially trace patient infections to particular healthcare workers.

Sleep control: Wireless sensors placed across the mattress sensing small motions, like breathing and heart rate and large motions caused by tossing and turning during sleep, providing data available through an app on the smartphone.

Dental Health: Bluetooth connected toothbrush with smartphone app analyzes the brushing uses and gives information on the brushing habits on the smartphone for private information or for showing statistics to the dentist.

Smart Living

Intelligent Shopping Applications: Getting advice at the point of sale according to customer habits, preferences, presence of allergic components for them, or expiring dates.

Energy and Water Use: Energy and water supply consumption monitoring to obtain advice on how to save cost and resources. Maximizing energy efficiency by introducing lighting and heating products, such as bulbs, thermostats and air conditioners.

Remote Control Appliances: Switching on and off remotely appliances to avoid accidents and save energy.

Weather Station: Displays outdoor weather conditions such as humidity, temperature, barometric pressure, wind speed and rain levels using meters with ability to transmit data over long distances.

Smart Home Appliances: Refrigerators with LCD screen telling what's inside, food that's about to expire, ingredients you need to buy and with all the information available on a smartphone app. Washing machines allowing you to monitor the laundry remotely, and run automatically when electricity rates are lowest. Kitchen ranges with interface to a smartphone app allowing remotely adjustable temperature control and monitoring the oven's self-cleaning feature.

Gas Monitoring: Real-information about gas usage and the status of gas lines could be provided by connecting residential gas meters to an Internet protocol (IP) network. As for the water monitoring, the possible outcome could be reductions in labor and maintenance costs, improved accuracy and lower costs in meter readings, and possibly gas consumption reductions.

Safety Monitoring: Baby monitoring, cameras, and home alarm systems making people feel safe in their daily life at home.

Smart Jewelry: Increased personal safety by wearing a piece of jewelry inserted with Bluetooth enabled technology used in a way that a simple push establishes contact with your smartphone, which through an app will send alarms to selected people in your social circle with information that you need help and your location.

Smart Environment Monitoring

Forest Fire Detection: Monitoring of combustion gases and preemptive fire conditions to define alert zones.

Air Pollution: Control of CO_2 emissions of factories, pollution emitted by cars and toxic gases generated in farms.

Landslide and Avalanche Prevention: Monitoring of soil moisture, vibrations and earth density to detect dangerous patterns in land conditions.

Earthquake Early Detection: Distributed control in specific places of tremors.

Protecting wildlife: Tracking collars utilizing GPS/GSM modules to locate and track wild animals and communicate their coordinates via SMS.

Meteorological Station Network: Study of weather conditions in fields to forecast ice formation, rain, drought, snow or wind changes.

Marine and Coastal Surveillance: Using different kinds of sensors integrated in planes, unmanned aerial vehicles, satellites, ship etc. to control the maritime activities and traffic in important areas, keep track of fishing boats, supervise environmental conditions and dangerous oil cargo etc.

Smart Manufacturing

Smart Product Management: Control of rotation of products in shelves and warehouses to automate restocking processes.

Compost: Control of humidity and temperature levels in alfalfa, hay, straw, etc. to prevent fungus and other microbial contaminants.

Offspring Care: Control of growing conditions of the offspring in animal farms to ensure its survival and health.

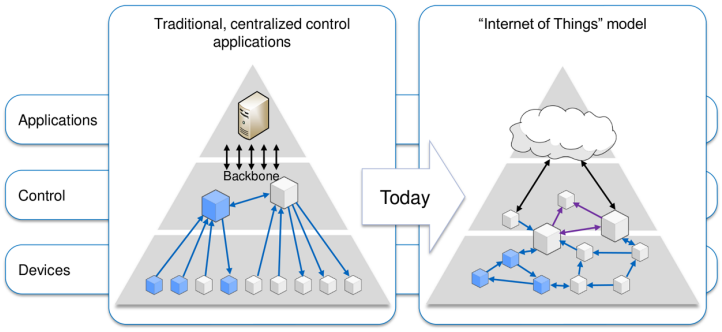

Figure 3.16 Interconnected, Cooperative "Internet of Things" Model for Manufacturing and Industrial Automation [57]

Animal Tracking: Location and identification of animals grazing in open pastures or location in big stables.

Toxic Gas Levels: Study of ventilation and air quality in farms and detection of harmful gases from excrements.

Production Line: Monitoring and management of the production line using RFID, sensors, video monitoring, remote information distribution and cloud solutions enabling the production line data to be transferred to the enterprise-based systems. This may result in more quickly improvement of the entire product quality assurance process by decision makers, updated workflow charts, and inspection procedures delivered to the proper worker groups via digital displays in real time.

Telework: Offering the employees technologies that enable home offices would reduce costs, improve productivity, and add employment opportunities at the same time as reducing real estate for employees, lower office maintenance and cleanings, and eliminating daily office commute.

Smart Energy

Smart Grid: Energy consumption monitoring and management.

Photovoltaic Installations: Monitoring and optimization of performance in solar energy plants.

Wind Turbines: Monitoring and analyzing the flow of energy from wind turbines, and two-way communication with consumers' smart meters to analyze consumption patterns.

Water Flow: Measurement of water pressure in water transportation systems.

Radiation Levels: Distributed measurement of radiation levels in nuclear power stations surroundings to generate leakage alerts.

Power Supply Controllers: Controller for AC-DC power supplies that determines required energy, and improve energy efficiency with less energy waste for power supplies related to computers, telecommunications, and consumer electronics applications.

Smart Buildings

Perimeter Access Control: Access control to restricted areas and detection of people in non-authorized areas.

Liquid Presence: Liquid detection in data centres, warehouses and sensitive building grounds to prevent break downs and corrosion.

Indoor Climate Control: Measurement and control of temperature, lighting, CO_2 fresh air in ppm etc.

Intelligent Thermostat: Thermostat that learns the users programming schedule after a few days, and from that programs itself. Can be used with an app to connect to the thermostat from a smart telephone, where control, watching the energy history, how much energy is saved and why can be displayed.

Intelligent Fire Alarm: System with sensors measuring smoke and carbon monoxide, giving both early warnings, howling alarms and speaks with a human voice telling where the smoke is or when carbon monoxide levels are rising, in addition to giving a message on the smartphone or tablet if the smoke or CO alarm goes off.

Intrusion Detection Systems: Detection of window and door openings and violations to prevent intruders.

Motion Detection: Infrared motion sensors which reliably sends alerts to alarm panel (or dialer) and with a system implementing reduced false alarms algorithms and adaption to environmental disturbances.

Art and Goods Preservation: Monitoring of conditions inside museums and art warehouses.

Residential Irrigation: Monitoring and smart watering system.

Smart Transport and Mobility

NFC Payment: Payment processing based in location or activity duration for public transport, gyms, theme parks, etc.

Quality of Shipment Conditions: Monitoring of vibrations, strokes, container openings or cold chain maintenance for insurance purposes.

Item Location: Searching of individual items in big surfaces like warehouses or harbours.

Storage Incompatibility Detection: Warning emission on containers storing inflammable goods closed to others containing explosive material.

Fleet Tracking: Control of routes followed for delicate goods like medical drugs, jewels or dangerous merchandises.

Electric Vehicle Charging Stations Reservation: Locates the nearest charging station and tell the user whether its in use. Drivers can ease their range anxiety by reserving charging stations ahead of time. Help the planning of extended EV road trips, so the EV drivers make the most of potential charging windows

Vehicle Auto-diagnosis: Information collection from CAN Bus to send real time alarms to emergencies or provide advice to drivers.

Management of cars: Car sharing companies manages the use of vehicles using the Internet and mobile phones through connections installed in each car.

Road Pricing: Automatic vehicle payment systems would improve traffic conditions and generate steady revenues if such payments are introduced in busy traffic zones. Reductions in traffic congestions and reduced CO2 emissions would be some of the benefits.

Connected Militarized Defence: By connecting command-centre facilities, vehicles, tents, and Special Forces real-time situational awareness for combat personnel in war areas and visualization of the location of allied/enemy personnel and material would be provided.

Smart Industry

Tank level: Monitoring of water, oil and gas levels in storage tanks and cisterns.

Silos Stock Calculation: Measurement of emptiness level and weight of the goods.

Explosive and Hazardous Gases: Detection of gas levels and leakages in industrial environments, surroundings of chemical factories and inside mines. Meters can transmit data that will be reliably read over long distances.

M2M Applications: Machine auto-diagnosis and assets control.

Maintenance and repair: Early predictions on equipment malfunctions and service maintenance can be automatically scheduled ahead of an actual part failure by installing sensors inside equipment to monitor and send reports.

Indoor Air Quality: Monitoring of toxic gas and oxygen levels inside chemical plants to ensure workers and goods safety.

Temperature Monitoring: Control of temperature inside industrial and medical fridges with sensitive merchandise.

Ozone Presence: Monitoring of ozone levels during the drying meat process in food factories.

Indoor Location: Asset indoor location by using active (ZigBee, UWB) and passive tags (RFID/NFC).

Aquaculture industry monitoring: Remotely operating and monitoring operational routines on the aquaculture site, using sensors, cameras, wireless communication infrastructure between sites and land base, winch systems etc. to perform site and environment surveillance, feeding and system operations.

Smart City

Smart Parking: Real-time monitoring of parking spaces availability in the city making residents able to identify and reserve the closest available spaces. Reduction in traffic congestions and increased revenue from dynamic pricing could be some of the benefits as well as simpler responsibility for traffic wardens recognizing non-compliant usage.

Structural Health: Monitoring of vibrations and material conditions in buildings, bridges and historical monuments.

Noise Urban Maps: Sound monitoring in bar areas and centric zones in real time.

Traffic Congestion: Monitoring of vehicles and pedestrian levels to optimize driving and walking routes.

Smart Lightning: Intelligent and weather adaptive lighting in street lights.

Waste Management: Detection of rubbish levels in containers to optimize the trash collection routes. Garbage cans and recycle bins with RFID tags allow the sanitation staff to see when garbage has been put out. Maybe "Pay as you throw"-programs would help to decrease garbage waste and increase recycling efforts.

Intelligent Transportation Systems: Smart Roads and Intelligent Highways with warning messages and diversions according to climate conditions and unexpected events like accidents or traffic jams.

Safe City: Digital video monitoring, fire control management, public announcement systems

Connected Learning: Improvements in teacher utilization, reduction in instructional supplies, productivity improvement, and lower costs are examples of benefits that may be gained from letting electronic resources deliver data-driven, authentic and collaborative learning experience to larger groups.

Smart irrigation of public spaces: Maintenance of parks and lawns by burying park irrigation monitoring sensors in the ground wirelessly connected to repeaters and with a wireless gateway connection to Internet.

Smart Tourism: Smartphone Apps supported by QR codes and NFC tags providing interesting and useful tourist information throughout the city. The information could include museums, art galleries, libraries, touristic attractions, tourism offices, monuments, shops, buses, taxis, gardens, etc.

The IoT application space is very diverse and IoT applications serve different users. Different user categories have different driving needs. From the IoT perspective there are three important user categories:

- The individual citizens
- Community of citizens (citizens of a city, a region, country or society as a whole)
- The enterprises.

Examples of the individual citizens/human users' needs for the IoT applications are as follows:

- To increase their safety or the safety of their family members - for example remotely controlled alarm systems, or activity detection for elderly people;
- To make it possible to execute certain activities in a more convenient manner - for example: a personal inventory reminder;

Figure 3.17 Internet of Things- proliferation of connected devices across industries (Source: Beecham Research, [75])

- To generally improve life-style - for example monitoring health parameters during a workout and obtaining expert's advice based on the findings, or getting support during shopping;
- To decrease the cost of living - for example building automation that will reduce energy consumption and thus the overall cost.

The society as a user has different drivers. It is concerned with issues of importance for the whole community, often related to medium to longer term challenges.

Some of the needs driving the society as a potential user of IoT are the following:

- To ensure public safety - in the light of various recent disasters such as the nuclear catastrophe in Japan, the tsunami in the Indian Ocean, earthquakes, terrorist attacks, etc. One of the crucial concerns of the society is to be able to predict such events as far ahead as possible and to make rescue missions and recovery as efficient as possible. One good example of an application of IoT technology was during the Japan nuclear catastrophe, when numerous Geiger counters owned by individuals were connected to the Internet to provide a detailed view of radiation levels across Japan.
- To protect the environment
    - Requirements for reduction of carbon emissions have been included in various legislations and agreements aimed at reducing the impact on the planet and making sustainable development possible.
    - Monitoring of various pollutants in the environment, in particular in the air and in the water.
    - Waste management, not just general waste, but also electrical devices and various dangerous goods are important and challenging topics in every society.
    - Efficient utilization of various energy and natural resources are important for the development of a country and the protection of its resources.
- To create new jobs and ensure existing ones are sustainable - these are important issues required to maintain a high level quality of living.

Enterprises, as the third category of IoT users have different needs and different drivers that can potentially push the introduction of IoT-based solutions.

Examples of the needs are as follows:

- Increased productivity - this is at the core of most enterprises and affects the success and profitability of the enterprise;
- Market differentiation - in a market saturated with similar products and solutions, it is important to differentiate, and IoT is one of the possible differentiators;
- Cost efficiency - reducing the cost of running a business is a "mantra" for most of the CEOs. Better utilization of resources, better information used in the decision process or reduced downtime are some of the possible ways to achieve this.

The explanations of the needs of each of these three categories are given from a European perspective. To gain full understanding of these issues, it is important to capture and analyse how these needs are changing across the world. With such a complete picture, we will be able to drive IoT developments in the right direction.

Another important topic which needs to be understood is the business rationale behind each application. In other words, understanding the value an application creates.

Important research questions are: who takes the cost of creating that value; what are the revenue models and incentives for participating, using or contributing to an application? Again due to the diversity of the IoT application domain and different driving forces behind different applications, it will not be possible to define a universal business model. For example, in the case of applications used by individuals, it can be as straightforward as charging a fee for a service, which will improve their quality of life. On the other hand, community services are more difficult as they are fulfilling needs of a larger community. While it is possible that the community as a whole will be willing to pay (through municipal budgets), we have to recognise the limitations in public budgets, and other possible ways of deploying and running such services have to be investigated.

3.3 IoT Smart-X Applications

It is impossible to envisage all potential IoT applications having in mind the development of technology and the diverse needs of potential users. In the following sections, we present several applications, which are important. These applications are described, and the research challenges are identified. The IoT applications are addressing the societal needs and the advancements

to enabling technologies such as nanoelectronics and cyber-physical systems continue to be challenged by a variety of technical (i.e., scientific and engineering), institutional, and economical issues.

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

3.3.1 Smart Cities

By 2020 we will see the development of Mega city corridors and networked, integrated and branded cities. With more than 60 percent of the world population expected to live in urban cities by 2025, urbanization as a trend will have diverging impacts and influences on future personal lives and mobility. Rapid expansion of city borders, driven by increase in population and infrastructure development, would force city borders to expand outward and engulf the surrounding daughter cities to form mega cities, each with a population of more than 10 million. By 2023, there will be 30 mega cities globally, with 55 percent in developing economies of India, China, Russia and Latin America [51].

This will lead to the evolution of smart cities with eight smart features, including Smart Economy, Smart Buildings, Smart Mobility, Smart Energy, Smart Information Communication and Technology, Smart Planning, Smart Citizen and Smart Governance. There will be about 40 smart cities globally by 2025.

The role of the cities governments will be crucial for IoT deployment. Running of the day-to-day city operations and creation of city development strategies will drive the use of the IoT. Therefore, cities and their services represent an almost ideal platform for IoT research, taking into account city requirements and transferring them to solutions enabled by IoT technology.

In Europe, the largest smart city initiatives completely focused on IoT is undertaken by the FP7 SmartSantander project [69]. This project aims at deploying an IoT infrastructure comprising thousands of IoT devices spread across several cities (Santander, Guildford, Luebeck and Belgrade). This will enable simultaneous development and evaluation of services and execution of various research experiments, thus facilitating the creation of a smart city environment.

Similarly, the OUTSMART [88] project, one of the FI PPP projects, is focusing on utilities and environment in the cities and addressing the role of IoT in waste and water management, public lighting and transport systems as well as environment monitoring.

A vision of the smart city as "horizontal domain" is proposed by the BUTLER project [90], in which many vertical scenarios are integrated and concur to enable the concept of smart life.

A smart city is defined as a city that monitors and integrates conditions of all of its critical infrastructures, including roads, bridges, tunnels, rail/subways, airports, seaports, communications, water, power, even major buildings, can better optimize its resources, plan its preventive maintenance activities, and monitor security aspects while maximizing services to its citizens. Emergency response management to both natural as well as man-made challenges to the system can be focused. With advanced monitoring systems and built-in smart sensors, data can be collected and evaluated in real time, enhancing city management's decision-making. For example, resources can be committed prior to a water main break, salt spreading crews dispatched only when a specific bridge has icing conditions, and use of inspectors reduced by knowing condition of life of all structures. In the long term Smart Cities vision, systems and structures will monitor their own conditions and carry out self-repair, as needed. The physical environment, air, water, and surrounding green spaces will be monitored in non-obtrusive ways for optimal quality, thus creating an enhanced living and working environment that is clean, efficient, and secure and that offers these advantages within the framework of the most effective use of all resources [81].

An illustrative example is depicted in Figure 3.18 [96]. The deployment of ICT to create 'smart cities' is gaining momentum in Europe, according to a study by Frost & Sullivan, accentuated by the numerous pilot projects running at regional, country and EU levels. Initiatives revolve around energy and water efficiency, mobility, infrastructure and platforms for open cities, citizen involvement, and public administration services. They are co-funded by the European Union through its ICT Policy Support and 7th Framework programmes, but, the report says, there is no clear business model for the uptake of smart cities. Projects are carried out in the form of collaborative networks established between the research community, businesses, the public sector, citizens and the wider community, and they foster an open innovation approach. Technologies such as smart metering, wireless sensor networks, open platforms, high-speed broadband and cloud computing are key building blocks of the smart city infrastructure [96].

A smart city is a developed urban area that creates sustainable economic development and high quality of life by excelling in multiple key areas: economy, mobility, environment, people, living, and government [97].

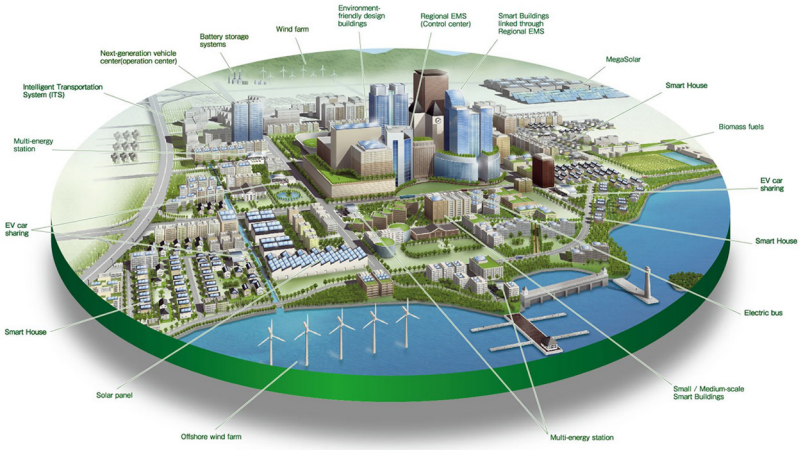

Figure 3.18 Smart City Concept. (Source: [95])

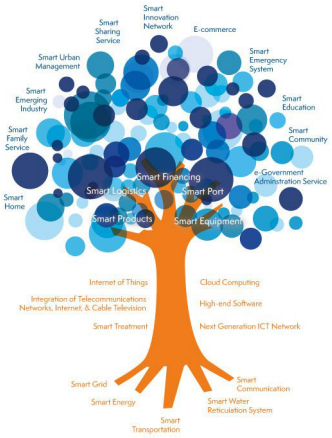

Figure 3.19 Organic Smart City Concept. (Source: [96])

Excelling in these key areas can be done so through strong human capital, social capital, and/or ICT infrastructure. With the introduction of IoT a city will act more like a living organism, a city that can respond to citizen's needs.

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

- Overcoming traditional silo based organization of the cities, with each utility responsible for their own closed world. Although not technological this is one of the main barriers

- Creating algorithms and schemes to describe information created by sensors in different applications to enable useful exchange of information between different city services
- Mechanisms for cost efficient deployment and even more important maintenance of such installations, including energy scavenging
- Ensuring reliable readings from a plethora of sensors and efficient calibration of a large number of sensors deployed everywhere from lampposts to waste bins
- Low energy protocols and algorithms
- Algorithms for analysis and processing of data acquired in the city and making "sense" out of it.
- IoT large scale deployment and integration

3.3.2 Smart Energy and the Smart Grid

There is increasing public awareness about the changing paradigm of our policy in energy supply, consumption and infrastructure. For several reasons our future energy supply should no longer be based on fossil resources. Neither is nuclear energy a future proof option. In consequence future energy supply needs to be based largely on various renewable resources. Increasingly focus must be directed to our energy consumption behaviour. Because of its volatile nature such supply demands an intelligent and flexible electrical grid which is able to react to power fluctuations by controlling electrical energy sources (generation, storage) and sinks (load, storage) and by suitable reconfiguration. Such functions will be based on networked intelligent devices (appliances, micro-generation equipment, infrastructure, consumer products) and grid infrastructure elements, largely based on IoT concepts. Although this ideally requires insight into the instantaneous energy consumption of individual loads (e.g. devices, appliances or industrial equipment) information about energy usage on a per-customer level is a suitable first approach.

Future energy grids are characterized by a high number of distributed small and medium sized energy sources and power plants which may be combined virtually ad hoc to virtual power plants; moreover in the case of energy outages or disasters certain areas may be isolated from the grid and supplied from within by internal energy sources such as photovoltaics on the roofs, block heat and power plants or energy storages of a residential area ("islanding").

A grand challenge for enabling technologies such as cyber-physical systems is the design and deployment of an energy system infrastructure that is able to provide blackout free electricity generation and distribution, is flexible enough to allow heterogeneous energy supply to or withdrawal from the grid,

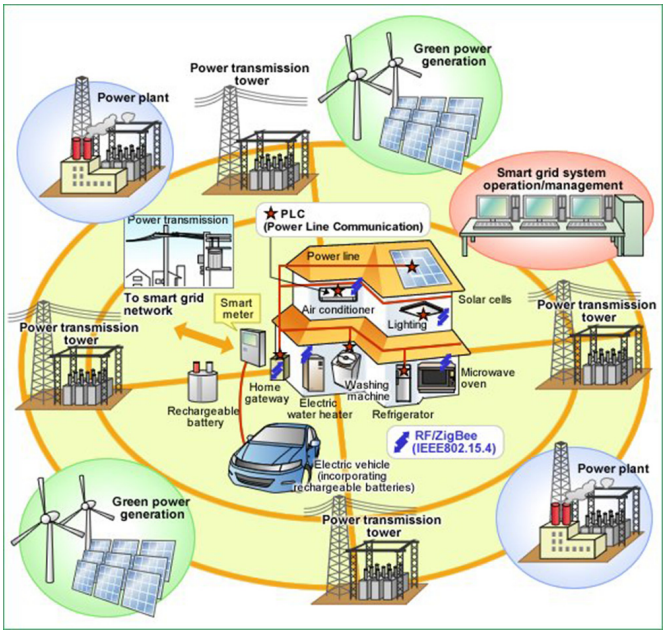

Figure 3.20 Smart Grid Representation

and is impervious to accidental or intentional manipulations. Integration of cyber-physical systems engineering and technology to the existing electric grid and other utility systems is a challenge. The increased system complexity poses technical challenges that must be considered as the system is operated in ways that were not intended when the infrastructure was originally built. As technologies and systems are incorporated, security remains a paramount concern to lower system vulnerability and protect stakeholder data [83]. These challenges will need to be address as well by the IoT applications that integrate heterogeneous cyber-physical systems.

The developing Smart Grid is expected to implement a new concept of transmission network which is able to efficiently route the energy which is produced from both concentrated and distributed plants to the final user with high security and quality of supply standards. Therefore the Smart Grid is expected to be the implementation of a kind of "Internet" in which the energy packet is managed similarly to the data packet - across routers and gateways which autonomously can decide the best pathway for the packet to reach its destination with the best integrity levels. In this respect the "Internet of Energy" concept is defined as a network infrastructure based on standard and

Figure 3.21 Internet of Energy Concept

interoperable communication transceivers, gateways and protocols that will allow a real time balance between the local and the global generation and storage capability with the energy demand. This will also allow a high level of consumer awareness and involvement.

The Internet of Energy (IoE) 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. Power consumption monitoring will be performed on all levels, from local individual devices up to national and international level [102].

Saving energy based on an improved user awareness of momentary energy consumption is another pillar of future energy management concepts. Smart meters can give information about the instantaneous energy consumption to the user, thus allowing for identification and elimination of energy wasting devices and for providing hints for optimizing individual energy consumption. In a smart grid scenario energy consumption will be manipulated by a volatile energy price which again is based on the momentary demand (acquired by smart meters) and the available amount of energy and renewable energy production. In a virtual energy marketplace software agents may negotiate energy prices and place energy orders to energy companies. It is already recognised that these decisions need to consider environmental information such as weather forecasts, local and seasonal conditions. These must be to a much finer time scale and spatial resolution.

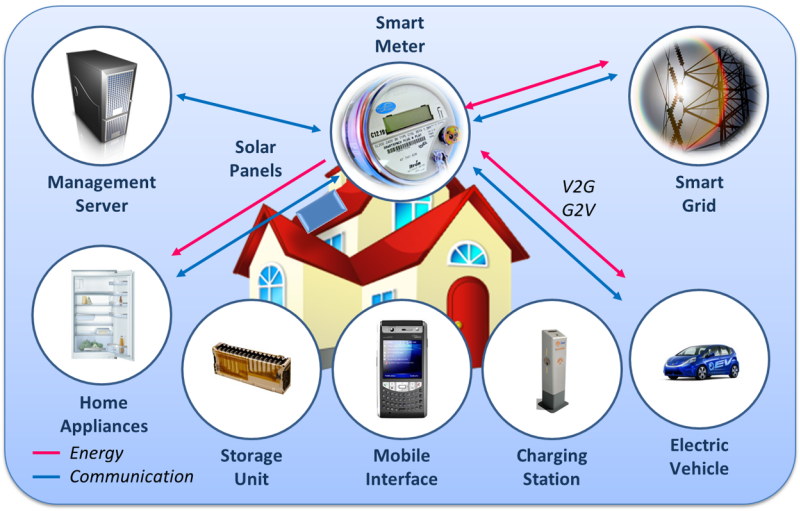

Figure 3.22 Internet of Energy: Residential Building Ecosystem [102]

In the long run electro mobility will become another important element of smart power grids. Electric vehicles (EVs) might act as a power load as well as moveable energy storage linked as IoT elements to the energy information grid (smart grid). IoT enabled smart grid control may need to consider energy demand and offerings in the residential areas and along the major roads based on traffic forecast. EVs will be able to act as sink or source of energy based on their charge status, usage schedule and energy price which again may depend on abundance of (renewable) energy in the grid. This is the touch point from where the following telematics IoT scenarios will merge with smart grid IoT.

This scenario is based on the existence of an IoT network of a vast multitude of intelligent sensors and actuators which are able to communicate safely and reliably. Latencies are critical when talking about electrical control loops. Even though not being a critical feature, low energy dissipation should be mandatory. In order to facilitate interaction between different vendors' products the technology should be based on a standardized communication protocol stack. When dealing with a critical part of the public infrastructure, data security is of the highest importance. In order to satisfy the extremely high requirements on reliability of energy grids, the components as well as their interaction must feature the highest reliability performance.

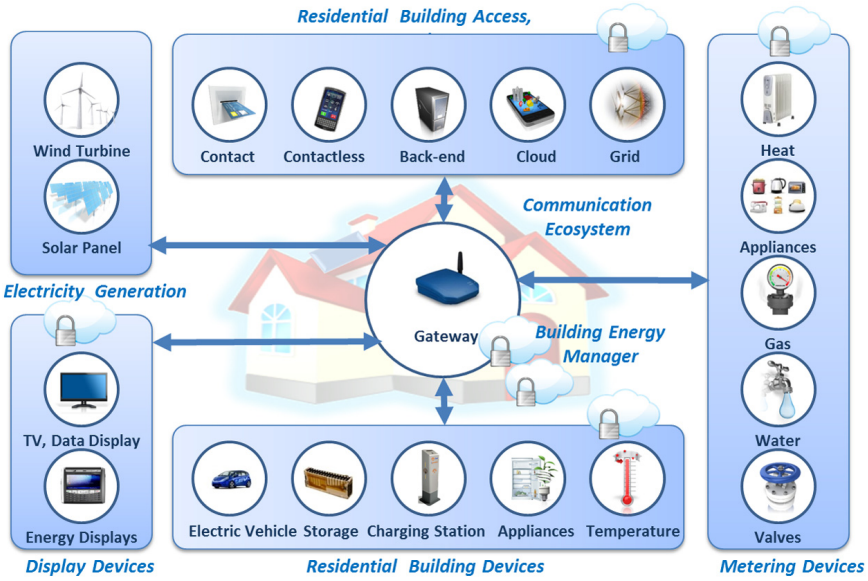

Figure 3.23 Internet of Energy – Residential Ecosystem

New organizational and learning strategies for sensor networks will be needed in order to cope with the shortcomings of classical hierarchical control concepts. The intelligence of smart systems does not necessarily need to be built into the devices at the systems' edges. Depending on connectivity, cloud-based IoT concepts might be advantageous when considering energy dissipation and hardware effort. Many IoT applications will go beyond one industrial sector. Energy, mobility and home/buildings sectors will share data through energy gateways that will control the transfer of energy and information.

Sophisticated and flexible data filtering, data mining and processing procedures and systems will become necessary in order to handle the high amount of raw data provided by billions of data sources. System and data models need to support the design of flexible systems which guarantee a reliable and secure real-time operation.

Some Research Challenges:

- Absolutely safe and secure communication with elements at the network edge
- Addressing scalability and standards interoperability
- Energy saving robust and reliable smart sensors/actuators

- Technologies for data anonymity addressing privacy concerns
- Dealing with critical latencies, e.g. in control loops
- System partitioning (local/cloud based intelligence)
- Mass data processing, filtering and mining; avoid flooding of communication network
- Real-time Models and design methods describing reliable interworking of heterogeneous systems (e.g. technical / economical / social / environmental systems). Identifying and monitoring critical system elements. Detecting critical overall system states in due time
- System concepts which support self-healing and containment of damage; strategies for failure contingency management
- Scalability of security functions
- Power grids have to be able to react correctly and quickly to fluctuations in the supply of electricity from renewable energy sources such as wind and solar facilities.

3.3.3 Smart Mobility and Transport

The connection of vehicles to the Internet gives rise to a wealth of new possibilities and applications which bring new functionalities to the individuals and/or the making of transport easier and safer. In this context the concept of Internet of Vehicles (IoV) [102] connected with the concept of Internet of Energy (IoE) represent future trends for smart transportation and mobility applications.

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

Representing human behaviour in the design, development, and operation of cyber physical systems in autonomous vehicles is a challenge. Incorporating human-in-the-loop considerations is critical to safety, dependability, and predictability. There is currently limited understanding of how driver behaviour will be affected by adaptive traffic control cyber physical systems. In addition, it is difficult to account for the stochastic effects of the human driver in a mixed traffic environment (i.e., human and autonomous vehicle drivers) such as that found in traffic control cyber physical systems. Increasing integration calls for security measures that are not physical, but more logical while still ensuring there will be no security compromise. As cyber physical systems become more complex and interactions between components increases, safety and security

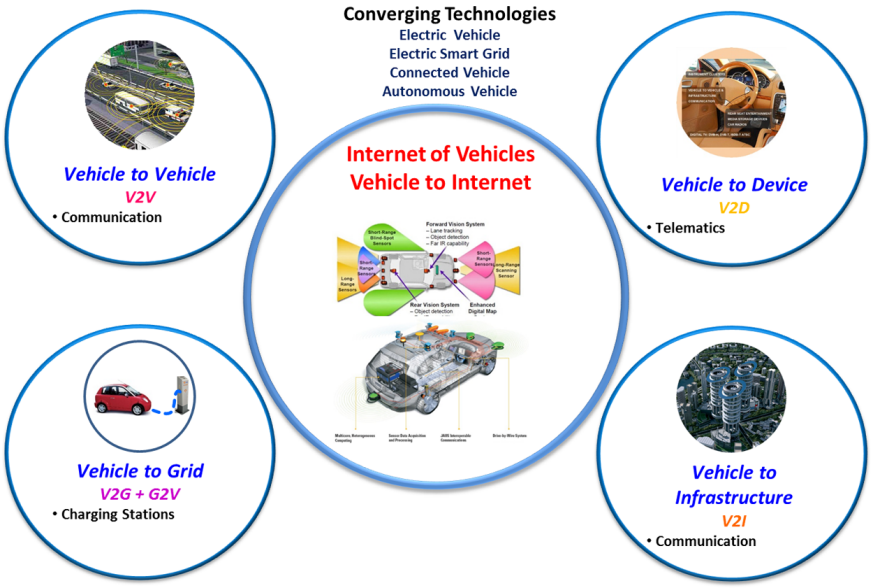

Figure 3.24 Technologies Convergence – Internet of Vehicles Case

will continue to be of paramount importance [83]. All these elements are of the paramount importance for the IoT ecosystems developed based on these enabling technologies.

When talking about IoT in the context of automotive and telematics, we may refer to the following application scenarios:

- Standards must be defined regarding the charging voltage of the power electronics, and a decision needs to be made as to whether the recharging processes should be controlled by a system within the vehicle or one installed at the charging station.
- Components for bidirectional operations and flexible billing for electricity need to be developed if electric vehicles are to be used as electricity storage media.
- **IoT as an inherent part of the vehicle control and management system**: Already today certain technical functions of the vehicles' on-board systems can be monitored on line by the service centre or garage to allow for preventative maintenance, remote diagnostics, instantaneous support and timely availability of spare parts. For this purpose data from on-board sensors are collected by a smart on-board unit and communicated via the Internet to the service centre.

- **IoT enabling traffic management and control**: Cars should be able to organise themselves in order to avoid traffic jams and to optimise drive energy usage. This may be done in coordination and cooperation with the infrastructure of a smart city's traffic control and management system. Additionally dynamic road pricing and parking tax can be important elements of such a system. Further mutual communications between the vehicles and with the infrastructure enable new methods for considerably increasing traffic safety, thus contributing to the reduction in the number of traffic accidents.
- **IoT enabling new transport scenarios (multi-modal transport):** In such scenarios, e.g. automotive OEMs see themselves as mobility providers rather than manufacturers of vehicles. The user will be offered an optimal solution for transportation from A to B, based on all available and suitable transport means. Thus, based on the momentary traffic situation an ideal solution may be a mix of individual vehicles, vehicle sharing, railway, and commuter systems. In order to allow for seamless usage and on-time availability of these elements (including parking space), availability needs to be verified and guaranteed by online reservation and online booking, ideally in interplay with the above mentioned smart city traffic management systems.
- **Autonomous driving and interfacing with the infrastructure (V2V, V2I):** The challenges address the interaction between the vehicle and the environment (sensors, actuators, communication, processing, information exchange, etc.) by considering road navigation systems that combines road localization and road shape estimation to drive on roads where a priori road geometry both is and is not available. Address a mixed-mode planning system that is able to both efficiently navigate on roads and safely manoeuvre through open areas and parking lots and develop a behavioural engine that is capable of both following the rules of the road and avoid them when necessary.

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

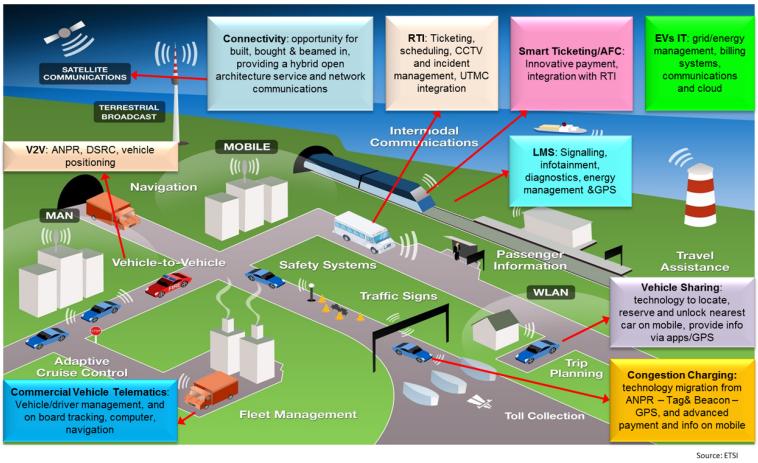

Figure 3.25 ITS Ecosystem (Source: ETSI)

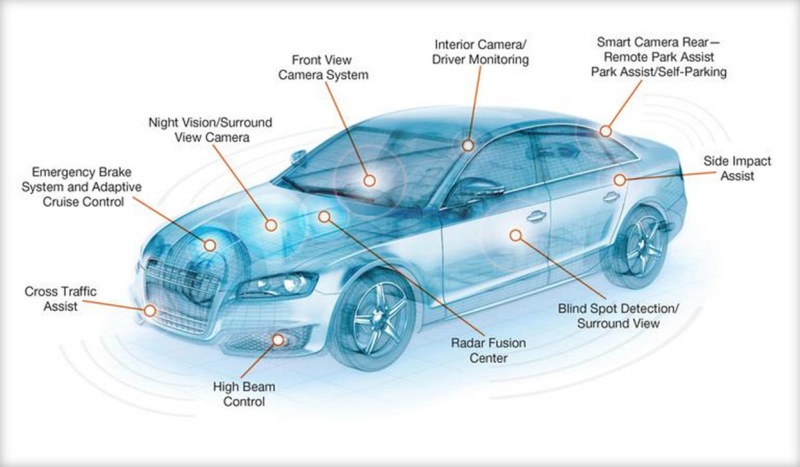

Figure 3.26 Communication and computer vision technologies for driver-assistance and V2V/V2I interaction [80].

the computer-controlled vehicles that Google, Volvo, and other companies are working on [80].

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

Technical elements of such systems are smart phones and smart vehicle on-board units which acquire information from the user (e.g. position, destination

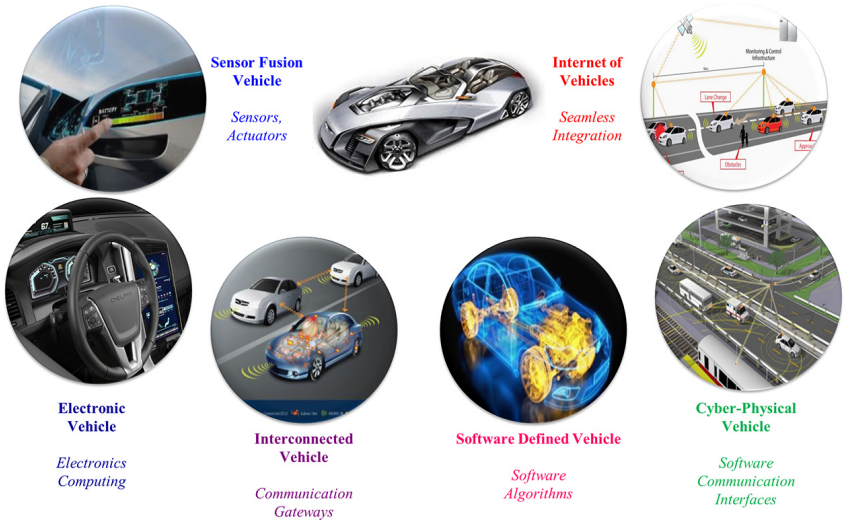

Figure 3.27 Internet of Vehicles Concept

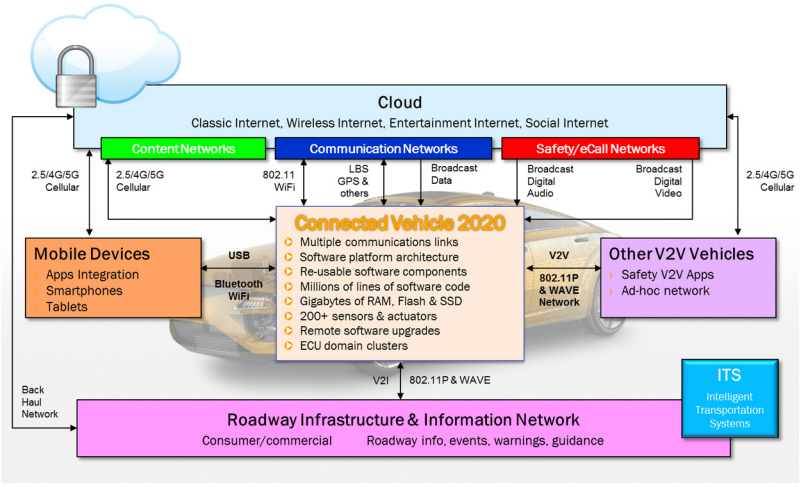

Figure 3.28 Connected Vehicle 2020-Mobility Ecosystem (Source: Continental Corporation)

and schedule) and from on board systems (e.g. vehicle status, position, energy usage profile, driving profile). They interact with external systems (e.g. traffic control systems, parking management, vehicle sharing managements, electric vehicle charging infrastructure). Moreover they need to initiate and perform the related payment procedures.

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

Smart sensors in the road and traffic control infrastructures need to collect information about road and traffic status, weather conditions, etc. This requires robust sensors (and actuators) which are able to reliably deliver information to the systems mentioned above. Such reliable communication needs to be based on M2M communication protocols which consider the timing, safety, and security constraints. The expected high amount of data will require sophisticated data mining strategies. Overall optimisation of traffic flow and energy usage may be achieved by collective organisation among the individual vehicles. First steps could be the gradual extension of DATEX-II by IoT related technologies and information. The (international) standardisation of protocol stacks and interfaces is of utmost importance to enable economic competition and guarantee smooth interaction of different vendor products.

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

Some research challenges:

- Safe and secure communication with elements at the network edge, inter-vehicle communication, and vehicle to infrastructure communication
- Energy saving robust and reliable smart sensors and actuators in vehicles and infrastructure
- Technologies for data anonymity addressing privacy concerns
- System partitioning (local/cloud based intelligence)
- Identifying and monitoring critical system elements. Detecting critical overall system states in due time
- Technologies supporting self-organisation and dynamic formation of structures / re-structuring
- Ensure an adequate level of trust and secure exchange of data among different vertical ICT infrastructures (e.g., intermodal scenario).

3.3.4 Smart Home, Smart Buildings and Infrastructure

The rise of Wi-Fi's role in home automation has primarily come about due to the networked nature of deployed electronics where electronic devices (TVs and AV receivers, mobile devices, etc.) have started becoming part of the home IP network and due the increasing rate of adoption of mobile computing devices (smartphones, tablets, etc.).

Several organizations are working to equip homes with technology that enables the occupants to use a single device to control all electronic devices and appliances. The solutions focus primarily on environmental monitoring, energy management, assisted living, comfort, and convenience. The solutions are based on open platforms that employ a network of intelligent sensors to provide information about the state of the home. These sensors monitor systems such as energy generation and metering; heating, ventilation, and air conditioning (HVAC); lighting; security; and environmental key performance indicators. The information is processed and made available through a number of access methods such as touch screens, mobile phones, and 3–D browsers [110]. The networking aspects are bringing online streaming services or network playback, while becoming a mean to control of the device functionality over the network. At the same time mobile devices ensure that consumers have access to a portable 'controller' for the electronics connected to the network. Both types of devices can be used as gateways for IoT applications. In this context many companies are considering building platforms that

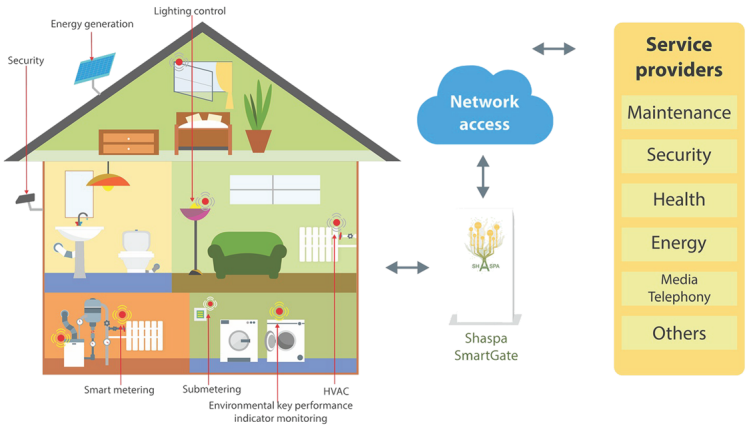

Figure 3.29 Integrated equipment and appliances [109].

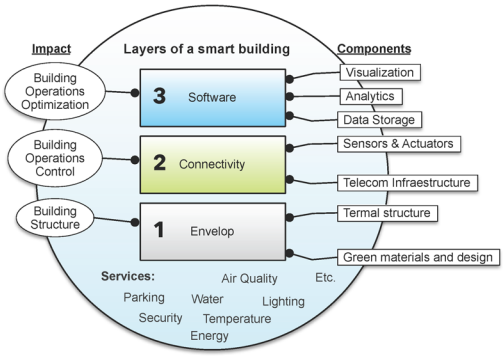

Figure 3.30 Smart Buildings Layers [36]

integrate the building automation with entertainment, healthcare monitoring, energy monitoring and wireless sensor monitoring in the home and building environments.

IoT applications using sensors to collect information about operating conditions combined with cloud hosted analytics software that analyse disparate data points will help facility managers become far more proactive about managing buildings at peak efficiency.

From the technological point of view, it is possible to identify the different layers of a smart building in more detail, to understand the correlation of the systems, services, and management operations. For each layer, is important to understand the implied actors, stakeholders and best practices to implement different technological solutions [36].

Issues of building ownership (i.e., building owner, manager, or occupants) challenge integration with questions such as who pays initial system cost and who collects the benefits over time. A lack of collaboration between the subsectors of the building industry slows new technology adoption and can prevent new buildings from achieving energy, economic and environmental performance targets.

From the layers of a smart building there are many integrated services that can be seen as subsystems. The set of services are managed to provide the best conditions for the activities of the building occupants. The figure below presents the taxonomy of basic services.

Integration of cyber physical systems both within the building and with external entities, such as the electrical grid, will require stakeholder cooperation to achieve true interoperability. As in all sectors, maintaining security will be a critical challenge to overcome [83].

Figure 3.31 Smart Building Services Taxonomy [36]

Figure 3.32 Internet of Buildings Concept

Within this field of research the exploitation of the potential of wireless sensor networks (WSNs) to facilitate intelligent energy management in buildings, which increases occupant comfort while reducing energy demand, is highly relevant. In addition to the obvious economic and environmental gains from the introduction of such intelligent energy management in buildings other positive effects will be achieved. Not least of which is the simplification of building control; as placing monitoring, information feedback equipment and control capabilities in a single location will make a buildings' energy management system easier to handle for the building owners, building managers, maintenance crews and other users of the building.

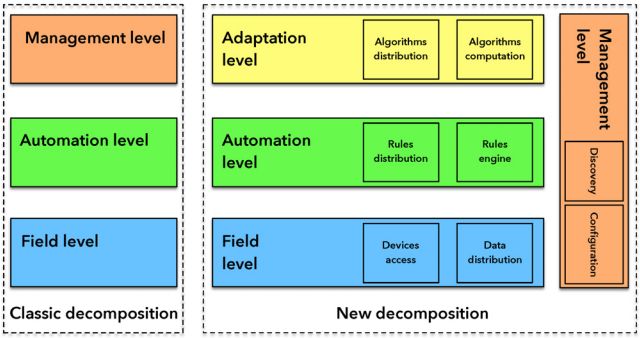

Figure 3.33 Level based architecture of building automation systems [48]

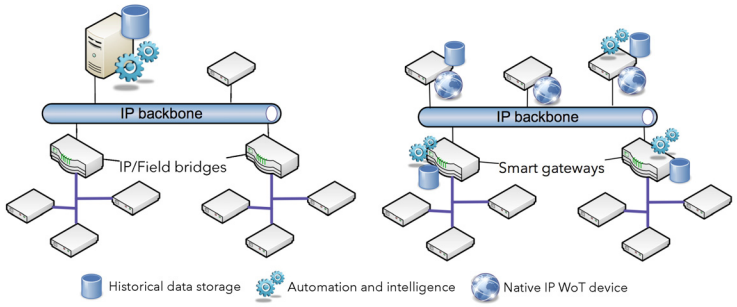

Figure 3.34 Role distribution for a classical building automation system and for a Web-of-Things architecture [48]

Using the Internet together with energy management systems also offers an opportunity to access a buildings' energy information and control systems from a laptop or a Smartphone placed anywhere in the world. This has a huge potential for providing the managers, owners and inhabitants of buildings with energy consumption feedback and the ability to act on that information.

The perceived evolution of building system architectures includes an adaptation level that will dynamically feed the automation level with control logic, i.e. rules. Further, in the IoT approach, the management level has also to be made available transversally as configuration; discovery and monitoring services must be made accessible to all levels. Algorithms and rules have also to be considered as Web resources in a similar way as for sensors and actuators. The repartition of roles for a classical building automation system to the new web of things enabled architecture is different and in this context, future works

will have to be carried on to find solutions to minimize the transfer of data and the distribution of algorithms [48].

In the context of the future 'Internet of Things', Intelligent Building Management Systems can be considered part of a much larger information system. This system is used by facilities managers in buildings to manage energy use and energy procurement and to maintain buildings systems. It is based on the infrastructure of the existing Intranets and the Internet, and therefore utilises the same standards as other IT devices. Within this context reductions in the cost and reliability of WSNs are transforming building automation, by making the maintenance of energy efficient, healthy, productive work spaces in buildings increasingly cost effective [72].

3.3.5 Smart Factory and Smart Manufacturing

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

The first evolutionary step towards a shared smart factory could be demonstrated by enabling access to today's external stakeholders in order to interact with an IoT-enabled manufacturing system. These stakeholders could include the suppliers of the productions tools (e.g. machines, robots), as well as the production logistics (e.g. material flow, supply chain management), and maintenance and re-tooling actors. An IoT-based architecture that challenges the hierarchical and closed factory automation pyramid, by allowing the above-mentioned stakeholders to run their services in multiple tier flat production system is proposed in [199]. This means that the services and applications of tomorrow do not need to be defined in an intertwined and strictly linked manner to the physical system, but rather run as services in a shared physical world. The room for innovation in the application space could be increased in the same degree of magnitude as this has been the case for embedded applications or Apps, which have exploded since the arrival

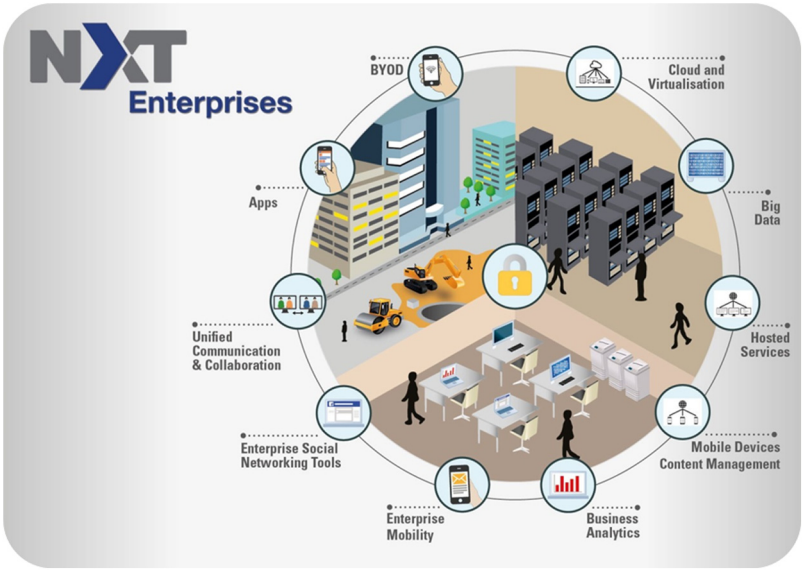

Figure 3.35 Connected Enterprise [61]

of smart phones (i.e. the provision of a clear and well standardized interface to the embedded hardware of a mobile phone to be accessed by all types of Apps).

Enterprises are making use of the huge amount of data available, business analytics, cloud services, enterprise mobility and many others to improve the way businesses are being conducted. These technologies include big data and business analytics software, cloud services, embedded technology, sensor networks / sensing technology, RFID, GPS, M2M, mobility, security and ID recognition technology, wireless network and standardisation.

One key enabler to this ICT-driven smart and agile manufacturing lies in the way we manage and access the physical world, where the sensors, the actuators, and also the production unit should be accessed, and managed in the same or at least similar IoT standard interfaces and technologies. These devices are then providing their services in a well-structured manner, and can be managed and orchestrated for a multitude of applications running in parallel.

The convergence of microelectronics and micromechanical parts within a sensing device, the ubiquity of communications, the rise of micro-robotics, the customization made possible by software will significantly change the world of manufacturing. In addition, broader pervasiveness of telecommunications

in many environments is one of the reasons why these environments take the shape of ecosystems.

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

Most companies have a difficult time justifying risky, expensive, and uncertain investments for smart manufacturing across the company and factory level. Changes to the structure, organization, and culture of manufacturing occur slowly, which hinders technology integration. Pre-digital age control systems are infrequently replaced because they are still serviceable. Retrofitting these existing plants with cyber-physical systems is difficult and expensive. The lack of a standard industry approach to production management results in customized software or use of a manual approach. There is also a need for a unifying theory of non-homogeneous control and communication systems [82].

3.3.6 Smart Health

The market for health monitoring devices is currently characterised by application-specific solutions that are mutually non-interoperable and are made up of diverse architectures. While individual products are designed to cost targets, the long-term goal of achieving lower technology costs across current and future sectors will inevitably be very challenging unless a more coherent approach is used. The IoT can be used in clinical care where hospitalized patients whose physiological status requires close attention can be constantly monitored using IoT -driven, noninvasive monitoring. This requires sensors to collect comprehensive physiological information and uses gateways and the cloud to analyze and store the information and then send the analyzed data wirelessly to caregivers for further analysis and review. These techniques improve the quality of care through constant attention and lower the cost of care by eliminating the need for a caregiver to actively engage in data collection and analysis. In addition the technology can be used for remote monitoring using small, wireless solutions connected through the IoT. These solutions can be used to securely capture patient health data from a variety of sensors, apply complex algorithms to analyze the data and then share it through wireless connectivity with medical professionals who can make appropriate health recommendations.

The links between the many applications in health monitoring are:

- gathering of data from sensors
- support user interfaces and displays

- network connectivity for access to infrastructural services
- low power, robustness, durability, accuracy and reliability.

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

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

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

Challenges exist in the overall cyber-physical infrastructure (e.g., hardware, connectivity, software development and communications), specialized processes at the intersection of control and sensing, sensor fusion and decision making, security, and the compositionality of cyber-physical systems. Proprietary medical devices in general were not designed for interoperation with other medical devices or computational systems, necessitating advancements in networking and distributed communication within cyber-physical architectures. Interoperability and closed loop systems appears to be the key for success. System security will be critical as communication of individual

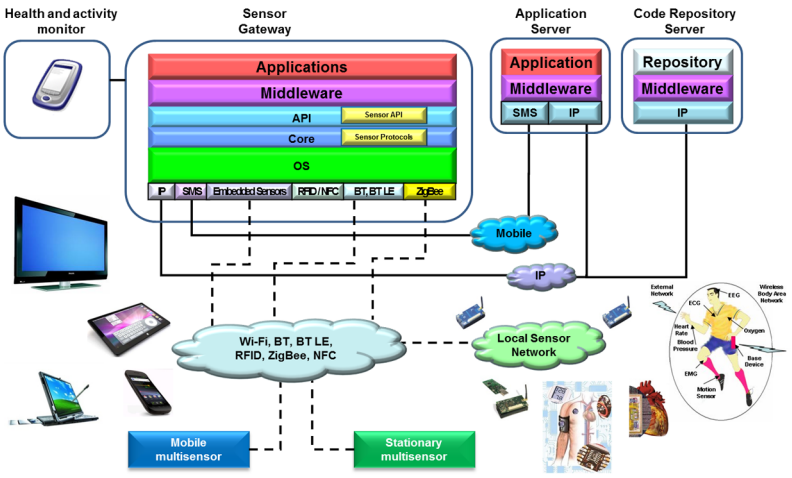

Figure 3.36 Smart Health Platform

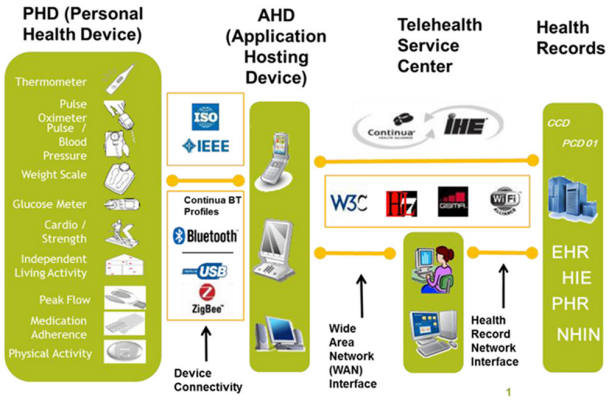

Figure 3.37 Interoperable standard interfaces in the Continua Personal Health Eco-System (Source: Continua Health Alliance)

patient data is communicated over cyber-physical networks. In addition, validating data acquired from patients using new cyber-physical technologies against existing gold standard data acquisition methods will be a challenge. Cyber-physical technologies will also need to be designed to operate with minimal patient training or cooperation [83].

New and innovative technologies are needed to cope with the trends on wired, wireless, high-speed interfaces, miniaturization and modular design approaches for products having multiple technologies integrated.

Internet of Things applications have a future market potential for electronic health services and connected telecommunication industry. In this context, the telecommunications can foster the evolution of ecosystems in different application areas. Medical expenditures are in the range of 10% of the European gross domestic product. The market segment of telemedicine, one of lead markets of the future will have growth rates of more than 19%.

The Continua Health Alliance, an industry consortium promoting telehealth and guaranteeing end-to-end interoperability from sensors to health record databases, has defined in its design guidelines, a dual interface for communication with physiological and residential sensors showing a Personal Area Network (PAN) interface based on Bluetooth Low Energy (BLE) standard and its health device profiles, and a Local Area Network (LAN) interface, based on the Zigbee Health Care application profile. The standards are relatively similar in terms of complexity but BLE, tends to have a longer battery life primarily due to the use of short packet overhead and faster data rates, reduced number of packet exchanges for a short discovery/connect time, and skipped

communication events, while Zigbee benefits from a longer range and better reliability with the use of a robust modulation scheme (Direct Sequence Spread Spectrum with orthogonal coding and a mesh-like clustered star networking technology)

Convergence of bio parameter sensing, communication technologies and engineering is turning health care into a new type of information industry. In this context the progress beyond state of the art for IoT applications for healthcare is envisaged as follows:

- Standardisation of interface from sensors and MEMS for an open platform to create a broad and open market for bio-chemical innovators.
- Providing a high degree of automation in the taking and processing of information;
- Real-time data over networks (streaming and regular single measurements) to be available to clinicians anywhere on the web with appropriate software and privileges;
- Data travelling over trusted web.
- Reuse of components over smooth progression between low-cost "home health" devices and higher cost "professional" devices.
- Data needs to be interchangeable between all authorised devices in use within the clinical care pathway, from home, ambulance, clinic, GP, hospital, without manual transfer of data.

3.3.7 Food and Water Tracking and Security

Food and fresh water are the most important natural resources in the world. Organic food produced without addition of certain chemical substances and according to strict rules, or food produced in certain geographical areas will be particularly valued. Similarly, fresh water from mountain springs is already highly valued. In the future it will be very important to bottle and distribute water adequately. This will inevitably lead to attempts to forge the origin or the production process. Using IoT in such scenarios to secure tracking of food or water from the production place to the consumer is one of the important topics.

This has already been introduced to some extent in regard to beef meat. After the "mad cow disease" outbreak in the late 20th century, some beef manufacturers together with large supermarket chains in Ireland are offering "from pasture to plate" traceability of each package of beef meat in an attempt to assure consumers that the meat is safe for consumption. However, this is

limited to certain types of food and enables tracing back to the origin of the food only, without information on the production process.

IoT applications need to have a development framework that will assure the following:

- The things connected to the Internet need to provide value. The things that are part of the IoT need to provide a valuable service at a price point that enables adoption, or they need to be part of a larger system that does.
- Use of rich ecosystem for the development. The IoT comprises things, sensors, communication systems, servers, storage, analytics, and end user services. Developers, network operators, hardware manufacturers, and software providers need to come together to make it work. The partnerships among the stakeholders will provide functionality easily available to the customers.
- Systems need to provide APIs that let users take advantage of systems suited to their needs on devices of their choice. APIs also allow developers to innovate and create something interesting using the system's data and services, ultimately driving the system's use and adoption.
- Developers need to be attracted since the implementation will be done on a development platform. Developers using different tools to develop solutions, which work across device platforms playing a key role for future IoT deployment.
- Security needs to be built in. Connecting things previously cut off from the digital world will expose them to new attacks and challenges.

The research challenges are:

- Design of secure, tamper-proof and cost-efficient mechanisms for tracking food and water from production to consumers, enabling immediate notification of actors in case of harmful food and communication of trusted information.
- Secure way of monitoring production processes, providing sufficient information and confidence to consumers. At the same time details of the production processes which might be considered as intellectual property, should not be revealed.
- Ensure trust and secure exchange of data among applications and infrastructures (farm, packing industry, retailers) to prevent the introduction of false or misleading data, which can affect the health of the citizens or create economic damage to the stakeholders.

3.3.8 Participatory Sensing

People live in communities and rely on each other in everyday activities. Recommendations for a good restaurant, car mechanic, movie, phone plan etc. were and still are some of the things where community knowledge helps us in determining our actions.

While in the past this community wisdom was difficult to access and often based on inputs from a handful of people, with the proliferation of the web and more recently social networks, the community knowledge has become readily available - just a click away.

Today, the community wisdom is based on conscious input from people, primarily based on opinions of individuals. With the development of IoT technology and ICT in general, it is becoming interesting to expand the concept of community knowledge to automated observation of events in the real world.

One application of participatory sensing is as a tool for health and wellness, where individuals can self-monitor to observe and adjust their medication, physical activity, nutrition, and interactions. Potential contexts include chronic-disease management and health behaviour change. Communities and health professionals can also use participatory approaches to better understand the development and effective treatment of disease. The same systems can be used as tools for sustainability. Individuals and communities can explore their transportation and consumption habits, and corporations can promote more sustainable practices among employees. In addition, participatory sensing offers a powerful "make a case" technique to support advocacy and civic engagement. It can provide a framework in which citizens can bring to light a civic bottleneck, hazard, personal-safety concern, cultural asset, or other data relevant to urban and natural-resources planning and services, all using data that are systematic and can be validated [121].

Smart phones are already equipped with a number of sensors and actuators: camera, microphone, accelerometers, temperature gauge, speakers, displays etc. A range of other portable sensing products that people will carry in their pockets will soon become available as well. Furthermore, our cars are equipped with a range of sensors capturing information about the car itself, and also about the road and traffic conditions.

Intel is working to simplify deployment of the Internet of Things (IoT) with its Intelligent Systems Framework (Intel®ISF), a set of interoperable solutions designed to address connecting, managing, and securing devices and data in a consistent and scalable manner.

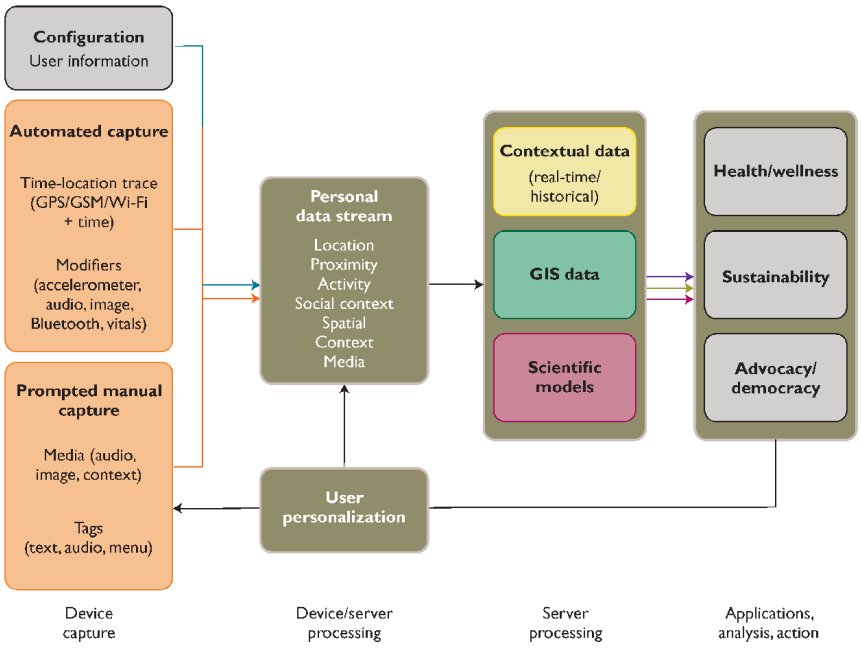

Figure 3.38 Common architectural components for participatory-sensing applications, including mobile device data capture, personal data stream storage, and leveraged data processing [121]

Participatory sensing applications aim at utilizing each person, mobile phone, and car and associated sensors as automatic sensory stations taking a multi-sensor snapshot of the immediate environment. By combining these individual snapshots in an intelligent manner it is possible to create a clear picture of the physical world that can be shared and for example used as an input to the smart city services decision processes.

However, participatory sensing applications come with a number of challenges that need to be solved:

- Design of algorithms for normalization of observations taking into account the conditions under which the observations were taken. For example temperature measurements will be different if taken by a mobile phone in a pocket or a mobile phone lying on a table;
- Design of robust mechanisms for analysis and processing of collected observations in real time (complex event processing) and generation of

"community wisdom" that can be reliably used as an input to decision taking;
- Reliability and trustworthiness of observed data, i.e. design of mechanisms that will ensure that observations were not tampered with and/or detection of such unreliable measurements and consequent exclusion from further processing. In this context, the proper identification and authentication of the data sources is an important function;
- Ensuring privacy of individuals providing observations
- Efficient mechanisms for sharing and distribution of "community wisdom".
- Addressing scalability and large scale deployments

3.3.9 Smart Logistics and Retail

The Internet of Things creates opportunities to achieve efficient solutions in the retail sector by addressing the right person, right content at the right time and right place.

A personalized connected experience is what users are looking for in today's digital environment. Connectivity is key to be connected anytime, anywhere with any devices.

Adapting to the tastes and priorities of changing populations will be a critical task for retailers worldwide.

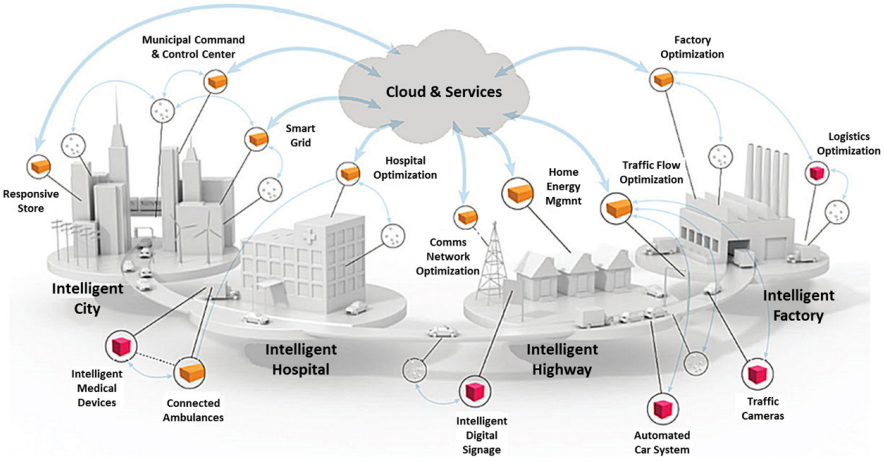

Figure 3.39 Internet of Things: Intelligent Systems Framework (Source: Intel)

To keep up with all these changes, retailers must deploy smart, connected devices throughout their operations.

By tying together everything from inventory tracking to advertising, retailers can gain visibility into their operations and nimbly respond to shifts in consumer behaviour. The challenge is finding a scalable, secure, manageable path to deploying all of these systems.

Retailers are also using sensors, beacons, scanning devices, and other IoT technologies to optimize internally: inventory, fleet, resource, and partner management through real-time analytics, automatic replenishment, notifications, store layout, and more. The Big data generated now affords retailers a factual understanding of how their products, customers, affiliates, employees, and external factors come together. Altogether, this is a $1.6T opportunity for retailers, with $81B in value already realized in 2013 [64].

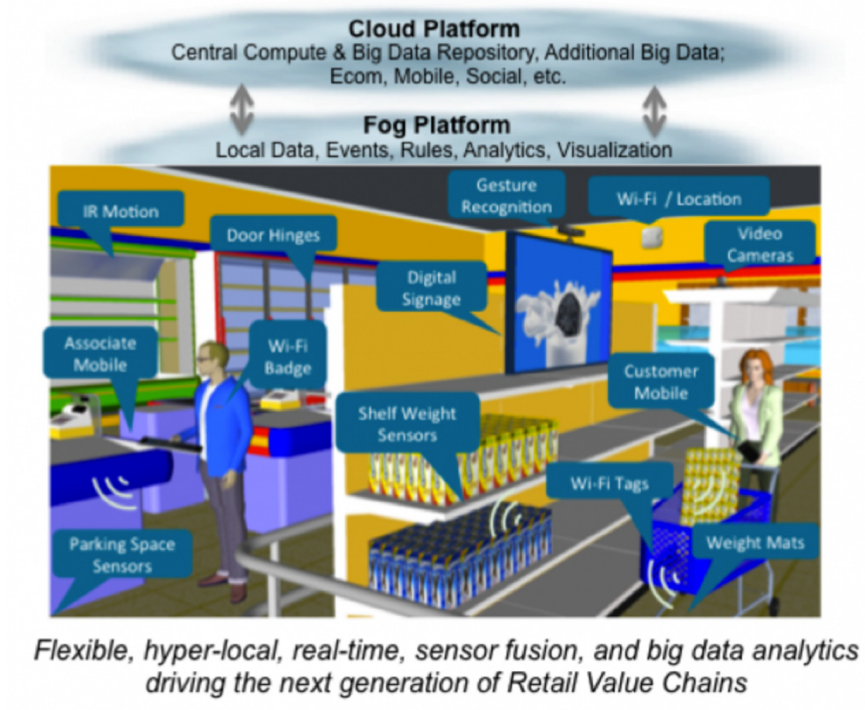

Figure 3.40 The Digital Retail Store (Source: Cisco)

3.4 Internet of Things and Related Future Internet Technologies

3.4.1 Cloud Computing

Since the publication of the 2011 SRA, cloud computing has been established as one of the major building blocks of the Future Internet. New technology enablers have progressively fostered virtualisation at different levels and have allowed the various paradigms known as "Applications as a Service", "Platforms as a Service" and "Infrastructure and Networks as a Service". Such trends have greatly helped to reduce cost of ownership and management of associated virtualised resources, lowering the market entry threshold to new players and enabling provisioning of new services. With the virtualisation of objects being the next natural step in this trend, the convergence of cloud computing and Internet of Things will enable unprecedented opportunities in the IoT services arena [104].

As part of this convergence, IoT applications (such as sensor-based services) will be delivered on-demand through a cloud environment [105]. This extends beyond the need to virtualize sensor data stores in a scalable fashion. It asks for virtualization of Internet-connected objects and their ability to become orchestrated into on-demand services (such as Sensing-as-a-Service).

Inadequate security will be a critical barrier to large-scale deployment of IoT systems and broad customer adoption of IoT applications. Simply extending existing IT security architectures to the IoT will not be sufficient. The connected things in the future will have limited resources that can't be easily or cost-effectively upgraded. In order to protect these things over a very long lifespan, this increases the importance of cloud-based security services with resource-efficient, thing-to-cloud interactions. With the growth of IoT, we're shifting toward a cyber-physical paradigm, where we closely integrate

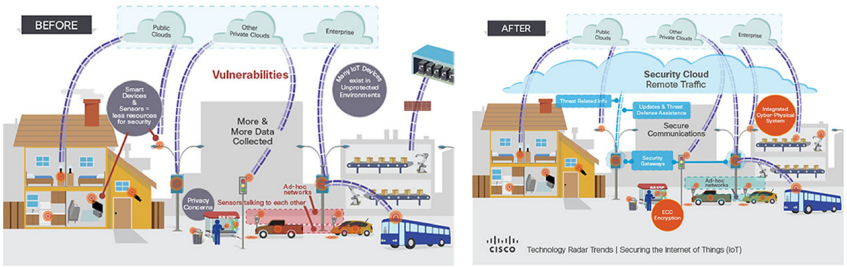

Figure 3.41 Securely Integrating the Cyber and Physical Worlds (Source: Cisco)

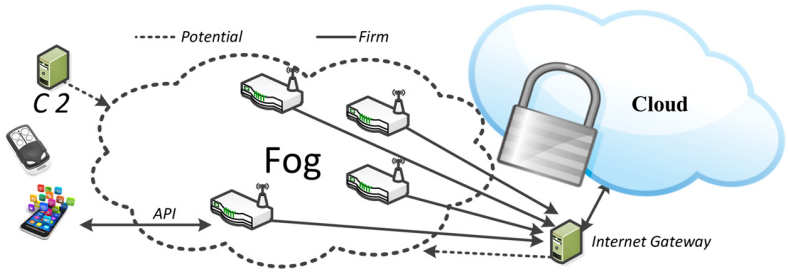

Figure 3.42 Fog Computing Paradigm

computing and communication with the connected things, including the ability to control their operations. In such systems, many security vulnerabilities and threats come from the interactions between the cyber and physical domains. An approach to holistically integrate security vulnerability analysis and protections in both domains will become increasingly necessary. There is growing demand to secure the rapidly increasing population of connected, and often mobile, things. In contrast to today's networks, where assets under protection are typically inside firewalls and protected with access control devices, many things in the IoT arena will operate in unprotected or highly vulnerable environments (i.e. vehicles, sensors, and medical devices used in homes and embedded on patients). Protecting such things poses additional challenges beyond enterprise networks [59].

Many Internet of Things applications require mobility support and geo-distribution in addition to location awareness and low latency, while the data need to be processed in "real-time" in micro clouds or fog. Micro cloud or Fog computing enables new applications and services applies a different data management and analytics and extends the Cloud Computing paradigm to the edge of the network. Similar to Cloud, Micro Cloud/Fog provides data, compute, storage, and application services to end-users.

The Micro Cloud or the fog needs to have the following features in order to efficiently implement the required IoT applications:

- Low latency and location awareness;
- Wide-spread geographical distribution;
- Mobility;
- Very large number of nodes,
- Predominant role of wireless access,
- Strong presence of streaming and real time applications,
- Heterogeneity.

Moreover, generalising the serving scope of an Internet-connected object beyond the "sensing service", it is not hard to imagine virtual objects that will be integrated into the fabric of future IoT services and shared and reused in different contexts, projecting an "Object as a Service" paradigm aimed as in other virtualised resource domains at minimising costs of ownership and maintenance of objects, and fostering the creation of innovative IoT services.

Relevant topics for the research agenda will therefore include:

- The description of requests for services to a cloud/IoT infrastructure,
- The virtualization of objects,
- Tools and techniques for optimization of cloud infrastructures subject to utility and SLA criteria,
- The investigation of utility metrics and (reinforcement) learning techniques that could be used for gauging on-demand IoT services in a cloud environment,
- Techniques for real-time interaction of Internet-connected objects within a cloud environment through the implementation of lightweight interactions and the adaptation of real-time operating systems.
- Access control models to ensure the proper access to the data stored in the cloud.

3.4.2 IoT and Semantic Technologies

The previous IERC SRIAs have identified the importance of semantic technologies towards discovering devices, as well as towards achieving semantic interoperability. Future research on IoT is likely to embrace the concept of Linked Open Data. This could build on the earlier integration of ontologies (e.g., sensor ontologies) into IoT infrastructures and applications.

Semantic technologies will also have a key role in enabling sharing and re-use of virtual objects as a service through the cloud, as illustrated in the previous paragraph. The semantic enrichment of virtual object descriptions will realise for IoT what semantic annotation of web pages has enabled in the Semantic Web. Associated semantic-based reasoning will assist IoT users to more independently find the relevant proven virtual objects to improve the performance or the effectiveness of the IoT applications they intend to use.

3.5 Networks and Communication

Present communication technologies span the globe in wireless and wired networks and support global communication by globally-accepted communication standards. The Internet of Things Strategic Research and Innovation Agenda (SRIA) intends to lay the foundations for the Internet of Things to be developed by research through to the end of this decade and for subsequent innovations to be realised even after this research period. Within this timeframe the number of connected devices, their features, their distribution and implied communication requirements will develop; as will the communication infrastructure and the networks being used. Everything will change significantly. Internet of Things devices will be contributing to and strongly driving this development.

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

3.5.1 Networking Technology

Mobile traffic today is driven by predictable activities such as making calls, receiving email, surfing the web, and watching videos. Over the next 5 to 10 years, billions of IoT devices with less predictable traffic patterns will join the network, including vehicles, machine-to-machine (M2M) modules, video surveillance that requires all the time bandwidth, or different types of sensors sensor that send out tiny bits of data each day. The rise of cloud computing requires new network strategies for fifth evolution of mobile the 5G, which represents clearly a convergence of network access technologies. The architecture of such network has to integrate the needs for IoT applications and to offer seamless integration. To make the IoT and M2M communication possible there is a need for fast, high-capacity networks.

5G networks will deliver 1,000 to 5,000 times more capacity than 3G and 4G networks today and will be made up of cells that support peak rates of between 10 and 100Gbps. They need to be ultra-low latency, meaning it will take data 1–10 milliseconds to get from one designated point to another, compared to 40–60 milliseconds today. Another goal is to separate communications infrastructure and allow mobile users to move seamlessly between 5G, 4G, and WiFi, which will be fully integrated with the cellular network. Networks will also increasingly become programmable, allowing

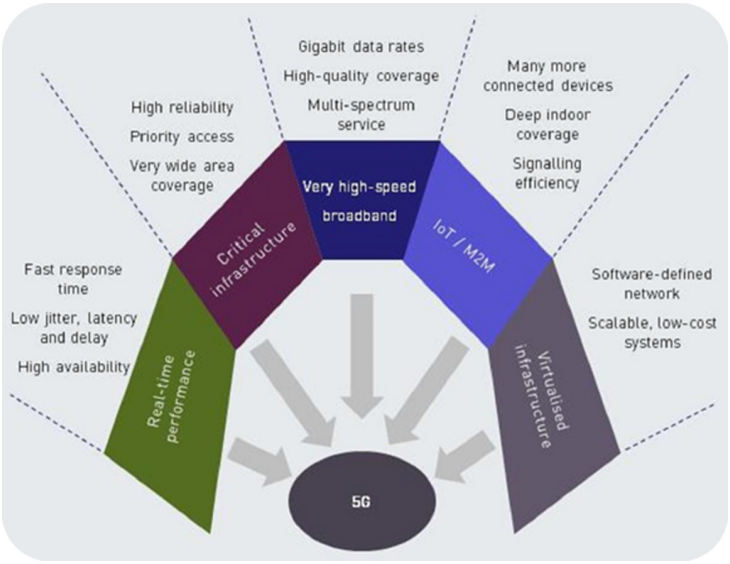

Figure 3.43 5G Features

operators to make changes to the network virtually, without touching the physical infrastructure. These features are important for IoT applications.

The evolution and pervasiveness of present communication technologies has the potential to grow to unprecedented levels in the near future by including the world of things into the developing Internet of Things.

Network users will be humans, machines, things and groups of them.

3.5.1.1 Complexity of the networks of the future

A key research topic will be to understand the complexity of these future networks and the expected growth of complexity due to the growth of Internet of Things. The research results of this topic will give guidelines and timelines for defining the requirements for network functions, for network management, for network growth and network composition and variability [150].

Wireless networks cannot grow without such side effects as interference.

3.5.1.2 Growth of wireless networks

Wireless networks especially will grow largely by adding vast amounts of small Internet of Things devices with minimum hardware, software and intelligence, limiting their resilience to any imperfections in all their functions.

Based on the research of the growing network complexity, caused by the Internet of Things, predictions of traffic and load models will have to guide further research on unfolding the predicted complexity to real networks, their standards and on-going implementations.

Mankind is the maximum user group for the mobile phone system, which is the most prominent distributed system worldwide besides the fixed telephone system and the Internet. Obviously the number of body area networks [36], [151], [152], and of networks integrated into clothes and further personal area networks – all based on Internet of Things devices - will be of the order of the current human population. They are still not unfolding into reality. In a second stage cross network cooperative applications are likely to develop, which are not yet envisioned.

3.5.1.3 Mobile networks

Applications such as body area networks may develop into an autonomous world of small, mobile networks being attached to their bearers and being connected to the Internet by using a common point of contact. The mobile phone of the future could provide this function.

Analysing worldwide industrial processes will be required to find limiting set sizes for the number of machines and all things being implied or used within their range in order to develop an understanding of the evolution steps to the Internet of Things in industrial environments.

3.5.1.4 Expanding current networks to future networks

Generalizing the examples given above, the trend may be to expand current end user network nodes into networks of their own or even a hierarchy of networks. In this way networks will grow on their current access side by unfolding these outermost nodes into even smaller, attached networks, spanning the Internet of Things in the future. In this context networks or even networks of networks will be mobile by themselves.

3.5.1.5 Overlay networks

Even if network construction principles should best be unified for the worldwide Internet of Things and the networks bearing it, there will not be one unified network, but several. In some locations even multiple networks overlaying one another physically and logically.

The Internet and the Internet of Things will have access to large parts of these networks. Further sections may be only represented by a top access node or may not be visible at all globally. Some networks will by intention be

shielded against external access and secured against any intrusion on multiple levels.

3.5.1.6 Network self-organization

Wireless networks being built for the Internet of Things will show a large degree of ad-hoc growth, structure, organization, and significant change in time, including mobility. These constituent features will have to be reflected in setting them up and during their operation [153].

Self-organization principles will be applied to configuration by context sensing, especially concerning autonomous negotiation of interference management and possibly cognitive spectrum usage, by optimization of network structure and traffic and load distribution in the network, and in self-healing of networks. All will be done in heterogeneous environments, without interaction by users or operators.

3.5.1.7 IPv6, IoT and Scalability

The current transition of the global Internet to IPv6 will provide a virtually unlimited number of public IP addresses able to provide bidirectional and symmetric (true M2M) access to Billions of smart things. It will pave the way to new models of IoT interconnection and integration. It is raising numerous questions: How can the Internet infrastructure cope with a highly heterogeneous IoT and ease a global IoT interconnection? How interoperability will happen with legacy systems? What will be the impact of the transition to IPv6 on IoT integration, large scale deployment and interoperability? It will probably require developing an IPv6-based European research infrastructure for the IoT.

3.5.1.8 Green networking technology

Network technology has traditionally developed along the line of predictable progress of implementation technologies in all their facets. Given the enormous expected growth of network usage and the number of user nodes in the future, driven by the Internet of Things, there is a real need to minimize the resources for implementing all network elements and the energy being used for their operation [154].

Disruptive developments are to be expected by analysing the energy requirements of current solutions and by going back to principles of communication in wired, optical and wireless information transfer. Research done by Bell Labs [155][156] in recent years shows that networks can achieve

an energy efficiency increase of a factor of 1,000 compared to current technologies [157].

The results of the research done by the GreenTouch consortium [155] should be integrated into the development of the network technologies of the future. These network technologies have to be appropriate to realise the Internet of Things and the Future Internet in their most expanded state to be anticipated by the imagination of the experts.

3.5.2 Communication Technology

3.5.2.1 Unfolding the potential of communication technologies

The research aimed at communication technology to be undertaken in the coming decade will have to develop and unfold all potential communication profiles of Internet of Things devices, from bit-level communication to continuous data streams, from sporadic connections to connections being always on, from standard services to emergency modes, from open communication to fully secured communication, spanning applications from local to global, based on single devices to globally-distributed sets of devices [158].

In this context the growth in mobile device market is pushing the deployment of Internet of Things applications where these mobile devices (smart phones, tablets, etc.) are seen as gateways for wireless sensors and actuators.

Based on this research the anticipated bottlenecks in communications and in networks and services will have to be quantified using appropriate theoretical methods and simulation approaches.

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

3.5.2.2 Correctness of construction

Correctness of construction [159] of the whole system is a systematic process that starts from the small systems running on the devices up to network and distributed applications. Methods to prove the correctness of structures and of transformations of structures will be required, including protocols of communication between all levels of communication stacks used in the Internet of Things and the Future Internet.

These methods will be essential for the Internet of Things devices and systems, as the smallest devices will be implemented in hardware and many

types will not be programmable. Interoperability within the Internet of Things will be a challenge even if such proof methods are used systematically.

3.5.2.3 An unified theoretical framework for communication

Communication between processes [160] running within an operating system on a single or multicore processor, communication between processes running in a distributed computer system [161], and the communication between devices and structures in the Internet of Things and the Future Internet using wired and wireless channels shall be merged into a unified minimum theoretical framework covering and including formalized communication within protocols.

In this way minimum overhead, optimum use of communication channels and best handling of communication errors should be achievable. Secure communication could be embedded efficiently and naturally as a basic service.

3.5.2.4 Energy-limited Internet of Things devices and their communication

Many types of Internet of Things devices will be connected to the energy grid all the time; on the other hand a significant subset of Internet of Things devices will have to rely on their own limited energy resources or energy harvesting throughout their lifetime.

Given this spread of possible implementations and the expected importance of minimum-energy Internet of Things devices and applications, an important topic of research will have to be the search for minimum energy, minimum computation, slim and lightweight solutions through all layers of Internet of Things communication and applications.

3.5.2.5 Challenge the trend to complexity

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

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

3.5.2.6 Disruptive approaches

Given these special restrictions, non-standard, but already existing ideas should be carefully checked again and be integrated into existing solutions, and disruptive approaches shall be searched and researched with high priority.

This very special domain of the Internet of Things may well develop into its most challenging and most rewarding domain – from a research point of view and, hopefully, from an economical point of view as well.

3.6 Processes

The deployment of IoT technologies will significantly impact and change the way enterprises do business as well as interactions between different parts of the society, affecting many processes. To be able to reap the many potential benefits that have been postulated for the IoT, several challenges regarding the modelling and execution of such processes need to be solved in order to see wider and in particular commercial deployments of IoT [162]. The special characteristics of IoT services and processes have to be taken into account and it is likely that existing business process modelling and execution languages as well as service description languages such as USDL [165], will need to be extended.

3.6.1 Adaptive and Event-Driven Processes

One of the main benefits of IoT integration is that processes become more adaptive to what is actually happening in the real world. Inherently, this is based on events that are either detected directly or by real-time analysis of sensor data. Such events can occur at any time in the process. For some of the events, the occurrence probability is very low: one knows that they might occur, but not when or if at all. Modelling such events into a process is cumbersome, as they would have to be included into all possible activities, leading to additional complexity and making it more difficult to understand the modelled process, in particular the main flow of the process (the 80% case). Secondly, how to react to a single event can depend on the context, i.e. the set of events that have been detected previously.

Research on adaptive and event-driven processes could consider the extension and exploitation of EDA (Event Driven Architectures) for activity monitoring and complex event processing (CEP) in IoT systems. EDA could be combined with business process execution languages in order to trigger specific steps or parts of a business process.

3.6.2 Processes Dealing with Unreliable Data

When dealing with events coming from the physical world (e.g., via sensors or signal processing algorithms), a degree of unreliability and uncertainty

is introduced into the processes. If decisions in a business process are to be taken based on events that have some uncertainty attached, it makes sense to associate each of these events with some value for the quality of information (QoI). In simple cases, this allows the process modeller to define thresholds: e.g., if the degree of certainty is more than 90%, then it is assumed that the event really happened. If it is between 50% and 90%, some other activities will be triggered to determine if the event occurred or not. If it is below 50%, the event is ignored. Things get more complex when multiple events are involved: e.g., one event with 95% certainty, one with 73%, and another with 52%. The underlying services that fire the original events have to be programmed to attach such QoI values to the events. From a BPM perspective, it is essential that such information can be captured, processed and expressed in the modelling notation language, e.g. BPMN. Secondly, the syntax and semantics of such QoI values need to be standardized. Is it a simple certainty percentage as in the examples above, or should it be something more expressive (e.g., a range within which the true value lies)? Relevant techniques should not only address uncertainty in the flow of a given (well-known) IoT-based business process, but also in the overall structuring and modelling of (possibly unknown or unstructured) process flows. Techniques for fuzzy modelling of data and processes could be considered.

3.6.3 Processes dealing with unreliable resources

Not only is the data from resources inherently unreliable, but also the resources providing the data themselves, e.g., due to the failure of the hosting device. Processes relying on such resources need to be able to adapt to such situations. The first issue is to detect such a failure. In the case that a process is calling a resource directly, this detection is trivial. When we're talking about resources that might generate an event at one point in time (e.g., the resource that monitors the temperature condition within the truck and sends an alert if it has become too hot), it is more difficult. Not having received any event can be because of resource failure, but also because there was nothing to report. Likewise, the quality of the generated reports should be regularly audited for correctness. Some monitoring software is needed to detect such problems; it is unclear though if such software should be part of the BPM execution environment or should be a separate component. Among the research challenges is the synchronization of monitoring processes with run-time actuating processes, given that management planes (e.g., monitoring

software) tend to operate at different time scales from IoT processes (e.g., automation and control systems in manufacturing).

3.6.4 Highly Distributed Processes

When interaction with real-world objects and devices is required, it can make sense to execute a process in a decentralized fashion. As stated in [165], the decomposition and decentralization of existing business processes increases scalability and performance, allows better decision making and could even lead to new business models and revenue streams through entitlement management of software products deployed on smart items. For example, in environmental monitoring or supply chain tracking applications, no messages need to be sent to the central system as long as everything is within the defined limits. Only if there is a deviation, an alert (event) needs to be generated, which in turn can lead to an adaptation of the overall process. From a business process modelling perspective though, it should be possible to define the process centrally, including the fact that some activities (i.e., the monitoring) will be done remotely. Once the complete process is modelled, it should then be possible to deploy the related services to where they have to be executed, and then run and monitor the complete process.

Relevant research issues include tools and techniques for the synthesis, the verification and the adaptation of distributed processes, in the scope of a volatile environment (i.e. changing contexts, mobility, internet connected objects/devices that join or leave).

3.7 Data Management

Data management is a crucial aspect in the Internet of Things. When considering a world of objects interconnected and constantly exchanging all types of information, the volume of the generated data and the processes involved in the handling of those data become critical.

A long-term opportunity for wireless communications chip makers is the rise of machine-to-machine (M2M) computing, which one of the enabling technologies for Internet of Things. This technology spans a broad range of applications. Worldwide M2M interconnected devices are on a steady upward march that is expected to surge 10-fold to a global total of 12.5 billion devices by 2020. The resulting forecast in M2M traffic shows a similar trajectory, with traffic predicted to grow 24-fold from 2012–2017, representing a CAGR (Compound Annual Growth Rate) of 89% over the same period. Revenue

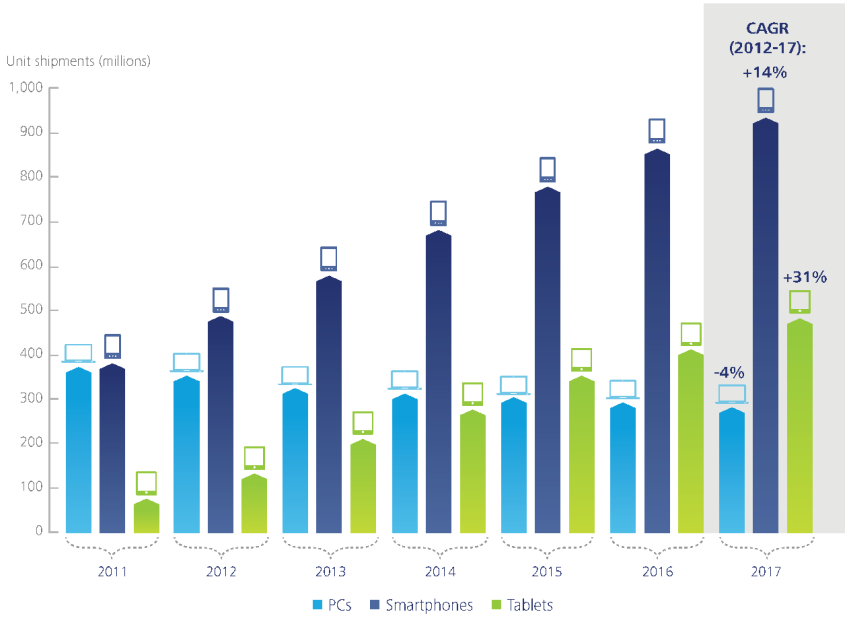

Figure 3.44 PCs, smartphones, and tablets: Unit shipment forecast, worldwide, 2011–2017 [74]

from M2M services spanning a wide range of industry vertical applications, including telematics, health monitoring, smart buildings and security, smart metering, retail point of sale, and retail banking, is set to reach $35 billion by 2016. Driving this surge in the M2M market are a number of forces such as the declining cost of mobile device and infrastructure technology, increased deployment of IP, wireless and wireline networks, and a low-cost opportunity for network carriers to eke out new revenue streams by utilizing existing infrastructure in new markets. This opportunity will likely be most prominent across a number of enterprise verticals, with the energy industry-in the form of smart grid and smart metering technologies-expected to experience significant growth in the M2M market [75].

In this context there are many technologies and factors involved in the "data management" within the IoT context.

Some of the most relevant concepts which enable us to understand the challenges and opportunities of data management are:

- Data Collection and Analysis
- Big data

- Semantic Sensor Networking
- Virtual Sensors
- Complex Event Processing.

3.7.1 Data Collection and Analysis (DCA)

Data Collection and Analysis modules or capabilities are the essential components of any IoT platform or system, and they are constantly evolving in order to support more features and provide more capacity to external components (either higher layer applications leveraging on the data stored by the DCA module or other external systems exchanging information for analysis or processing).

The DCA module is part of the core layer of any IoT platform. Some of the main functions of a DCA module are:

User/customer data storing:

Provides storage of the customer's information collected by sensors

User data & operation modelling:

Allows the customer to create new sensor data models to accommodate collected information and the modelling of the supported operations

On demand data access:

Provides APIs to access the collected data

Device event publish/subscribe/forwarding/notification:

Provides APIs to access the collected data in real time conditions

Customer rules/filtering:

Allows the customer to establish its own filters and rules to correlate events

Customer task automation:

Provides the customer with the ability to manage his automatic processes. (e.g. scheduled platform originated data collection).

Customer workflows:

Allows the customer to create his own workflow to process the incoming events from a device

Multitenant structure:

Provides the structure to support multiple organizations and reseller schemes.

In the coming years, the main research efforts should be targeted to some features that should be included in any Data Collection and Analysis platform:

- **Multi-protocol**. DCA platforms should be capable of handling or understanding different input (and output) protocols and formats. Different

standards and wrappings for the submission of observations should be supported
- **De-centralisation**. Sensors and measurements/observations captured by them should be stored in systems that can be de-centralised from a single platform. It is essential that different components, geographically distributed in different locations may cooperate and exchange data. Related with this concept, federation among different systems will make possible the global integration of IoT architectures.
- **Security**. DCA platforms should increase the level of data protection and security, from the transmission of messages from devices (sensors, actuators, etc.) to the data stored in the platform.
- **Data mining** features. Ideally, DCA systems should also integrate capacities for the processing of the stored info, making it easier to extract useful data from the huge amount of contents that may be recorded.

3.7.2 Big Data

Big data is about the processing and analysis of large data repositories, so disproportionately large that it is impossible to treat them with the conventional tools of analytical databases. Some statements suggest that we are entering the "Industrial Revolution of Data," [167], where the majority of data will be stamped out by machines. These machines generate data a lot faster than people can, and their production rates will grow exponentially with Moore's Law. Storing this data is cheap, and it can be mined for valuable information. Examples of this tendency include:

- Web logs;
- RFID;
- Sensor networks;
- Social networks;
- Social data (due to the Social data revolution);
- Internet text and documents;
- Internet search indexing;
- Call detail records;
- Astronomy, atmospheric science, genomics, biogeochemical, biological, and other complex and/or interdisciplinary scientific research;
- Military surveillance;
- Medical records;
- Photography archives;

- Video archives;
- Large scale e-commerce.

The trend is part of an environment quite popular lately: the proliferation of web pages, image and video applications, social networks, mobile devices, apps, sensors, and so on, able to generate, according to IBM, more than 2.5 quintillion bytes per day, to the extent that 90% of the world's data have been created over the past two years.

Big data requires exceptional technologies to efficiently process large quantities of data within a tolerable amount of time. Technologies being applied to big data include massively parallel processing (MPP) databases, data-mining grids, distributed file systems, distributed databases, cloud computing platforms, the Internet, and scalable storage systems. These technologies are linked with many aspects derived from the analysis of natural phenomena such as climate and seismic data to environments such as health, safety or, of course, the business environment.

The biggest challenge of the Petabyte Age will not be storing all that data, it will be figuring out how to make sense of it. Big data deals with unconventional, unstructured databases, which can reach petabytes, exabytes or zettabytes, and require specific treatments for their needs, either in terms of storage or processing/display.

Companies focused on the big data topic, such as Google, Yahoo!, Facebook or some specialised start-ups, currently do not use Oracle tools to process their big data repositories, and they opt instead for an approach based on distributed, cloud and open source systems. An extremely popular example is Hadoop, an Open Source framework in this field that allows applications to work with huge repositories of data and thousands of nodes. These have been inspired by Google tools such as the MapReduce and Google File system,

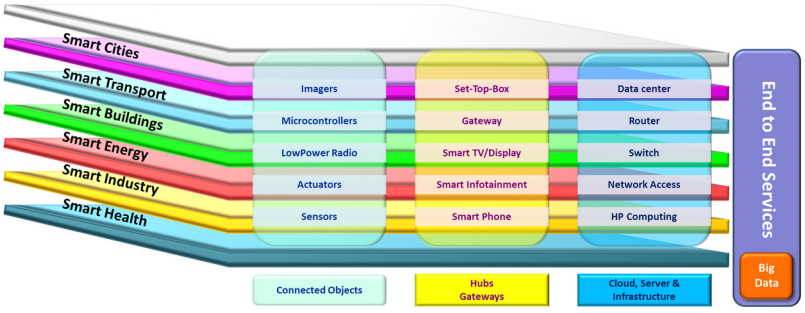

Figure 3.45 Internet of Things holistic view

or NoSQL systems, which in many cases do not comply with the ACID (atomicity, consistency, isolation, durability) characteristics of conventional databases.

In future, it is expected a huge increase in adoption, and many, many questions that must be addressed. Among the imminent research targets in this field are:

- Privacy. Big data systems must avoid any suggestion that users and citizens in general perceive that their privacy is being invaded.
- Integration of both relational and NoSQL systems.
- More efficient indexing, search and processing algorithms, allowing the extraction of results in reduced time and, ideally, near to "real time" scenarios.
- Optimised storage of data. Given the amount of information that the new IoT world may generate, it is essential to avoid that the storage requirements and costs increase exponentially.

3.7.3 Semantic Sensor Networks and Semantic Annotation of data

The information collected from the physical world in combination with the existing resources and services on the Web facilitate enhanced methods to obtain business intelligence, enabling the construction of new types of front-end application and services which could revolutionise the way organisations and people use Internet services and applications in their daily activities. Annotating and interpreting the data, and also the network resources, enables management of the e large scale distributed networks that are often resource and energy constrained, and provides means that allow software agents and intelligent mechanisms to process and reason the acquired data.

There are currently on-going efforts to define ontologies and to create frameworks to apply semantic Web technologies to sensor networks. The Semantic Sensor Web (SSW) proposes annotating sensor data with spatial, temporal, and thematic semantic metadata [169]. This approach uses the current OGC and SWE [171] specifications and attempts to extend them with semantic web technologies to provide enhanced descriptions to facilitate access to sensor data. W3C Semantic Sensor Networks Incubator Group [172] is also working on developing ontology for describing sensors. Effective description of sensor, observation and measurement data and utilising semantic Web technologies for this purpose, are fundamental steps to the construction of semantic sensor networks.

However, associating this data to the existing concepts on the Web and reasoning the data is also an important task to make this information widely available for different applications, front-end services and data consumers.

Semantics allow machines to interpret links and relations between different attributes of a sensor description and also other resources. Utilising and reasoning this information enables the integration of the data as networked knowledge [174]. On a large scale this machine interpretable information (i.e. semantics) is a key enabler and necessity for the semantic sensor networks. Emergence of sensor data as linked-data enables sensor network providers and data consumers to connect sensor descriptions to potentially endless data existing on the Web. By relating sensor data attributes such as location, type, observation and measurement features to other resources on the Web of data, users will be able to integrate physical world data and the logical world data to draw conclusions, create business intelligence, enable smart environments, and support automated decision making systems among many other applications.

The linked-sensor-data can also be queried, accessed and reasoned based on the same principles that apply to linked-data. The principles of using linked data to describe sensor network resources and data in an implementation of an open platform to publish and consume interoperable sensor data is described in [175].

In general, associating sensor and sensor network data with other concepts (on the Web) and reasoning makes the data information widely available for different applications, front-end services and data consumers. The semantic description allow machines to interpret links and relations between the different attributes of a sensor description and also other data existing on the Web or provided by other applications and resources. Utilising and reasoning this information enables the integration of the data on a wider scale, known as networked knowledge [174]. This machine-interpretable information (i.e. semantics) is a key enabler for the semantic sensor networks.

3.7.4 Virtual Sensors

A virtual sensor can be considered as a product of spatial, temporal and/or thematic transformation of raw or other virtual sensor producing data with necessary provenance information attached to this transformation. Virtual sensors and actuators are a programming abstraction simplifying the development of decentralized WSN applications [176].

Models for interacting with wireless sensors such as Internet of Things and sensor cloud aim to overcome restricted resources and efficiency. New sensor clouds need to enable different networks, cover a large geographical area, connect together and be used simultaneously by multiple users on demand. Virtual sensors, as the core of the sensor cloud architecture, assist in creating a multiuser environment on top of resource-constrained physical wireless sensors and can help in supporting multiple applications.

The data acquired by a set of sensors can be collected, processed according to an application-provided aggregation function, and then perceived as the reading of a single virtual sensor. Dually, a virtual actuator provides a single entry point for distributing commands to a set of real actuator nodes. We follow that statement with this definition:

- A virtual sensor behaves just like a real sensor, emitting time-series data from a specified geographic region with newly defined thematic concepts or observations which the real sensors may not have.
- A virtual sensor may not have any real sensor's physical properties such as manufacturer or battery power information, but does have other properties, such as: who created it; what methods are used, and what original sensors it is based on.

3.8 Security, Privacy & Trust

The Internet of Things presents security-related challenges that are identified in the IERC 2010 Strategic Research and Innovation Roadmap but some elaboration is useful as there are further aspects that need to be addressed by the research community. While there are a number of specific security, privacy and trust challenges in the IoT, they all share a number of transverse non-functional requirements:

- Lightweight and symmetric solutions, Support for resource constrained devices
- Scalable to billions of devices/transactions

Solutions will need to address federation/administrative co-operation

- Heterogeneity and multiplicity of devices and platforms
- Intuitively usable solutions, seamlessly integrated into the real world

3.8.1 Trust for IoT

As IoT-scale applications and services will scale over multiple administrative domains and involve multiple ownership regimes, there is a need for a trust framework to enable the users of the system to have confidence that the information and services being exchanged can indeed be relied upon. The trust framework needs to be able to deal with humans and machines as users, i.e. it needs to convey trust to humans and needs to be robust enough to be used by machines without denial of service. The development of trust frameworks that address this requirement will require advances in areas such as:

- Lightweight Public Key Infrastructures (PKI) as a basis for trust management. Advances are expected in hierarchical and cross certification concepts to enable solutions to address the scalability requirements.
- Lightweight key management systems to enable trust relationships to be established and the distribution of encryption materials using minimum communications and processing resources, as is consistent with the resource constrained nature of many IoT devices.
- Quality of Information is a requirement for many IoT-based systems where metadata can be used to provide an assessment of the reliability of IoT data.
- Decentralised and self-configuring systems as alternatives to PKI for establishing trust e.g. identity federation, peer to peer.
- Novel methods for assessing trust in people, devices and data, beyond reputation systems. One example is Trust Negotiation. Trust Negotiation is a mechanism that allows two parties to automatically negotiate, on the basis of a chain of trust policies, the minimum level of trust required to grant access to a service or to a piece of information.
- Assurance methods for trusted platforms including hardware, software, protocols, etc.
- Access Control to prevent data breaches. One example is Usage Control, which is the process of ensuring the correct usage of certain information according to a predefined policy after the access to information is granted.

3.8.2 Security for IoT

As the IoT becomes a key element of the Future Internet and a critical national/international infrastructure, the need to provide adequate security for the IoT infrastructure becomes ever more important.

IoT applications use sensors and actuators embedded in the environment and they collect large volumes of data on room temperatures, humidity, and

lighting to optimize energy consumption and avoid operational failures that have a real impact on the environment. In the retail industry, a refrigerator failing to maintain proper cooling temperatures could place high value medical or food inventory at risk. Having all of these devices connected, it is as well needed have the right data model. The data model has to accommodate high data rate sensor data and to assimilate and analyze the information. In this context database read/write performance is critical, particularly with high data rate sensor data. The database must support high-speed read and writes, be continuously available (100% of the time) to gather this data at uniform intervals and be scalable in order to maintain a cost-effective horizontal data store over time.

Large-scale applications and services based on the IoT are increasingly vulnerable to disruption from attack or information theft. Advances are required in several areas to make the IoT secure from those with malicious intent, including

- DoS/DDOS attacks are already well understood for the current Internet, but the IoT is also susceptible to such attacks and will require specific techniques and mechanisms to ensure that transport, energy, city infrastructures cannot be disabled or subverted.
- General attack detection and recovery/resilience to cope with IoT-specific threats, such as compromised nodes, malicious code hacking attacks.
- Cyber situation awareness tools/techniques will need to be developed to enable IoT-based infrastructures to be monitored. Advances are required to enable operators to adapt the protection of the IoT during the lifecycle of the system and assist operators to take the most appropriate protective action during attacks.
- The IoT requires a variety of access control and associated accounting schemes to support the various authorisation and usage models that are required by users. The heterogeneity and diversity of the devices/gateways that require access control will require new lightweight schemes to be developed.
- The IoT needs to handle virtually all modes of operation by itself without relying on human control. New techniques and approaches e.g. from machine learning, are required to lead to a self-managed IoT.

3.8.3 Privacy for IoT

As much of the information in an IoT system may be personal data, there is a requirement to support anonymity and restrictive handling of personal information.

There are a number of areas where advances are required:

- Cryptographic techniques that enable protected data to be stored processed and shared, without the information content being accessible to other parties. Technologies such as homomorphic and searchable encryption are potential candidates for developing such approaches.
- Techniques to support Privacy by Design concepts, including data minimisation, identification, authentication and anonymity.
- Fine-grain and self-configuring access control mechanism emulating the real world

There are a number of privacy implications arising from the ubiquity and pervasiveness of IoT devices where further research is required, including

- Preserving location privacy, where location can be inferred from things associated with people.
- Prevention of personal information inference, that individuals would wish to keep private, through the observation of IoT-related exchanges.
- Keeping information as local as possible using decentralised computing and key management.
- Use of soft Identities, where the real identity of the user can be used to generate various soft identities for specific applications. Each soft identity can be designed for a specific context or application without revealing unnecessary information, which can lead to privacy breaches.

3.9 Device Level Energy Issues

One of the essential challenges in IoT is how to interconnect "things" in an interoperable way while taking into account the energy constraints, knowing that the communication is the most energy consuming task on devices. RF solutions for a wide field of applications in the Internet of Things have been released over the last decade, led by a need for integration and low power consumption.

3.9.1 Low Power Communication

Several low power communication technologies have been proposed from different standardisation bodies. The most common ones are:

- **IEEE 802.15.4** has developed a low-cost, low-power consumption, low complexity, low to medium range communication standard at the link and the physical layers [181] for resource constrained devices.

- **Bluetooth low energy** (Bluetooth LE, [182]) is the ultra-low power version of the Bluetooth technology [183] that is up to 15 times more efficient than Bluetooth.
- **Ultra-Wide Bandwidth (UWB) Technology** [183] is an emerging technology in the IoT domain that transmits signals across a much larger frequency range than conventional systems. UWB, in addition to its communication capabilities, it can allow for high precision ranging of devices in IoT applications.
- **ISO 18000–7 DASH7** standard developed by DASH7 Alliance is a low power, low complexity, radio protocol for all sub 1GHz radio devices. It is a non-proprietary technology based on an open standard, and the solutions may contain a pool of companion technologies operating in their own ways. Common for these technologies are that they use a Sub 1 GHz silicon radio (433 MHz) as their primary communicating device [25]. The applications using DASH7 include supply chain management, inventory/yard management, manufacturing and warehouse optimization, hazardous material monitoring, smart meter and commercial green building development.
- **RFID/NFC** proposes a variety of standards to offer contactless solutions. Proximity cards can only be read from less than 10 cm and follows the ISO 14443 standard [185] and is also the basis of the NFC standard. RFID tags or vicinity tags dedicated to identification of objects have a reading distance which can reach 7 to 8 meters.

Nevertheless, front-end architectures have remained traditional and there is now a demand for innovation. Regarding the ultra-low consumption target, super-regenerative have proven to be very energetically efficient architectures used for Wake-Up receivers. It remains active permanently at very low power consumption, and can trigger a signal to wake up a complete/standard receiver [186–187]. In this field, standardization is required, as today only proprietary solutions exist, for an actual gain in the overall market to be significant.

On the other hand, power consumption reduction of an RF full-receiver can be envisioned, with a target well below 5mW to enable very small form factor and long life-time battery. Indeed, targeting below 1mW would then enable support from energy harvesting systems enabling energy autonomous RF communications. In addition to this improvement, lighter communication protocols should also be envisioned as the frequent synchronization requirement makes frequent activation of the RF link mandatory, thereby overhead in the power consumption.

It must also be considered that recent advances in the area of CMOS technology beyond 90 nm, even 65 nm nodes, leads to new paradigms in the field of RF communication. Applications which require RF connectivity are growing as fast as the Internet of Things, and it is now economically viable to propose this connectivity solution as a feature of a wider solution. It is already the case for the micro-controller which can now easily embed a ZigBee or Bluetooth RF link, and this will expand to meet other large volume applications sensors.

Progressively, portable RF architectures are making it easy to add the RF feature to existing devices. This will lead to RF heavily exploiting digital blocks and limiting analogue ones, like passive / inductor silicon consuming elements, as these are rarely easy to port from one technology to another. Nevertheless, the same performance will be required so receiver architectures will have to efficiently digitalize the signal in the receiver or transmitter chain [188]. In this direction, Band-Pass Sampling solutions are promising as the signal is quantized at a much lower frequency than the Nyquist one, related to deep under-sampling ratio [189]. Consumption is therefore greatly reduced compared to more traditional early-stage sampling processes, where the sampling frequency is much lower.

Continuous-Time quantization has also been regarded as a solution for high-integration and easy portability. It is an early-stage quantization as well, but without sampling [190]. Therefore, there is no added consumption due to the clock, only a signal level which is considered. These two solutions are clear evolutions to pave the way to further digital and portable RF solutions.

Cable-powered devices are not expected to be a viable option for IoT devices as they are difficult and costly to deploy. Battery replacements in devices are either impractical or very costly in many IoT deployment scenarios. As a consequence, for large scale and autonomous IoT, alternative energy sourcing using ambient energy should be considered.

3.9.2 Energy Harvesting

Four main ambient energy sources are present in our environment: mechanical energy, thermal energy, radiant energy and chemical energy. The power consumption varies depending on the communication protocols and data rate used to transmit the date. The approximate power consumption for different protocols is as following 3G-384kbps-2W, GPRS-24kbps-1W, WiFi-10Mbps-32–200mW, Bluetooth-1Mbps-2.5–100 mW, and Zigbee-250kbps-1mW.

Ambient light, thermal gradients, vibration/motion or electromagnetic radiation can be harvested to power electronic devices. The major components of an autonomous wireless sensor are the energy harvesting transducer, energy processing, sensor, microcontroller and the wireless radio. For successful energy harvesting implementations there are three key areas in the energy processing stage that must be addressed: energy conversion, energy storage, and power management.

Harvesting 100 μW during 1 year corresponds to a total amount of energy equivalent to 1 g of lithium. Considering this approach of looking at energy consumption for one measurement instead of average power consumption, it results that, today:

- Sending 100 bits of data consumes about 5 μJ,
- Measuring acceleration consumes about 50 μJ,
- Making a complete measurement: measure + conversion + emission consume 250–500 μJ.

Therefore, with 100 μW harvested continuously, it is possible to perform a complete measurement every 1–10 seconds. This duty cycle can be sufficient for many applications. For other applications, basic functions' power consumptions are expected to be reduced by 10 to 100 within 10 years; which will enable continuous running mode of EH-powered IoT devices.

Even though many developments have been performed over the last 10 years, energy harvesting – except PV cells – is still an emerging technology that has not yet been adopted by industry. Nevertheless, further improvements of present technologies should enable the needs of IoT to be met.

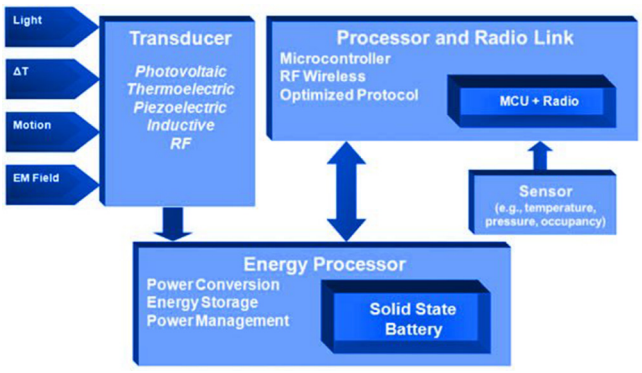

Figure 3.46 Energy harvesting - components of an autonomous wireless sensor (Source: Cymbet)

An example of interoperable wireless standard that enables switches, gateways and sensors from different manufacturers to combine seamlessly and wireless communicates with all major wired bus systems such as KNX, LON, BACnet or TCP/IP is presented in [120].

The development of energy harvesting and storage devices is instrumental to the realization of the ubiquitous connectivity that the IoT proclaims and the potential market for portable energy storage and energy harvesting could be in distributed smart swarms of mobile systems for the Internet of Things.

The energy harvesting wireless sensor solution is able to generate a signal from an extremely small amount of energy. From just 50 μWs a standard energy harvesting wireless module can easily transmit a signal 300 meters (in a free field).

3.9.3 Future Trends and Recommendations

In the future, the number and types of IoT devices will increase, therefore interoperability between devices will be essential. More computation and yet less power and lower cost requirements will have to be met. Technology integration will be an enabler along with the development of even lower power technology and improvement of battery efficiency. The power consumption of computers over the last 60 years was analysed in [192] and the authors concluded that electrical efficiency of computation has doubled roughly every year and a half. A similar trend can be expected for embedded computing using similar technology over the next 10 years. This would lead to a reduction by an order of 100 in power consumption at same level of computation. Allowing for a 10 fold increase in IoT computation, power consumption should still be reduced by an order of 10.

On the other hand, energy harvesting techniques have been explored to respond to the energy consumption requirements of the IoT domain. For vibration energy harvesters, we expect them to have higher power densities in the future (from 10 μW/g to 30 μW/g) and to work on a wider frequency bandwidth. Actually, the goal of vibration energy harvesters' researchers is to develop Plug and Play (PnP) devices, able to work in any vibrating environment, within 10 years. In the same time, we expect basic functions' energy consumption to decrease by at least a factor of 10. All these progresses will allow vibration energy harvesters to attract new markets, from industry to healthcare or defence.

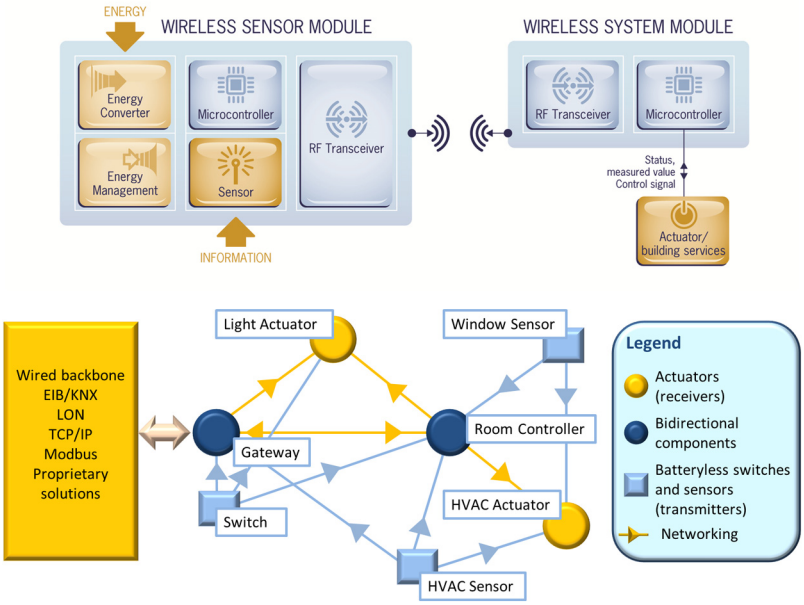

Figure 3.47 Energy harvesting wireless sensor network (Source: EnOcean)

The main challenge for thermoelectric solutions is to increase thermoelectric materials' intrinsic efficiency, in order to convert a higher part of the few mW of thermal energy available. This efficiency improvement will be mainly performed by using micro and nanotechnologies (such as superlattices or quantum dots).

For solar energy harvesting, photovoltaic cells are probably the most advanced and robust solution. They are already used in many applications and for most of them, today's solutions are sufficient. Yet, for IoT devices, it could be interesting to improve the photovoltaic cells efficiency to decrease photovoltaic cells' sizes and to harvest energy in even darker places.

In the future batteries will recharge from radio signals, cell phones will recharge from Wi-Fi. Smaller Cells (micro, pico, femto) will result in more cell sites with less distance apart but they will be greener, provide power/cost savings and at the same time, higher throughput. Connected homes will enable consumers to manage their energy, media, security and appliances; will be part of the IoT applications in the future.

3.10 IoT Related Standardization

The IERC previous SRAs [68] [85] addresses the topic of standardization and is focused on the actual needs of producing specific standards. This chapter examines further standardization considerations.

3.10.1 The Role of Standardization Activities

Standards are needed for interoperability both within and between domains. Within a domain, standards can provide cost efficient realizations of solutions, and a domain here can mean even a specific organization or enterprise realizing an IoT. Between domains, the interoperability ensures cooperation between the engaged domains, and is more oriented towards a proper "Internet of Things". 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. For IoT, this is of particular importance.

A 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 policy making 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.

A typical example is the standardization of vehicle emergency call services called eCall driven from the EC [193]. Based on the objective of increased road safety, directives were established that led to the standardization of solutions for services and communication by e.g. ETSI, and subsequently 3GPP. Another example is the Smart Grid standardization mandate M/490 [194] from the EC towards the European Standards Organisations (ESOs), and primarily ETSI, CEN and CENELEC.

The standardization bodies are addressing the issue of interoperable protocol stacks and open standards for the IoT. This includes as well expending the HTTP, TCP, IP stack to the IoT-specific protocol stack. This is quite challenging considering the different wireless protocols like ZigBee, RFID, Bluetooth, BACnet 802.15.4e, 6LoWPAN, RPL, CoAP , AMQP and MQTT.

HTTP relies on the Transmission Control Protocol (TCP). TCP's flow control mechanism is not appropriate for LLNs and its overhead is considered too high for short-lived transactions. In addition, TCP does not have multicast support and is rather sensitive to mobility. CoAP is built on top of the User Datagram Protocol (UDP) and therefore has significantly lower overhead and multicast support [103].

The conclusion is that 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 and organizations such as the Global Certification Forum [195] which is a joint partnership between mobile network operators, mobile handset manufacturers and test equipment manufacturers. Current corresponding M2M efforts are very domain specific and fragmented. The emerging IoT and M2M dependant industries should also benefit from ensuring interoperability of devices via activities such as conformance testing and certification on a broader scale.

To achieve this very important objective of a "certification" or validation programme, we also need non ambiguous test specifications which are also standards. This represents a critical step and an economic issue as this activity is resource consuming. As for any complex technology, implementation of test specifications into cost-effective test tools should also to be considered. A good example is the complete approach of ETSI using a methodology (e.g. based on TTCN-3) considering all the needs for successful certification programmes.

The conclusion therefore is that just as the applied sector can benefit from standards supporting their particular regulated or mandated needs, equally, these sectors can benefit from conforming and certified solutions, protocols and devices. This is certain to help the IoT- supporting industrial players to succeed.

It is worth noting that setting standards for the purpose of interoperability is not only driven by proper SDOs, but for many industries and applied sectors it can also be driven by Special Interest Groups, Alliances and the Open Source communities. It is of equal importance from an IoT perspective to consider these different organizations when addressing the issue of standardization.

From the point of view of 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 development of interoperable global standards. In this context the IERC position is very clear. Global standards are needed to achieve economy of scale and interworking. Wireless sensor networks, RFID, M2M are evolving to intelligent devices which need networking capabilities for a large number of applications and these technologies are "edge" drivers towards the "Internet of Things", while the network identifiable devices will have an impact on telecommunications networks. IERC is 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.

To achieve these goals it is necessary to overview the international IoT standardization items and associated roadmap; to propose a harmonized European IoT standardisation roadmap; work to provide a global harmonization of IoT standardization activities; and develop a basic framework of standards (e.g., concept, terms, definition, relation with similar technologies).

3.10.2 Current Situation

The current M2M related standards and technologies landscape is highly fragmented. The fragmentation can be seen across different applied domains where there is very little or no re-use of technologies beyond basic communications or networking standards. Even within a particular applied sector, a number of competing standards and technologies are used and promoted. The entire ecosystem of solution providers and users would greatly benefit from less fragmentation and should strive towards the use of a common set of basic tools. This would provide faster time to market, economy of scale and reduce overall costs.

Another view is standards targeting protocols vs. systems. Much emphasis has been put on communications and protocol standards, but very little effort has previously been invested in standardizing system functions or system architectures that support IoT. Localized system standards are plentiful for specific deployments in various domains. One such example is in building automation and control with (competing) standards like BACnet and KNX. However, system standards on the larger deployment and global scale are not in place. The on going work in ETSI M2M TC is one such approach, but is currently limited to providing basic application enablement on top of different networks. It should also be noted that ETSI represent one industry – the telecommunications industry. The IoT stakeholders are

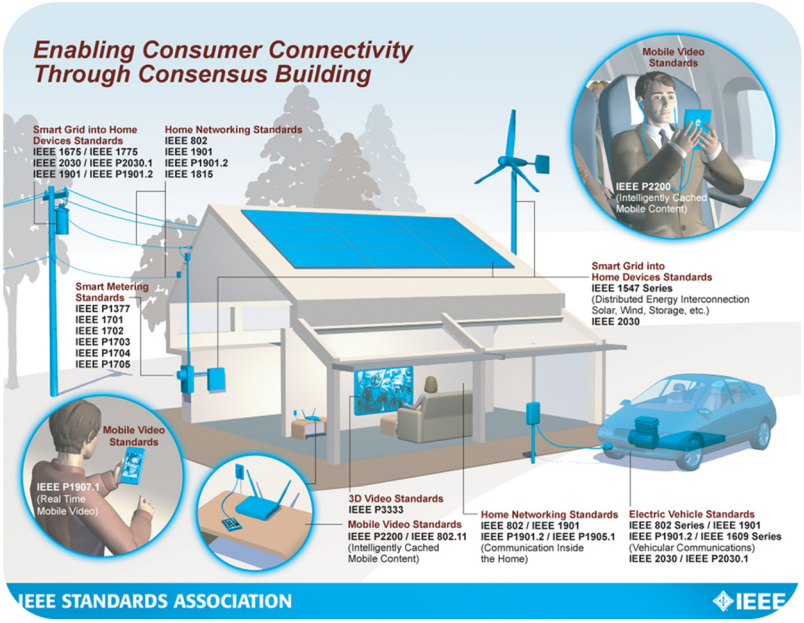

Figure 3.48 Enabling Consumer Connectivity Through Consensus Building (Source: IEEE-SA)

represented by a number of different industries and sectors reaching far beyond telecommunications.

IEEE-SA is also collaborating with other Standards Development Organizations to create a more efficient and collaborative standards-development environment.

Developing smart grids around the world will produce benefits - from the ability to respond to demand with more or less generation, to identifying waste and reducing costs. But it's connecting to what's in the home that will produce the greatest efficiencies, because the homes/buildings are where the grid connects to the user. By bringing the user online, the smart grid can manage demand, eliminate waste, lower peak loads, and stimulate investment in more energy efficient appliances. Utilities, manufacturers and suppliers are using IEEE standards to make the Smart Grid work with their products and the customers' homes/buildings. The standards addressing this area are as following [67]:

- Smart Grid Interoperability — IEEE 2030^{TM}
- Smart Metering — IEEE P1377^{TM}, IEEE 1701^{TM}, IEEE 1702^{TM}, IEEE P1703^{TM}, IEEE P1704^{TM}, IEEE P1705^{TM}

- Utility Network Protocol — IEEE 1815™
- Interconnecting Distributed Resources with Electrical Power Systems - IEEE 1547™ series
- Communication over Power Lines — IEEE 1901™, IEEE P1901.2™
- Local and Metropolitan Area Networks — IEEE 802§series

The electric vehicle will interface with the homes/buildings and the electrical grid is being shaped by the feedback of owners and manufacturers today. The standards addressing this area are as following [67]:

- Smart Grid Interoperability – IEEE 2030™, IEEE P2030.1™
- Communication over Power Lines – IEEE 1901™, IEEE P1901.2™
- Local and Metropolitan Area Networks – IEEE 802§series
- Interconnecting Distributed Resources with Electrical Power Systems - IEEE 1547™ series
- Smart Metering/Utility Network Protocol – IEEE 1701™, IEEE 1702™, IEEE P1703™, IEEE P1704™, IEEE P1705™, IEEE P1377™, IEEE 1815™

The IoT will bring home/building networking for connecting devices and humans to communicate. This will empower the devices themselves and allow them to interact. In order to make home/building-wide systems with components from many manufacturers work requires connectivity standards and an assurance of interoperability. The standards addressing this area are as following [67]:

- Convergent Digital Home Network – IEEE P1905.1™
- Power Lines Communications – IEEE 1901™, IEEE P1901.2™, IEEE 1675™, IEEE 1775™
- Low-Frequency and Wireless Protocol – IEEE 1902.1™
- Local and Metropolitan Area Networks – IEEE 802®series
- Utility Network Protocol – IEEE 1815™

3.10.3 Areas for Additional Consideration

The technology fragmentation mentioned above is particularly evident on the IoT device side. To drive further standardization of device technologies in the direction of standard Internet protocols and Web technologies, and towards the application level, would mitigate the impacts of fragmentation and strive towards true interoperability. Embedded web services, as driven by the IETF and IPSO Alliance, will ensure a seamless integration of IoT devices with the

Internet. It will also need to include semantic representation of IoT device hosted services and capabilities.

The service layer infrastructure will require standardization of necessary capabilities like interfaces to information and sensor data repositories, discovery and directory services and other mechanisms that have already been identified in projects like SENSEI [195], IoT-A [196], and IoT6. Current efforts in ETSI M2M TC do not address these aspects.

The IoT will require federated environments where producers and consumers of services and information can collaborate across both administrative and application domains. This will require standardized interfaces on discovery capabilities as well as the appropriate semantic annotation to ensure that information becomes interoperable across sectors. Furthermore, mechanisms for authentication and authorization as well as provenance of information, ownership and "market mechanisms" for information become particularly important in a federated environment. Appropriate SLAs will be required for standardization. F-ONS [199] is one example activity in the direction of federation by GS1. Similar approaches will be needed in general for IoT including standardized cross-domain interfaces of sensor based services.

A number of IoT applications will be coming from the public sector. The Directive on Public Sector Information [201] requires open access to data. Integration of data coming from various application domains is not an easy task as data and information does not adhere to any standardized formats including their semantics. Even within a single domain, data and information is not easily integrated or shared. Consideration of IoT data and information integration and sharing within domains as well as between domains need, also be considered at the international level.

Instrumental in a number of IoT applications is the spatial dimension. Standardization efforts that provide necessary harmonization and interoperability with spatial information services like INSPIRE [202] will be the key.

IoT with its envisioned billions of devices producing information of very different characteristics will place additional requirements on the underlying communications and networking strata. Efforts are needed to ensure that the networks can accommodate not only the number of devices but also the very different traffic requirements including delay tolerance, latency and reliability. This is of particular importance for wireless access networks which traditionally have been optimized based on a different set of characteristics. 3GPP, as an example, has acknowledged this and has started to address the

short term needs, but the long term needs still require identification and standardization.

3.10.4 Interoperability in the Internet-of-Things

The Internet of Things (IoT) is shaping the evolution of the future Internet. After connecting people anytime and everywhere, the next step is to interconnect heterogeneous things / machines / smart objects both between themselves and with the Internet; allowing by thy way, the creation of value-added open and interoperable services/applications, enabled by their interconnection, in such a way that they can be integrated with current and new business and development processes.

As for the IoT, future networks will continue to be heterogeneous, multi-vendors, multi-services and largely distributed. Consequently, the risk of non-interoperability will increase. This may lead to unavailability of some services for end-users that can have catastrophic consequences regarding applications related for instance to emergency or health, etc. Or, it could also mean that users/applications are likely to loose key information out of the IoT due to this lack of interoperability. Thus, it is vital to guarantee that network components will interoperate to unleash the full value of the Internet of Things.

3.10.4.1 IoT Interoperability necessary framework

Interoperability is a key challenge in the realms of the Internet of Things (IoT)! This is due to the intrinsic fabric of the IoT as: (i) high–dimensional, with the co-existence of many systems (devices, sensors, equipment, etc.) in the environment that need to communicate and exchange information; (ii) highly-heterogeneous, where these vast systems are conceived by a lot of manufacturers and are designed for much different purposes and targeting diverse application domains, making it extremely difficult (if not impossible) to reach out for global agreements and widely accepted specification; (iii) dynamic and non-linear, where new Things (that were not even considered at start) are entering (and leaving) the environment all the time and that support new unforeseen formats and protocols but that need to communicate and share data in the IoT; and (iv) hard to describe/model due to existence of many data formats, described in much different languages, that can share (or not) the same modelling principles, and that can be interrelated in many ways with one another. **This qualifies interoperability in the IoT as a problem of complex nature!**

Also, the Internet of Things can be seen as both the first and the final frontier of interoperability. First, as it is the initial mile of a sensing system and where interoperability would enable Things to talk and collaborate altogether for an higher purpose; and final, as it is possibly the place where interoperability is more difficult to tackle due to the unavoidable complexities of the IoT. We therefore need some novel approaches and comprehensions of Interoperability for the Internet of Things also making sure that it endures, that it is sustainable. **It is then needed sustainable interoperability in the Internet of Things!**

This means that we need to cope at the same time with the complex nature and sustainability requirement of interoperability in the Internet of Things. For this, it is needed a framework for sustainable interoperability that especially targets the Internet of Things taking on its specifics and constraints. This framework can (and should) learn from the best-of-breed interoperability solutions from related domains (e.g. enterprise interoperability), to take the good approaches and principles of these while understanding the differences and particulars that the Internet of Things poses. The **framework for sustainable interoperability in Internet of Things applications** needs (at least) to address the following aspects:

- Management of Interoperability in the IoT: In order to correctly support interoperability in the Internet of Things one needs to efficiently and effectively manage interoperability resources. **What then needs to be managed, to what extent and how, in respect to interoperability in the Internet of Things?**
- Dynamic Interoperability Technologies for the IoT: In order for interoperability to endure in the complex IoT environment, one needs to permit Things to enter and dynamically interoperate without the need of being remanufactured. Then, what approaches and methods to create dynamic interoperability in IoT?
- Measurement of Interoperability in the IoT: In order to properly manage and execute interoperability in the IoT it is needs to quantify and/or qualify interoperability itself. As Lord Kelvin stated: "If one can not measure it, one can not improve it". Then, **what methods and techniques to provide an adequate measurement of Interoperability in the Internet of Things?**
- Interaction and integration of IoT in the global Internet: IPv6 integration, global interoperability, IoT-Cloud integration, etc. In other words, how to bridge billion of smart things globally, while respecting their specific constraints.

3.10.4.2 Technical IoT Interoperability

There are different areas on interoperability such as at least four areas on technical interoperability, syntactic, semantic interoperability and organizational interoperability. **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 and we need to pay a specific attention as many protocols are developed within SDOs and therefore it will require market proof approach to validate and implement these protocols leading to have true interoperable and global IoT products.

Validation

Validation is an important aspect of interoperability (also in the Internet of Things). Testing and Validation provide the assurance that interoperability methods, protocols, etc. can cope with the specific nature and requirements of the Internet of Things.

The main way, among others, is to provide **efficient and accurate test suites and associated interoperability testing methodology** (with associated test description/coding languages) that help in testing thoroughly both the underlying protocols used by interconnected things / machines / smart objects and the embedded services / applications. The testing features and facilities need to become build into the design and deployment process, as the conditions of communication means, object/things availability and accessibility may change over time or location.

It is really important that these new testing methods consider the real context of future communicating systems where these objects will be deployed. Indeed, contrary to most of the existing testing methods, interconnected things / machines / smart objects in the IoT are naturally distributed. As they are distributed, the usual and classical approach of a single centralized testing system dealing with all these components and the test execution is no more applicable. The distributed nature of the tested components imposes to move towards distributed testing methods. To be more confident in the real interoperability of these components when they will be deployed in real networks, testing has to be done in a (close to) real operational environment. In this context of IoT where objects are connected through radio links, communicating environment may be unreliable and non-controllable if don't address seriously interoperability testing challenges with the same intensity

and complexity of the IoT research itself. **Research in IoT challenges leads to IoT validation and interoperability challenges**.

3.11 IoT Protocols Convergence

In order to use the full potential of IoT paradigm the interconnected devices need to communicate using lightweight protocols that don't require extensive use of CPU resources. C, Java, MQTT, Python and some scripting languages are the preferable choices used by IoT applications. The IoT nodes use separate IoT gateways if there is needed protocol conversion, database storage, or decision making in order to supplement the low-intelligence node.

One of the most important aspects for a convergence protocol that support information exchange between domains, is the ability to convey the information (data) contained in a particular domain to other domains. This section provides an overview of the existing data exchange protocols that can be applied for data exchange among various domains.

Today there are two dominant architectures for data exchange protocols; bus-based, and broker-based. In the broker-based architecture, the broker

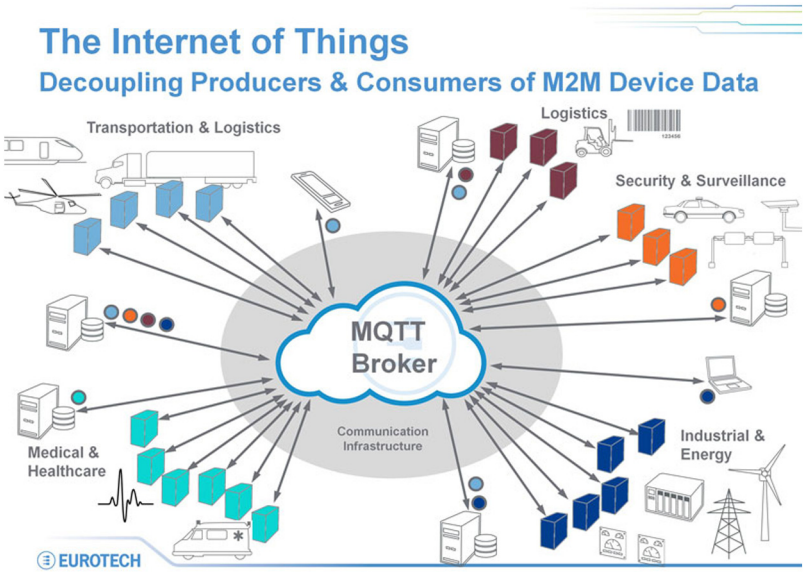

Figure 3.49 Message Queuing Telemetry Transport publish/subscribe protocol used to implement IoT and M2M applications (Source: Eurotech)

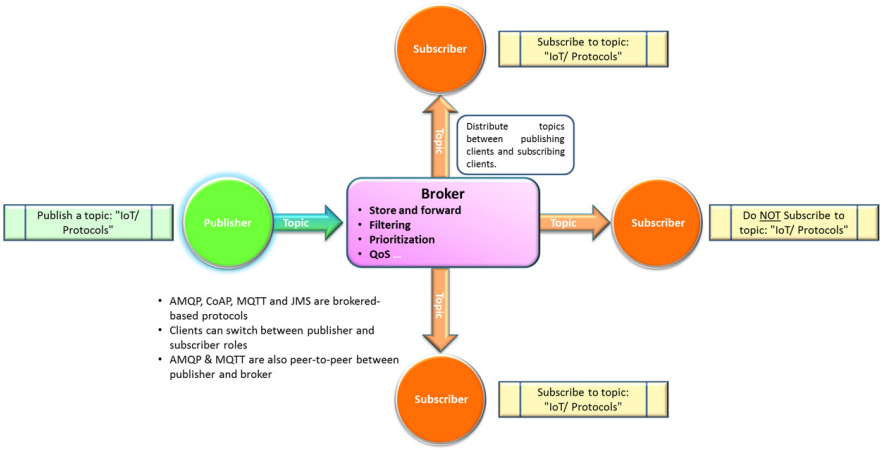

Figure 3.50 Broker based architecture for data exchange protocols

controls the distribution of the information. For example, it stores, forwards, filters and prioritizes publish requests from the publisher (the source of the information) client to the subscriber (the consumer of the information) clients. Clients switch between publisher and subscriber roles depending on their objectives. Examples of broker –based protocols include Advanced Message Queuing Protocol (AMPQ), Constrained Applications Protocol (CoAP), Message Queue Telemetry Transport (MQTT) and Java Message Service API (JMS).

In the bus-based architecture, clients publish messages for a specific topic which are directly delivered to the subscribers of that topic. There is no centralized broker or broker-based services. Examples of bus-based protocols include Data Distribution Service (DDS), Representational State Transfer (REST) and Extensible Messaging and Presence Protocol (XMPP).

Another important way to classify these protocols is whether they are message-centric or data-centric. Message centric protocols such as AMQP, MQTT, JMS and REST focus on the delivery of the message to the intended recipient(s), regardless of the data payload it contains. A data-centric protocol such as DDS, CoAP and XMPP focus on delivering the data and assumes the data is understood by the receiver. Middleware understands the data and ensures that the subscribers have a synchronized and consistent view of the data.

Yet another fundamental aspect of these protocols is whether it is web-based like CoAP or application-based such as with XMPP, and AMQP. These

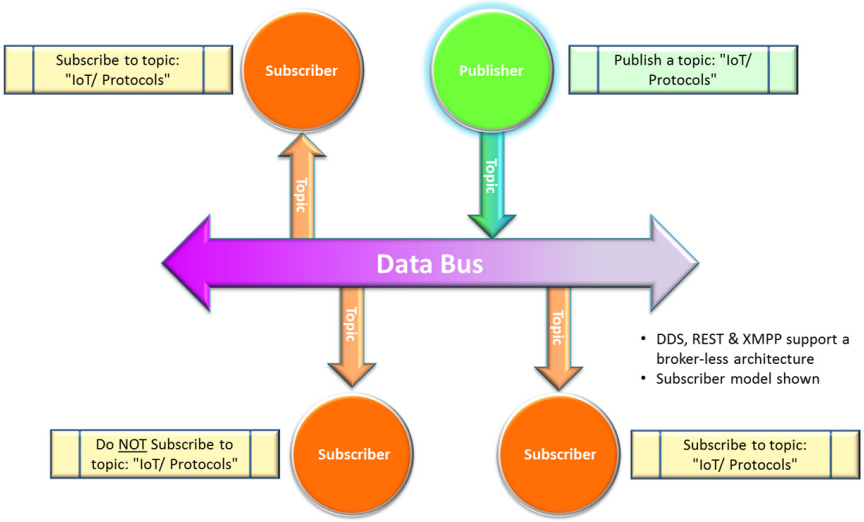

Figure 3.51 Bus-based architecture for data exchange protocols

aspects have fundamental effect on the environment, performance and tools available for implementers.

The following sections describe the example protocols in more detail, [31–33].

3.11.1 Message Queue Telemetry Transport (MQTT)

MQTT is an open-sourced protocol for passing messages between multiple clients through a central broker. It was designed to be simple and easy to implement. The MQTT architecture is broker-based, and uses long-lived outgoing TCP connection to the broker. MQTT also supports hierarchical topics (e.g., "subject/sub-subject/sub-sub-subject") file system structure.

MQTT can be used for two-way communications over unreliable networks where cost per transmitted bit is comparatively high. It is also compatible with low power consumption devices. The protocol is light-weight (simple) and therefore well suited for constrained environments. MQTT has a mechanism for asynchronous communication and for communicating disconnect messages when a device has disconnected. The most recent message can also be stored and forwarded. Multiple versions of MQTT are available to address specific limitations.

With MQTT, only partial interoperability between publishers and subscribers can be guaranteed because the meaning of data is not negotiated. Clients must know message format up-front. In addition, it does not support labeling messages with types or metadata. MQTT may include large topic strings that may not be suitable for small packet size of some transport protocols such as IEEE 802.15.4 without using MQTT-SN. MQTT may require EXI (Efficient XML Interchange) to compress the message length that could reduce communication efficiency.

TCP may negatively affect the network efficiency as the number of nodes (connection to the broker) increases. If the number of nodes is greater than a thousand, poor performance and complexity may also result because automatic/dynamic discovery is not supported in MQTT.

Because the protocol was designed to be simple, users must decide whether it is too simple and susceptible to potential hacking.

3.11.2 Constrained Applications Protocol (CoAP)

CoAP is an internet-based client/server model document transfer protocol similar to HTTP but designed for constrained devices. A sensor is typically a "server" of information and the "client" the consumer who can also alter states. It supports a one-to-one protocol for transferring state information between client and server.

CoAP utilizes User Datagram Protocol (UDP), and supports broadcast and multicast addressing. It does not support TCP. CoAP communication is through connectionless datagrams, and can be used on top of SMS and other packet-based communications protocols.

CoAP supports content negotiation and discovery, allowing devices to probe each other to find ways to exchange data. CoAP was designed for interoperability with the web (including HTTP and RESTful protocols), and supports asynchronous communications. The small packets are easy to generate. CoAP supports "observing" resource state changes as they occur so it is best suited to a state-transfer model, not purely an event-based model. CoAP supports a means for resource discovery.

UDP may be easier to implement in microcontrollers than TCP, but the security tools used for TCP (SSL/TLS) are not available in UDP. Datagram Transport Layer Security (DTLS) can be used instead. In addition, system issues such as the amount of support required for HTTP, Tunneling and Port Forwarding in NAT environments needs to be evaluated.

3.11.3 Advanced Message Queuing Protocol (AMQP)

AMQP is an application layer message-centric brokered protocol that emerged from the financial sector with the objective of replacing proprietary and non-interoperable messaging systems. The key features of AMQP are message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security. Discovery is done via the broker.

It provides flow controlled, message-oriented communication with message-delivery guarantees such as at-most-once (where each message is delivered once or never), at-least-once (where each message is certain to be delivered, but may do so multiple times) and exactly-once (where the message will always certainly arrive and do so only once), and authentication and/or encryption based on SASL and/or TLS. It assumes an underlying reliable transport layer protocol such as Transmission Control Protocol (TCP) using SSL/TLS, [30].

AMQP mandates the behavior of the messaging provider and client to the extent that implementations from different vendors are truly interoperable. Previous attempts to standardize middleware have happened at the API level (e.g. JMS) and thus did not ensure interoperability. Unlike JMS, which merely defines an API, AMQP is a wire-protocol. Consequently any product that can create and interpret messages that conform to this data format can interoperate with any other compliant implementation irrespective of the programming language, [30].

Support for more than a thousand nodes may result in poor performance and increased complexity.

3.11.4 Java Message Service API (JMS)

JMS is a message oriented middleware API for creating, reading, sending, receiving messages between two or more clients, based on the Java Enterprise Edition. It was meant to separate application and transport layer functions and allows the communications between different components of a distributed application to be loosely coupled, reliable and asynchronous over TCP/IP.

JMS supports both the point to point and publish/subscribe models using message queuing, and durable subscriptions (i.e., store and forward topics to subscribers when they "log in"). Subscription control is through topics and queues with message filtering. Discovery is via the broker (server). The same Java classes can be used to communicate with different JMS providers by using the Java Naming and Directory interface for the desired provider.

When considering JMS API, keep in mind that it cannot guarantee interoperability between producers and consumers using different JMS implementations. Also, systems with more than a thousand nodes may result in poor performance and increased complexity.

3.11.5 Data Distribution Service (DDS)

DDS is a data-centric middleware language used to enable scalable, real-time, dependable high performance and interoperable data exchanges. The original target applications were financial trading, air traffic control, smart grid management and other big data, mission critical applications.

It is a decentralized broker-less protocol with direct peer-to-peer communications between publishers and subscribers and was designed to be language and operating system independent. DDS sends and receives data, events, and command information on top of UDP but can also run over other transports such as IP Multicast, TCP/IP, shared memory etc. DDS supports real-time many-to-many managed connectivity and also supports automatic discovery.

Applications using DDS for communications are decoupled and do not require intervention from the user applications, which can simplify complex network programming. QoS parameters that are used to configure its auto-discovery mechanisms are setup one time. DSS automatically handles hot-swapping redundant publishers if the primary publisher fails. Subscription control is via partitions and topics with message filtering.

DDS Security specification is still pending. Implementers should be aware that DSS needs DSSI ("wire-protocol") to make sure all implementations can interoperate.

DSS is available commercially and a version of it has been made "open" in as much as a "public" version is available.

3.11.6 Representational State Transfer (REST)

REST is a language and operating system independent architecture for designing network applications using simple HTTP to connect between machines. It was designed as a lightweight point-to-point, stateless client/server, cacheable protocol for simple client/server (request/reply) communications from devices to the cloud over TCP/IP.

Use of stateless model supported by HTTP and can simplify server design and can easily be used in the presence of firewalls, but may result in the need for

additional information exchange. It does not support Cookies or asynchronous, loosely coupled publish-and-subscribe message exchanges.

Support for systems with more than a thousand nodes may result in poor performance and complexity.

3.11.7 Extensible Messaging and Presence Protocol (XMPP)

XMPP is a communications protocol for message oriented middleware based on XML (formally "Jabber"). It is a brokerless decentralized client-server (as previously defined) model and is used by text messaging applications. It is near real-time and massively scalable to hundreds of thousands of nodes. Binary data must be base64 encoded before it can be transmitted in-band.

It is useful for devices with large and potentially complicated traffic, and where extra security is required. For example, it can be used to isolate security to between applications rather than to rely on TCP or the web. The users or devices (servers) can keep control through preference settings.

New extensions being added to enhance its application to the IoT, including Service Discovery (XEP-0030), Concentrators for connecting legacy sensors and devices (XEP-0325), SensorData (XEP-0323), and Control (XEP-0322) and the Transport of XMPP over HTTM (XP-0124).

3.12 Discussion

The Internet of Things will grow to 26 billion units (without considering PCs, tablets and smartphones) installed in 2020 representing an almost 30-fold increase from 0.9 billion in 2009. IoT product and service suppliers will generate incremental revenue exceeding $300 billion, mostly in services, in 2020. It will result in $1.9 trillion in global economic value-add through sales into diverse end markets. Due to the low cost of adding IoT capability to consumer products, it is expected that "ghost" devices with unused connectivity will be common. This will be a combination of products that have the capability built in but require software to "activate" it and products with IoT functionality that customers do not actively leverage. In addition, enterprises will make extensive use of IoT technology, and there will be a wide range of products sold into various markets, such as advanced medical devices; factory automation sensors and applications in industrial robotics; sensor motes for increased agricultural yield; and automotive sensors and infrastructure integrity monitoring systems for diverse areas, such as road and railway transportation, water distribution and electrical transmission.

By 2020, component costs will have come down to the point that connectivity will become a standard feature, even for processors costing less than $1. This opens up the possibility of connecting just about anything, from the very simple to the very complex, to offer remote control, monitoring and sensing and it is expected that the variety of devices offered to explode [77].

The IoT encompasses sensor, actuators, electronic processing, microcontrollers, embedded software, communications services and information services associated with the things.

The economic value added at the European and global level is significant across sectors in 2020. The IoT applications are still implemented by the different industrial verticals with a high adoption in manufacturing, healthcare and home/buildings.

IoT will also facilitate new business models based on the real-time data acquired by billions of sensor nodes. This will push for development of advances sensor, nanoelectronics, computing, network and cloud technologies and will lead to value creation in utilities, energy, smart building technology, transportation and agriculture.

Acknowledgments

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

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

The IoT European Research Cluster SRA is part of a continuous IoT community dialogue supported by the European Commission (EC) DG Connect – Communications Networks, Content and Technology, E1 - Network technologies Unit for the European and international IoT stakeholders. The result is a lively document that is updated every year with expert feedback from on-going and future projects financed by the EC. Many colleagues have assisted over the last few years with their views on the Internet of Things Strategic Research and Innovation agenda document. Their contributions are gratefully acknowledged.

Table 3.1 Future Technological Developments

Development	2015–2020	Beyond 2020
Identification Technology	• Identity management • Open framework for the IoT • Soft Identities • Semantics • Privacy awareness	"Thing/Object DNA" identifier
Internet of Things Architecture Technology	Network of networks architectures • IoT architecture developments • Adaptive, context based architectures • Self-* properties	Cognitive architectures • Experimental architectures
Internet of Things Infrastructure	Cross domain application deployment • Integrated IoT infrastructures • Multi application infrastructures • Multi provider infrastructures	Global, general purpose IoT infrastructures • Global discovery mechanism
Internet of Things Applications	Configurable IoT devices • IoT in food/water production and tracing • IoT in manufacturing industry • IoT in industrial lifelong service and maintenance • IoT device with strong processing and analytics capabilities • Application capable of handling heterogeneous high capability data collection an d processing infrastructures	IoT information open market
Communication Technology	Wide spectrum and spectrum aware protocols • Ultra low power chip sets • On chip antennas • Millimeter wave single chips • Ultra low power single chip radios • Ultra low power system on chip	Unified protocol over wide spectrum • Multi-functional reconfigurable chips
Network Technology	Network context awareness • Self aware and self organizing networks • Sensor network location transparency • IPv6- enabled scalability	Network cognition • Self-learning, self-repairing networks • Ubiquitous IPv6-based IoT deployment

(*Continued*)

Table 3.1 Continued

Development	2015–2020	Beyond 2020
Software and algorithms	Goal oriented software • Distributed intelligence, problem solving • Things-to-Things collaboration environments • IoT complex data analysis • IoT intelligent data visualization • Hybrid IoT and industrial automation systems	User oriented software • The invisible IoT • Easy-to-deploy IoT sw • Things-to-Humans collaboration • IoT 4 All • User-centric IoT
Hardware	Smart sensors (bio-chemical) • More sensors and actuators (tiny sensors) • Sensor integration with NFC • Home printable RFID tags	Nano-technology and new materials
Data and Signal Processing Technology	Context aware data processing and data responses • Energy, frequency spectrum aware data processing	Cognitive processing and optimisation
Discovery and Search Engine Technologies	Automatic route tagging and identification management centres • Semantic discovery of sensors and sensor data	Cognitive search engines • Autonomous search engines
Power and Energy Storage Technologies	Energy harvesting (biological, chemical, induction) • Power generation in harsh environments • Energy recycling • Long range wireless power • Wireless power	Biodegradable batteries • Nano-power processing unit
Security, Privacy & Trust Technologies	User centric context-aware privacy and privacy policies • Privacy aware data processing • Security and privacy profiles selection based on security and privacy needs • Privacy needs automatic evaluation • Context centric security • Homomorphic Encryption • Searchable Encryption • Protection mechanisms for IoT DoS/DdoS attacks	Self adaptive security mechanisms and protocols • Self-managed secure IoT

Table 3.1 (Continued)

Development	2015–2020	Beyond 2020
Material	SiC, GaN	Diamond
Technology	• Improved/new semiconductor manufacturing processes/technologies for higher temperature ranges	• Graphen
Interoperability	Optimized and market proof interoperability approaches used • Interoperability under stress as market grows • Cost of interoperability reduced • Several successful certification programmes in place	Automated self-adaptable and agile interoperability
Standardisation	IoT standardization refinement • M2M standardization as part of IoT standardisation • Standards for cross interoperability with heterogeneous networks • IoT data and information sharing	Standards for autonomic communication protocols

Table 3.2 Internet of Things Research Needs

Research needs	2015–2020	Beyond 2020
Identification Technology	Convergence of IP and IDs and addressing scheme • Unique ID • Multiple IDs for specific cases • Extend the ID concept (more than ID number) • Electro Magnetic Identification – EMID	Multi methods – one ID
IoT Architecture	Internet (Internet of Things) (global scale applications, global interoperability, many trillions of things)	
Internet of Things Infrastructure	Application domain-independent abstractions & functionality • Cross-domain integration and management • Large-scale deployment of infrastructure • Context-aware adaptation of operation	Self management and configuration

(*Continued*)

Table 3.2 (Continued)

Research needs	2015–2020	Beyond 2020
Internet of Things Applications	IoT information open market • Standardization of APIs • IoT device with strong processing and analytics capabilities • Ad-hoc deployable and configurable networks for industrial use • Mobile IoT applications for IoT industrial operation and service/maintenance • Mobile IoT applications for IoT industrial operation and service/maintenance • Fully integrated and interacting IoT applications for industrial use	Building and deployment of public IoT infrastructure with open APIs and underlying business models • Mobile applications with bio-IoT-human interaction
SOA Software Services for IoT	Quality of Information and IoT service reliability • Highly distributed IoT processes • Semi-automatic process analysis and distribution	Fully autonomous IoT devices
Internet of Things Architecture Technology	Code in tags to be executed in the tag or in trusted readers • Global applications • Adaptive coverage • Universal authentication of objects • Graceful recovery of tags following power loss • More memory • Less energy consumption • 3-D real time location/position embedded systems	Intelligent and collaborative functions • Object intelligence • Context awareness • Cooperative position cyber-physical systems
Communication Technology	Longer range (higher frequencies – tenths of GHz) • Protocols for interoperability • On chip networks and multi standard RF architectures • Multi-protocol chips • Gateway convergence	Self configuring, protocol seamless networks

	• Hybrid network technologies convergence • 5G developments • Collision-resistant algorithms • Plug and play tags • Self repairing tags	
Network Technology	Grid/Cloud network • Software defined networks • Service based network • Multi authentication • Integrated/universal authentication • Brokering of data through market mechanisms • Scalability enablers • IPv6-based networks for smart cities	Need based network • Internet of **Everything** • Robust security based on a combination of ID metrics • Autonomous systems for non stop information technology service • Global European IPv6-based Internet of Everything
Software and algorithms	Self management and control • Micro operating systems • Context aware business event generation • Interoperable ontologies of business events • Scalable autonomous software Evolving software • Self reusable software • Autonomous things: • Self configurable • Self healing • Self management • Platform for object intelligence	Self generating "molecular" software • Context aware software
Hardware Devices	Polymer based memory • Ultra low power EPROM/FRAM • Molecular sensors • Autonomous circuits • Transparent displays • Interacting tags • Collaborative tags • Heterogeneous integration • Self powering sensors • Low cost modular devices	Biodegradable antennas • Autonomous "bee" type devices

(*Continued*)

Table 3.2 (Continued)

Research needs	2015–2020	Beyond 2020
	• Ultra low power circuits • Electronic paper • Nano power processing units • Silent Tags • Biodegradable antennae	
Hardware Systems, Circuits and Architectures	Multi protocol front ends • Ultra low cost chips with security • Collision free air to air protocol • Minimum energy protocols • Multi-band, multi-mode wireless sensor architectures implementations • Adaptive architectures • Reconfigurable wireless systems • Changing and adapting functionalities to the environments • Micro readers with multi standard protocols for reading sensor and actuator data • Distributed memory and processing Low cost modular devices • Protocols correct by construction	Heterogeneous architectures • "Fluid" systems, continuously changing and adapting
Data and Signal Processing Technology	Common sensor ontologies (cross domain) • Distributed energy efficient data processing • Autonomous computing • Tera scale computing	Cognitive computing
Discovery and Search Engine Technologies	Scalable Discovery services for connecting things with services while respecting security, privacy and confidentiality • "Search Engine" for Things • IoT Browser • Multiple identities per object • On demand service discovery/integration • Universal authentication	Cognitive registries

Power and Energy Storage Technologies	Paper based batteries • Wireless power everywhere, anytime • Photovoltaic cells everywhere • Energy harvesting • Power generation for harsh environments	Biodegradable batteries
Interoperability	Dynamic and adaptable interoperability for technical and semantic areas • Open platform for IoT validation	Self-adaptable and agile interoperability approaches
Security, Privacy & Trust Technologies	Low cost, secure and high performance identification/ authentication devices • Access control and accounting schemes for IoT • General attack detection and recovery/resilience for IoT • Cyber Security Situation Awareness for IoT • Context based security activation algorithms • Service triggered security • Context-aware devices • Object intelligence Decentralised self configuring methods for trust establishment • Novel methods to assess trust in people, devices and data • Location privacy preservation • Personal information protection from inference and observation • Trust Negotiation	Cognitive security systems • Self-managed secure IoT • Decentralised approaches to privacy by information localisation
Governance (legal aspects)	Legal framework for transparency of IoT bodies and organizations	Adoption of clear European norms/standards regarding Privacy and Security for IoT

(*Continued*)

Table 3.2 (Continued)

Research needs	2015–2020	Beyond 2020
	• Privacy knowledge base and development privacy standards	
Economic	Business cases and value chains for IoT • Emergence of IoT in different industrial sectors	
Material Technology	Carbon nanotube • Conducting Polymers and semiconducting polymers and molecules • Modular manufacturing techniques	Graphen

List of Contributors

Abdur Rahim Biswas, IT, create-net, iCore
Alessandro Bassi, FR, Bassi Consulting, IoT-A
Ali Rezafard, IE, Afilias, EPCglobal Data Discovery JRG
Amine Houyou, DE, SIEMENS, IoT@Work
Antonio Skarmeta, SP, University of Murcia, IoT6
Carlos Agostinho, PT, UNINOVA
Carlo Maria Medaglia, IT, University of Rome 'Sapienza', IoT-A
César Viho, FR, Probe-IT
Claudio Pastrone, IT, ISMB, ebbits, ALMANAC
Daniel Thiemert, UK, University of Reading, HYDRA
David Simplot-Ryl, FR, INRIA/ERCIM, ASPIRE
Elias Tragos, GR, FORTH, RERUM
Eric Mercier, FR, CEA-Leti
Erik Berg, NO, Telenor, IoT-I
Francesco Sottile, IT, ISMB, BUTLER
Franck Le Gall, FR, Inno, PROBE-IT, BUTLER
François Carrez, GB, IoT-I
Frederic Thiesse, CH, University of St. Gallen, Auto-ID Lab
Friedbert Berens, LU, FB Consulting S.à r.l, BUTLER
Gary Steri, IT, EC, JRC
Gianmarco Baldini, IT, EC, JRC
Giuseppe Abreu, DE, Jacobs University Bremen, BUTLER
Ghislain Despesse, FR, CEA-Leti

Hanne Grindvoll, NO, SINTEF ICT
Harald Sundmaeker, DE, ATB GmbH, SmartAgriFood, CuteLoop
Henri Barthel, BE, GS1 Global
Igor Nai Fovino, IT, EC, JRC
Jan Höller, SE, EAB
Jens-Matthias Bohli, DE, NEC
John Soldatos, GR, Athens Information Technology, ASPIRE, OpenIoT
Jose-Antonio, Jimenez Holgado, ES, TID
Klaus Moessner, UK, UNIS, IoT.est
Kostas Kalaboukas, GR, SingularLogic, EURIDICE
Latif Ladid, LU, UL, IPv6 Forum
Levent Gürgen, FR, CEA-Leti
Luis Muñoz, ES, Universidad De Cantabria
Manfred Hauswirth, IE, DERI, OpenIoT, VITAL
Marco Carugi, IT, ITU-T, ZTE
Marilyn Arndt, FR, Orange
Mario Hoffmann, DE, Fraunhofer-Institute SIT, HYDRA
Markus Eisenhauer, DE, Fraunhofer-FIT, HYDRA, ebbits
Markus Gruber, DE, ALUD
Martin Bauer, DE, NEC, IoT-A
Martin Serrano, IE, DERI, OpenIoT
Maurizio Spirito, IT, Istituto Superiore Mario Boella, , ebbits, ALMANAC
Maarten Botterman, NL, GNKS, SMART-ACTION
Nicolaie L. Fantana, DE, ABB AG
Nikos Kefalakis, GR, Athens Information Technology, OpenIoT
Paolo Medagliani, FR, Thales Communications & Security, CALYPSO
Payam Barnaghi, UK, UNIS, IoT.est
Philippe Cousin, FR, easy global market, PROBE-IT,
Raffaele Giaffreda, IT, CNET, iCore
Ricardo Neisse, IT, EC, JRC
Richard Egan, UK, TRT
Rolf Weber, CH, UZH
Sébastien Boissseau, FR, CEA-Leti
Sébastien Ziegler, CH, Mandat International, IoT6
Sergio Gusmeroli, IT, TXT e-solutions,
Stefan Fisher, DE, UZL
Stefano Severi, DE, Jacobs University Bremen, BUTLER
Srdjan Krco, RS, DunavNET,, IoT-I, SOCIOTAL
Sönke Nommensen, DE, UZL, SmartSantander

Trevor Peirce, BE, CASAGRAS2
Veronica Gutierrez Polidura, ES, Universidad De Cantabria
Vincent Berg, FR, CEA-Leti
Vlasios Tsiatsis, SE, EAB
Wolfgang König, DE, ALUD
Wolfgang Templ, DE, ALUD

Contributing Projects and Initiatives

ASPIRE, BRIDGE, CASCADAS, CONFIDENCE, CuteLoop, DACAR, ebbits, ARTEMIS, ENIAC, EPoSS, EU-IFM, EURIDICE, GRIFS, HYDRA, IMS2020, Indisputable Key, iSURF, LEAPFROG, PEARS Feasibility, PrimeLife, RACE networkRFID, SMART, StoLPaN, SToP, TraSer, WALTER, IoT-A, IoT@Work, ELLIOT, SPRINT, NEFFICS, IoT-I, CASAGRAS2, eDiana, OpenIoT, IoT6, iCore PROBE-IT, BUTLER, IoT-est, SmartAgriFood, ALMANAC, CITYPULSE,COSMOS,CLOUT, RERUM, SMARTIE, SOCIOTAL, VITAL

List of Abbreviations and Acronyms

Acronym	**Meaning**
3GPP3GPP	3rd Generation Partnership Project
AAL	Ambient Assisted Living
ACID	Atomicity, Consistency, Isolation, Durability
ACL	Access Control List
AMR	Automatic Meter Reading Technology
API	Application Programming Interface
AWARENESS	EU FP7 coordination action Self-Awareness in Autonomic Systems
BACnet	Communications protocol for building automation and control networks
BAN	Body Area Network
BDI	Belief-Desire-Intention architecture or approach
Bluetooth	Proprietary short range open wireless technology standard
BPM	Business process modelling
BPMN	Business Process Model and Notation
BUTLER	EU FP7 research project uBiquitous, secUre inTernet of things with Location and contExt-awaReness
CAGR	Compound annual growth rate
CE	Council of Europe
CENCEN	Comité Européen de Normalisation

CENELEC	Comité Européen de Normalisation Électrotechnique
CEO	Chief executive officer
CEP	Complex Event Processing
CMOS	Complementary metal-oxide-semiconductor
CSS	Chirp Spread Spectrum
D1.3	Deliverable 1.3
DATEX-II	Standard for data exchange involving traffic centres
DCA	Data Collection and Analysis
DNS	Domain Name System
DoS/DDOS	Denial of service attack Distributed denial of service attack
EC	European Commission
eCall	eCall – eSafety Support A European Commission funded project, coordinated by ERTICO-ITS Europe
EDA	Event Driven Architecture
EH	Energy harvesting
EMF	Electromagnetic Field
ERTICO-ITS	Multi-sector, public / private partnership for intelligent transport systems and services for Europe
ESOs	European Standards Organisations
ESP	Event Stream Processing
ETSI	European Telecommunications Standards Institute
EU	European Union
Exabytes	10^{18} bytes
FI	Future Internet
FI PPP	Future Internet Public Private Partnership programme
FIA	Future Internet Assembly
FIS 2008	Future Internet Symposium 2008
F-ONS	Federated Object Naming Service
FP7	Framework Programme 7
FTP	File Transfer Protocol
GFC	Global Certification Forum
GreenTouch	Consortium of ICT research experts
GS1	Global Standards Organization
Hadoop	Project developing open-source software for reliable, scalable, distributed computing
IAB	Internet Architecture Board
IBM	International Business Machines Corporation
ICAC	International Conference on Autonomic Computing
ICANN	Internet Corporation for Assigned Name and Numbers
ICT	Information and Communication Technologies
iCore	EU research project Empowering IoT through cognitive technologies
IERC	European Research Cluster for the Internet of Things
IETF	Internet Engineering Task Force
INSPIRE	Infrastructure for Spatial Information in the European Community

IoE	Internet of EnergyInternet of Energy
IoM	Internet of MediaInternet of Media
IoP	Internet of PersonsInternet of Persons, Internet of PeopleInternet of People
IoS	Internet of ServicesInternet of Services
IoT	Internet of Things
IoT6	EU FP7 research project Universal integration of the Internet of Things through an IPv6-based service oriented architecture enabling heterogeneous components interoperability
IoT-A	Internet of Things ArchitectureInternet of Things Architecture
IoT-A	Internet of Things ArchitectureInternet of Things Architecture
IoT-est	EU ICT FP7 research project Internet of Things environment for service creation and testing
IoT-i	Internet of Things Initiative
IoV	Internet of Vehicles
IP	Internet Protocol
IPSO Alliance	Organization promoting the Internet Protocol (IP) for Smart Object communications
IPv6	Internet Protocol version 6
ISO 19136	Geographic information, Geography Mark-up Language, ISO Standard
IST	Intelligent Transportation System
KNX	Standardized, OSI-based network communications protocol for intelligent buildings
LNCS	Lecture Notes in Computer Science
LOD	Linked Open Data Cloud
LTE	Long Term Evolution
M2M	Machine to Machine
MAC	Media Access Control data communication protocol sub-layer
MAPE-K	Model for autonomic systems: Monitor, Analyse, Plan, Execute in interaction with a Knowledge base
makeSense	EU FP7 research project on Easy Programming of Integrated Wireless Sensors
MB	Megabyte
MIT	Massachusetts Institute of Technology
MPP	Massively parallel processing
NIEHS	National Institute of Environmental Health Sciences
NFC	Near Field Communication
NoSQL	not only SQL – a broad class of database management systems

OASIS	Organisation for the Advancement of Structured Information Standards
OEM	Original equipment manufacturer
OGC	Open Geospatial Consortium
OMG	Object Management Group
OpenIoT	EU FP7 research project Part of the Future Internet public private partnership Open source blueprint for large scale self-organizing cloud environments for IoT applications
Outsmart	EU project Provisioning of urban/regional smart services and business models enabled by the Future Internet
PAN	Personal Area Network
PET	Privacy Enhancing Technologies
Petabytes	10^{15} byte
PHY	Physical layer of the OSI model
PIPES	Public infrastructure for processing and exploring streams
PKI	Public key infrastructure
PPP	Public-private partnership
Probe-IT	EU ICT-FP7 research project Pursuing roadmaps and benchmarks for the Internet of Things
PSI	Public Sector Information
PV	Photo Voltaic
QoI	Quality of Information
RF	Radio frequency
RFID	Radio-frequency identification
SASO	IEEE international conferences on Self-Adaptive and Self-Organizing Systems
SDO	Standard Developing Organization
SEAMS	International Symposium on Software Engineering for Adaptive and Self-Managing Systems
SENSEI	EU FP7 research project Integrating the physical with the digital world of the network of the future
SIG	Special Interest Group
SLA	Service-level agreement / Software license agreement
SmartAgriFood	EU ICT FP7 research project Smart Food and Agribusiness: Future Internet for safe and healthy food from farm to fork
SmartSantander	EU ICT FP7 research project Future Internet research and experimentation
SOA	Service Oriented Approach
SON	Self Organising Networks
SSW	Semantic Sensor Web
SRA	Strategic Research Agenda
SRIA	Strategic Research and Innovation Agenda
SRA2010	Strategic Research Agenda 2010
SWE	Sensor Web Enablement
TC	Technical Committee

TTCN-3	Testing and Test Control Notation version 3
USDL	Unified Service Description Language
UWB	Ultra-wideband
W3C	World Wide Web Consortium
WS&AN	Wireless sensor and actuator networks
WSN	Wireless sensor network
WS-BPEL	Web Services Business Process Execution Language
Zettabytes	10^{21} byte
ZigBee	Low-cost, low-power wireless mesh network standard based on IEEE 802.15.4

References

[1] NFC Forum, online at http://nfc-forum.org
[2] METIS, Mobile and wireless communications Enablers for the Twenty-twenty (2020) Information Society, online at https://www.metis2020.com/
[3] Wemme, L., "NFC: Global Promise and Progress", NFC Forum, 22.01.2014, online at http://nfc-forum.org/wp-content/uploads/2014/01/Omnicard_Wemme_2014_website.pdf
[4] Bluetooth Special Interest Group, online at https://www.bluetooth.org/en-us/members/about-sig
[5] Bluetooth Developer Portal, online at https://developer.bluetooth.org/Pages/default.aspx
[6] Bluetooth, online at http://www.bluetooth.com
[7] ANT+, online at http://www.thisisant.com/
[8] ANT, "Message Protocol and Usage rev.5.0", online at http://www.thisisant.com/developer/resources/downloads#documents_tab
[9] ANT, "FIT2 Fitness Module Datasheet", online at http://www.thisisant.com/developer/resources/downloads#documents_tab
[10] Wi-Fi Alliance, online at http://www.wi-fi.org/
[11] Z-Wave alliance, online at http://www.z-wavealliance.org
[12] Pätz, C., "Smart lighting. How to develop Z-Wave Devices", EE Times europe LEDLighting, 04.10.2012, online at http://www.ledlighting-eetimes.com/en/how-to-develop-z-wave-devices.html?cmp_id=71&news_id=222908151
[13] KNX, online at http://www.knx.org/knx-en/knx/association
[14] European Editors, "Using Ultra-Low-Power Sub-GHz Wireless for Self-Powered Smart-Home Networks", 12.05.2013, online at

http://www.digikey.com/en-US/articles/techzone/2013/dec/using-ultra-low-power-sub-ghz-wireless-for-self-powered-smart-home-networks
[15] HART Communication Foundation, online at http://www.hartcomm.org
[16] Mouser Electronics, "Wireless Mesh Networking – Featured Wireless Mesh Networking Protocols", online at http://no.mouser.com/applications/wireless_mesh_networking_protocols/
[17] IETF, online at https://www.ietf.org
[18] Bormann, C., "6LoWPAN Roadmap and Implementation Guide", 6LoWPAN Working Group, April 2013, http://tools.ietf.org/html/draft-bormann-6lowpan-roadmap-04
[19] Shelby, Z. and Bormann, C., "6LoWPAN: The Wireless Embedded Internet", Wiley, Great Britain, ISBN 9780470747995, 2009, online at http://elektro.upi.edu/pustaka.elektro/Wireless%20Sensor%20Network/6LoWPAN.pdf
[20] WiMAX Forum, online at http://www.wimaxforum.org
[21] A. Passemard, "The Internet of Things Protocol stack – from sensors to business value", online at http://entrepreneurshiptalk.wordpress.com/2014/01/29/the-internet-of-thing-protocol-stack-from-sensors-to-business-value/
[22] EnOcean Alliance, online at http://www.enocean-alliance.org/en/profile/
[23] EnOcean Wireless Standard, online at http://www.enocean.com
[24] EnOcean Alliance, "EnOcean Equipment Profiles (EEP)", Ver. 2.6, December 2013, online at http://www.enocean.com/en/home/
[25] DASH7 Alliance, online at http://www.dash7.org
[26] Maarten Weyn, "Dash7 Alliance Protocol Technical Presentation", December 2013, online at http://www.slideshare.net/MaartenWeyn1/dash7-alliance-protocol-technical-presentation
[27] Visible Assets, Inc., "Rubee Technology", online at http://www.rubee.com/Techno/index.html
[28] Stevens, J., Weich, C., GilChrist, R., "RuBee (IEEE 1902.1) – The Physics Behind, Real-Time, High Security Wireless Asset Visibility Networks in Harsh Environments", online at http://www.rubee.com/WhiteSEC/RuBee-Security-080610.pdf
[29] RuBee Hardware, online at http://www.rubee.com/page2/Hard/index.html
[30] Foster, A., "A Comparison Between DDS, AMQP, MQTT, JMS, REST and CoAP", Version 1.4, January 2014, online at http://www.prismtech.com/sites/default/files/documents/MessagingComparsionJan2014USROW_vfinal.pdf

[31] Elkstein, M., "Learn REST: A tutorial", online at http://rest.elkstein.org
[32] Jaffey, T., "MQTT and CoAP IoT Protocols.pdf", September 2013, online at https://docs.google.com/document/d/1_kTNkl84o_yoC56dzFfkYHoHuepINP3nDNokycXINXI/edit?usp=sharing&pli=1
[33] Puzanov, O., "IoT Protocol Wars: MQTT vs COAP vs XMPP", online at http://www.iotprimer.com/2013/11/iot-protocol-wars-mqtt-vscoap-vs-xmpp.html
[34] Home Gateway Initiative (HGI), online at www.homegatewayinitiative.org
[35] Artemis IoE project, online at www.artemis-ioe.eu
[36] Larios V.M., Robledo J.G., Gómez L., and Rincon R., "IEEE-GDL CCD Smart Buildings Introduction", online at http://smartcities.ieee.org/images/files/ images/pdf/whitepaper_phi_smartbuildingsv6.pdf
[37] Analysys Mason, "Imagine an M2M world with 2.1 billion connected things", online at http://www.analysysmason.com/about-us/news/insight/M2M_forecast_Jan2011/
[38] Casaleggio Associati, "The Evolution of Internet of Things", February 2011, online at http://www.casaleggio.it/pubblicazioni/Focus_internet_of_things_v1.81%20-%20eng.pdf
[39] J. B., Kennedy, "When woman is boss, An interview with Nikola Tesla", in Colliers, January 30, 1926.
[40] M. Weiser, "The Computer for the 21st Century," *Scientific Am.*, Sept., 1991, pp. 94–104; reprinted in *IEEE Pervasive Computing*, Jan.-Mar. 2002, pp. 19–25."
[41] K. Ashton, "That 'Internet of Things' Thing", online at http://www.rfidjournal.com/article/view/4986, June 2009
[42] N. Gershenfeld, "When Things Start to Think", Holt Paperbacks, New York, 2000
[43] Raymond James & Associates, " The Internet of Things - A Study in Hype, Reality, Disruption, and Growth", online at http://sitic.org/wp-content/uploads/The-Internet-of-Things-A-Study-in-Hype-Reality-Disruption-and-Growth.pdf, January 2014.
[44] IDC, "Worldwide Internet of Things 2013–2020 Forecast: Billions of Things, Trillions of Dollars," Doc #: 243661, October 2013.
[45] N. Gershenfeld, R. Krikorian and D. Cohen, *Scientific Am.*, Sept., 2004
[46] World Economic Forum, "The Global Information Technology Report 2012 - Living in a Hyperconnected World" online at http://www3.weforum.org/docs/Global_IT_Report_2012.pdf
[47] "Key Enabling Technologies", Final Report of the HLG-KET, June 2011

[48] G. Bovet, A. Ridi and J. Hennebert, "Toward Web Enhanced Building Automation System", in Eds. N. Bessis and C. Dobre - Big Data and Internet of Things: A Roadmap for Smart Environments, ISBN: 978–3-319–05028-7, Studies in Computational Intelligence, Volume 546, 2014 pp. 259–283, online at http://hal.archives-ouvertes.fr/docs/00/97/35/10/PDF/BuildingsWoT.pdf

[49] International Technology Roadmap for Semiconductors, ITRS 2012 Update, online at http://www.itrs.net/Links/2012ITRS/2012Chapters/2012Overview.pdf

[50] W. Arden, M. Brillouët, P. Cogez, M. Graef, et al., "More than Moore" White Paper, online at http://www.itrs.net/Links/2010ITRS/IRC-ITRS-MtM-v2%203.pdf

[51] Frost & Sullivan "Mega Trends: Smart is the New Green" online at http://www.frost.com/prod/servlet/our-services-page.pag?mode=open&sid=230169625

[52] E. Savitz, "Gartner: 10 Critical Tech Trends For The Next Five Years" online at http://www.forbes.com/sites/ericsavitz/2012/10/22/gartner-10-critical-tech-trends-for-the-next-five-years/

[53] E. Savitz, "Gartner: Top 10 Strategic Technology Trends For 2013" online at http://www.forbes.com/sites/ericsavitz/2012/10/23/gartner-top-10-strategic-technology-trends-for-2013/

[54] P. High "Gartner: Top 10 Strategic Technology Trends For 2014" online at http://www.forbes.com/sites/peterhigh/2013/10/14/gartner-top-10-strategic-technology-trends-for-2014/#

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

[56] Industrial Internet of Things (IoT) Advisory Service, ARC Advisory Group, online at, http://www.arcweb.com/services/pages/industrial-internet-of-things-service.aspx

[57] rtSOA - A Data Driven, Real Time Service Oriented Architecture for Industrial Manufacturing, online at http://www-db.in.tum.de/research/projects/rtSOA/

[58] P. C. Evans and M. Annunziata, Industrial Internet: Pushing the Boundaries of Minds and Machines, General Electric Co., online

at http://files.gereports.com/wp-content/uploads/2012/11/ge-industrial-internet-vision-paper.pdf
[59] Cisco, "Securely Integrating the Cyber and Physical Worlds", online at http://www.cisco.com/web/solutions/trends/tech-radar/securing-the-iot.html
[60] NXT Cities, online at http://www.communicasia.com/wp-content/themes/cmma2014/images/img-nxtcities-large.jpg
[61] NXT Enterprises, online at http://www.communicasia.com/wp-content/themes/cmma2014/images/img-nxtenterprise-large.jpg
[62] NXT Connect, online at http://www.communicasia.com/wp-content/themes/cmma2014/images/img-nxtconnect-large.jpg
[63] H. Bauer, F. Grawert, and S. Schink, Semiconductors for wireless communications: Growth engine of the industry, online at www.mckinsey.com/
[64] L. Fretwell and P. Schottmiller, Cisco Presentation, online at http://www.cisco.com/assets/events/i/nrf-Internet_of_Everything_Whats_the_Art_of_the_Possible_in_Retail.pdf, January 2014.
[65] ITU-T, Internet of Things Global Standards Initiative, http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx
[66] International Telecommunication Union - ITU-T Y.2060 - (06/2012) – Next Generation Networks – Frameworks and functional architecture models - Overview of the Internet of things
[67] IEEE-SA - Enabling Consumer Connectivity Through Consensus Building, online at http://standardsinsight.com/ieee_company_detail/consensus-building
[68] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, et al., "Internet of Things Strategic Research Agenda", Chapter 2 in Internet of Things - Global Technological and Societal Trends, River Publishers, 2011, ISBN 978–87-92329–67-7
[69] O. Vermesan, P. Friess, P. Guillemin, H. Sundmaeker, et al., "Internet of Things Strategic Research and Innovation Agenda", Chapter 2 in Internet of Things – Converging Technologies for Smart Environments and Integrated Ecosystems, River Publishers, 2013, ISBN 978–87-92982–73-5
[70] SmartSantander, EU FP7 project, Future Internet Research and Experimentation, online at http://www.smartsantander.eu/
[71] Internet of Things Concept, online at http://xarxamobal.diba.cat/XGMSV/imatges/actualitat/iot.jpg

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

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

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

[75] S. Wilson, Deloitte Research, "Rising tide Exploring pathways to growth in the mobile semiconductor industry", 2013, online at http://dupress.com/articles/rising-tide-exploring-pathways-to-growth-in-the-mobile-semiconductor-industry/

[76] Gartner, "Hype Cycle for Emerging Technologies", 2011, online at http://www.gartner.com/it/page.jsp?id=1763814

[77] Gartner, 2013, online at http://www.gartner.com/newsroom/id/2636073

[78] K. Karimi and G. Atkinson, " What the Internet of Things (IoT) Needs to Become a Reality", White Paper, 2013, online at http://www.freescale.com/files/32bit/doc/white_paper/INTOTHNGSWP.pdf

[79] D. Evans, "The Internet of Things - How the Next Evolution of the Internet Is Changing Everything", CISCO White Paper, April 2011, online at http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

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

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

[82] EU 2012. The ARTEMIS Embedded Computing Systems Initiative, October 2012 online at http://www.artemis-ju.eu/

[83] Foundations for Innovation in Cyber-Physical Systems, Workshop Report, NIST, 2013, online at http://www.nist.gov/el/upload/CPS-WorkshopReport-1–30-13-Final.pdf

[84] IERC – European Research Cluster on the Internet of Things, "Internet of Things - Pan European Research and Innovation Vision", October, 2011,

online at, http://www.theinternetofthings.eu/sites/default/files/Rob%20van%20Kranenburg/IERC_IoT-Pan%20European%20Research%20and%20Innovation%20Vision_2011.pdf

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

[86] SENSEI, EU FP7 project, *D1.4:* Business models and Value Creation, 2010, online at: http://www.ict-sensei.org.

[87] IoT-I, Internet of Things Initiative, FP7 EU project, 0nline at http://www.iot-i.eu

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

[89] OUTSMART, FP7 EU project, part of the Future Internet Private Public Partnership, "OUTSMART - Provisioning of urban/regional smart services and business models enabled by the Future Internet", online at http://www.fi-ppp-outsmart.eu/en-uk/Pages/default.aspx

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

[91] NXP Semiconductors N.V., "What's Next for Internet-Enabled Smart Lighting?", online at http://www.nxp.com/news/press-releases/2012/05/whats-next-for-internet-enabled-smart-lighting.html

[92] J. Formo, M. Gårdman, and J. Laaksolahti, "Internet of things marries social media", in *Proceedings of the 13th International Conference on MobileHCI,* ACM, New York, NY, USA, pp. 753–755, 2011

[93] J. G. Breslin, S. Decker, and M. Hauswirth, et. al., "Integrating Social Networks and Sensor Networks", *W3C Workshop on the Future of Social Networking,* Barcelona, 15–16 January 2009

[94] M. Kirkpatrick, "The Era of Location-as-Platform Has Arrived", *ReadWriteWeb*, January 25, 2010

[95] F. Calabrese, K. Kloeckl, and C. Ratti (MIT), "WikiCity: Real-Time Location-Sensitive tools for the city", in *IEEE Pervasive Computing*, July-September 2007

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

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

[98] N. Maisonneuve, M. Stevens, M. E. Niessen, L. Steels, "NoiseTube: Measuring and mapping noise pollution with mobile phones", in *Information Technologies in Environmental Engineering (ITEE 2009)*, Proceedings of

the 4th International ICSC SymposiumThessaloniki, Greece, May 28–29, 2009

[99] J-S. Lee, B. Hoh, "Sell your experiences: a market mechanism based incentive for participatory sensing", *2010 IEEE International Conference onPervasive Computing and Communications (PerCom)*, pp.60–68, March 29, 2010, - April 2, 2010.

[100] R. Herring, A. Hofleitner, S. Amin, T. Nasr, A. Khalek, P. Abbeel, and A. Bayen, "Using Mobile Phones to Forecast Arterial Traffic Through Statistical Learning", *89th Transportation Research Board Annual Meeting,* Washington D.C., January 10–14, 2010

[101] M. Kranz, L. Roalter, and F. Michahelles, "Things That Twitter: Social Networks and the Internet of Things", in *What can the Internet of Things do for the Citizen (CIoT) Workshop* at *The Eighth International Conference on Pervasive Computing (Pervasive 2010)*, Helsinki, Finland, May 2010

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

[103] W. Colitti, K. Steenhaut, and N. De Caro, "Integrating Wireless Sensor Networks with the Web," Extending the Internet to Low Power and Lossy Networks (IP+ SN 2011), 2011 online at http://hinrg.cs.jhu.edu/joomla/images/stories/IPSN_2011_koliti.pdf

[104] M. M. Hassan, B. Song, and E. Huh, "A framework of sensor-cloud integration opportunities and challenges", in *Proceedings of the 3*rd *International Conference on Ubiquitous Information Management and Communication,* ICUIMC 2009, Suwon, Korea, January 15–16, pp. 618–626, 2009

[105] M. Yuriyama and T. Kushida, "Sensor-Cloud Infrastructure – Physical Sensor Management with Virtualized Sensors on Cloud Computing", NBiS 2010: 1–8

[106] C. Bizer, T. Heath, K. Idehen, and T. Berners-Lee, "Linked Data on the Web", *Proceedings of the 17th International Conference on World Wide Web (WWW'08),* New York, NY, USA, ACM, pp.1265–1266, 2008

[107] T. Heath and C. Bizer, "Linked Data: Evolving the Web into a Global Data Space", *Synthesis Lectures on the Semantic Web: Theory and Technology*, 1st edition. Morgan & Claypool, 1:1, 1–136, 2011

[108] IBM, "An architectural blueprint for autonomic computing", IBM White paper. June 2005

[109] "Autonomic Computing: IBM's perspective on the state of Information Technology", 2001, http://www.research.ibm.com/autonomic/manifesto /autonomic_computing.pdf
[110] Connected Devices for Smarter Home Environments, IBM Data Magazine, 2014, online at http://ibmdatamag.com/2014/04/connected-devices-for-smarter-home-environments/
[111] International Conference on Autonomic Computinghttp://www. autonomic-conference.org/
[112] IEEE International Conferences on Self-Adaptive and Self-Organizing Systems, http://www.saso-conference.org/
[113] International Symposium on Software Engineering for Adaptive and Self-Managing Systems, http://www.seams2012.cs.uvic.ca/
[114] Awareness project, Self-Awareness in Autonomic Systemshttp://www .aware-project.eu/
[115] M. C. Huebscher, J. A. McCann, "A survey of autonomic computing – degrees, models, and applications", *ACM Computing Surveys (CSUR)*, Volume 40 Issue 3, August 2008
[116] A. S. Rao, M. P. Georgeff, "BDI Agents: From Theory to Practice", in *Proceedings of The First International Conference on Multi-agent Systems (ICMAS)*,1995. pp.312–319
[117] G. Dimitrakopoulos, P. Demestichas, W. Koenig, *Future Network & Mobile Summit 2010 Conference Proceedings.*
[118] John Naisbit and Patricia Aburdene (1991), *Megatrends 2000*, Avon
[119] D. C. Luckham, Event Processing for Business: Organizing the Real-Time Enterprise, John Wiley & Sons, 2012.
[120] T. Mitchell, *Machine Learning*, McGraw Hill, 1997
[121] D. Estrin, "Participatory Sensing: Applications and Architecture, online at http://research.cens.ucla.edu/people/estrin/resources/conferences/ 2010-Estrin-participatory-sensing-mobisys.pdf O. Etzion, P. Niblett, *Event Processing in Action*, Manning, 2011
[122] V. J. Hodgem, J. Austin, "A Survey of Outlier Detection Methodologies", *Artificial Intelligence Review*, 22 (2), pages 85–126, 2004.
[123] F. Angiulli, and C. Pizzuti, "Fast outlier detection in high dimensional spaces" in *Proc. European Conf. on Principles of Knowledge Discovery and Data Mining*, 2002
[124] H. Fan, O. Zaïane, A. Foss, and J. Wu, "Nonparametric outlier detection for efficiently discovering top-n outliers from engineering data", in *Proc. Pacific-Asia Conf. on Knowledge Discovery and Data Mining (PAKDD)*, Singapore, 2006

[125] A. Ghoting, S. Parthasarathy, and M. Otey, "Fast mining of distance-based outliers in high dimensional spaces", in *Proc. SIAM Int. Conf. on Data Mining (SDM)*, Bethesda, ML, 2006

[126] G. Box, G. Jenkins, *Time series analysis: forecasting and control*, rev. ed., Oakland, California: Holden-Day, 1976

[127] J. Hamilton, *Time Series Analysis*, Princeton Univ. Press, 1994

[128] J. Durbin and S.J. Koopman, *Time Series Analysis by State Space Methods*, Oxford University Press, 2001

[129] R. O. Duda, P. E. Hart, D. G. Stork, *Pattern Classification, 2nd Edition*, Wiley, 2000

[130] C.M. Bishop, *Neural Networks for Pattern Recognition*, Oxford University Press, 1995

[131] C. M. Bishop, *Pattern Recognition and Machine Learning*, Springer, 2006

[132] M. J. Zaki, "Generating non-redundant association rules", *Proceedings of the sixth ACM SIGKDD international conference on Knowledge discovery and data mining*, 34–43, 2000

[133] M. J. Zaki, M. Ogihara, "Theoretical foundations of association rules", *3rd ACM SIGMOD Workshop on Research Issues in Data Mining and Knowledge Discovery*, 1998

[134] N. Pasquier, Y. Bastide, R. Taouil, L. Lakhal, "Discovering Frequent Closed Itemsets for Association Rules", *Proceedings of the 7th International Conference on Database Theory*, (398–416), 1999

[135] C. M. Kuok, A. Fu, M. H. Wong, "Mining fuzzy association rules in databases", *SIGMOD Rec.* 27, 1 (March 1998), 41–46.

[136] T. Kohonen, *Self-Organizing Maps*, Springer, 2001

[137] S.-H. Hamed, S. Reza, "TASOM: A New Time Adaptive Self-Organizing Map", *IEEE Transactions on Systems, Man, and Cybernetics–Part B: Cybernetics* 33 (2): 271–282, 2003

[138] L.J.P. van der Maaten, G.E. Hinton, "Visualizing High-Dimensional Data Using t-SNE", *Journal of Machine Learning Research* 9(Nov): 2579–2605, 2008

[139] I. Guyon, S. Gunn, M. Nikravesh, and L. Zadeh (Eds), *Feature Extraction, Foundations and Applications*, Springer, 2006

[140] Y. Bengio, "Learning deep architectures for AI", *Foundations and Trends in Machine Learning*, 2(1):1–12, 2009

[141] Y. Bengio, Y. LeCun, "Scaling learning algorithms towards AI", *Large Scale Kernel Machines*, MIT Press, 2007

[142] B. Hammer, T. Villmann, "How to process uncertainty in machine learning?", *ESANN'2007 proceedings - European Symposium on Artificial Neural Networks*, Bruges (Belgium), 2007

[143] J. Quinonero-Candela, C. Rasmussen, F. Sinz, O. Bousquet, and B. Schölkopf, "Evaluating Predictive Uncertainty Challenge", in *Machine Learning Challenges: Evaluating Predictive Uncertainty, Visual Object Classification, and Recognising Tectual Entailment,* First PASCAL Machine Learning Challenges Workshop (MLCW 2005), Springer, Berlin, Germany, 1–27, 2006

[144] D. Koller and N. Friedman, *Probabilistic graphical models: principles and techniques*, MIT press, 2009

[145] M. R. Endsley, "Measurement of situation awareness in dynamic systems", *Human Factors*, 37, 65–84, 1995

[146] R. Fuller, *Neural Fuzzy System*, Åbo Akademi University, ESF Series A: 443, 1995, 249 pages. [ISBN 951–650-624–0, ISSN 0358–5654]

[147] S. Haykin, *Neural Networks: A Comprehensive Foundation, 2nd edn.*, Prentice-Hall, New York (1999)

[148] L. Rabiner, "A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition," *Proceedings of the IEEE*, vol. 77, no. 2, Feb. 1989

[149] S.K. Murthy, "Automatic construction of decision trees from data: a multi-disciplinary survey", *Data Mining Knowledge Discovery*, 1998.

[150] A. El Gamal, and Y-H Kim,"Network Information Theory", *Cambridge University Press*, 2011

[151] Z. Ma, "An Electronic Second Skin", in *Science*, vol. 333, 830–831 12 August, 2011

[152] Body Area Networks, IEEE 802.15 WPAN Task Group 6 (TG6), online athttp://www.ieee802.org/15/pub/TG6.html

[153] M. Debbah, "Mobile Flexible Networks: Research Agenda for the Next Decade", 2008, online at http://www.supelec.fr/d2ri/flexibleradio/pub/atc-debbah.pdf

[154] S. Venkatesan, "Limits on transmitted energy per bit in a cellular wireless access network", Private communication, Radio Access Domain, Bell Labs, New Jersey, USA

[155] GreenTouch Consortium, online at www.greentouch.org

[156] GreenTouch, "Annual Report 2010–2011", online at http://www.greentouch.org/uploads/documents/GreenTouch_2010–2011_Annual_Report.pdf

[157] G. Rittenhouse et al., "Understanding Power Consumption in Data Networks: A Systematic Approach", Eco. White paper, Alcatel-Lucent Bell Labs, Nov. 2009

[158] A. Gluhak, M. Hauswirth, S. Krco, N. Stojanovic, M. Bauer, R. Nielsen, S. Haller, N. Prasad, V. Reynolds, and O. Corcho, "An Architectural Blueprint for a Real-World Internet", in *The Future Internet - Future Internet Assembly 2011: Achievements and Technological Promises*, Lecture Notes in Computer Science, Vol. 6656, 1 st Edition, Chapter 3.3 Interaction Styles, 2011

[159] G. Grov, Al. Bundy, C. B. Jones, and A. Ireland, "The Al4FM approach for proof automation within formal methods", Submission to *Grand Challenges in Computing Research 2010*, UKCRC, online at http://www.ukcrc.org.uk/grand-challenge/gccr10-sub-20.cfm

[160] C.A.R. Hoare, "Communicating Sequential Processes", Prentice Hall International, 1985 + 2004, ISBN 0131532715, and http://www.usingcsp .com/

[161] R. Milner, "Communicating and Mobile Systems: The calculus", *Cambridge University Press*, 1999, ISBN 0–521-65869–1

[162] S. Haller and C. Magerkurth, "The Real-time Enterprise: IoT-enabled Business Processes", IETF IAB Workshop on Interconnecting Smart Objects with the Internet, March 2011

[163] OMG, Business Process Model and Notation specification, available at http://www.omg.org/technology/documents/br_pm_spec_catalog.htm, last accessed: November 15, 2011

[164] OASIS, Web Services Business Process Execution Language, http://docs.oasis-open.org/wsbpel/2.0/wsbpel-v2.0.html, last accessed: November 15, 2011.

[165] W3C, Unified Service Description Language Incubator Group, online at http://www.w3.org/2005/Incubator/usdl/, last accessed: November 15, 2011

[166] makeSense, EU FP7 Project, online at http://www.project-makesense.eu/, last accessed: November 15, 2011

[167] J. Hellerstein, "Parallel Programming in the Age of Big Data", 2008, online at http://gigaom.com/2008/11/09/mapreduce-leads-the-way-for-parallel-programming/

[168] E. Dans, " Big Data: a small introduction", 2011, Retrieved from online at http://www.enriquedans.com/2011/10/big-data-una-pequena-introduccion.html.

[169] A. Sheth, C. Henson, and S. Sahoo, "Semantic sensor web", *Internet Computing*, IEEE, vol. 12, no. 4, pp. 78–83, July-Aug. 2008.
[170] Open Geospatial Consortium, Geospatial and location standards,http://www.opengeospatial.org.
[171] M. Botts, G. Percivall, C. Reed, and J. Davidson, "oGC Sensor Web Enablement: Overview and High Level Architecture", *The Open Geospatial Consortium*, 2008, online at http://portal.opengeospatial.org/files/?artifact id=25562
[172] W3C Semantic Sensor Network Incubator Group, Incubator Activity, online at http://www.w3.org/2005/Incubator/ssn/
[173] Semantic Sensor Network Incubator Group, State of the Art Survey, http://www.w3.org/2005/Incubator/ssn/wiki/State_of_the_art_survey.
[174] S. Decker and M. Hauswirth, "Enabling networked knowledge", in *CIA '08: Proceedings of the 12th international workshop on Cooperative Information Agents XII*, Berlin, Heidelberg: Springer-Verlag, pp. 1–15, 2008
[175] P. Barnaghi, M. Presser, and K. Moessner, "Publishing Linked Sensor Data", in *Proceedings of the 3rd International Workshop on Semantic Sensor Networks (SSN)*, Organised in conjunction with the International Semantic Web Conference (ISWC) 2010, November 2010
[176] Logical Neighborhoods, Virtual Sensors and Actuators, online at http://logicalneighbor.sourceforge.net/vs.html
[177] K. M. Chandy and W. R. Schulte, "What is Event Driven Architecture (EDA) and Why Does it Matter?", 2007, online at http://complexevents.com/?p=212, (accessed on: 25.02.2008)
[178] D. Luckham, "What's the Difference Between ESP and CEP?", 2006, online at http://complexevents.com/?p=103, accessed on 15.12.2008
[179] The CEP Blog, http://www.thecepblog.com/
[180] EnOcean - the Energy Harvesting Wirless Standard for Building Automation and Industrial Automation, online at http://www.enocean.com/en/radio-technology/
[181] IEEE Std 802.15.4^{TM}-2006, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), online at http://www.ieee802.org/15/pub/TG4.html
[182] Bluetooth Low Energy (LE) Technology Info Site, online athttp://www.bluetooth.com/English/Products/Pages/low_energy.aspx
[183] The Official Bluetooth Technology Info Site, online at http://www.bluetooth.com/

[184] M-G. Di Benedetto and G. Giancola, *Understanding Ultra Wide Band Radio Fundamentals*, Prentice Hall, June 27, 2004
[185] ISO, International Organization for Standardization (ISO), Identification cards – Contactless integrated circuit(s) cards – Vicinity cards, ISO/IEC 14443, 2003
[186] N. Pletcher, S. Gambini, and J. Rabaey, "A 52 μW Wake-Up Receiver With 72 dBm Sensitivity Using an Uncertain-IF Architecture", in *IEEE Journal of Solid-State Circuits*, vol. 44, no1, January, pp. 269–280. 2009
[187] A. Vouilloz, M. Declercq, and C. Dehollain, "A Low-Power CMOS Super-Regenerative Receiver at 1 GHz", in *IEEE Journal of Solid-State Circuits*, vol. 36, no3, March, pp. 440–451, 2001
[188] J. Ryckaert, A. Geis, L. Bos, G. van der Plas, J. Craninckx, "A 6.1 GS/s 52.8 mW 43 dB DR 80 MHz Bandwidth 2.4 GHz RF Bandpass S-? ADC in 40 nm CMOS", in *IEEE Radio-Frequency Integrated Circuits Symposium*, 2010
[189] L. Lolis, C. Bernier, M. Pelissier, D. Dallet, and J.-B. Bégueret, "Band-pass Sampling RX System Design Issues and Architecture Comparison for Low Power RF Standards", *IEEE ISCAS 2010*
[190] D. Lachartre, "A 550 μW inductorless bandpass quantizer in 65 nm CMOS for 1.4-to-3 GHz digital RF receivers", *VLSI Circuits 2011*, pp. 166–167, 2011
[191] S. Boisseau and G. Despesse,"Energy Harvesting, Wireless Sensor Networks & Opportunities for Industrial Applications", in *EETimes,* 27th Feb 2012, online at http://www.eetimes.com
[192] J.G. Koomey, S. Berard, M. Sanchez, and H. Wong, "Implications of Historical Trends in the Electrical Efficiency of Computing", in *IEEE Annals of the History of Computing*, vol. 33, no. 3, pp. 46–54, March 2011
[193] eCall - eSafety Support, online at http://www.esafetysupport.org/en/ecall_toolbox/european_commission/index.html
[194] European Commission, "Smart Grid Mandate, Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployments", M/490 EN,,Brussels 1st March, 2011
[195] Global Certification Forum, online at http://www.globalcertification forum.org
[196] SENSEI, EU FP7 project, online at http://www.sensei-project.eu
[197] IoT-A, EU FP7 project, online at http://www.iot-a.eu
[198] IoT6, EU FP7 project, online at http://www.iot6.eu
[199] IoT@Work, EU FP7 project, online at https://www.iot-at-work.eu/

[200] Federated Object Naming Service, GS1, online at http://www.gs1.org/gsmp/community/working_groups/gsmp#FONS
[201] Directive 2003/98/EC of the European Parliament and of the Council on the reuse of public sector information, 17 November 2003, online at http://ec.europa.eu/information_society/policy/psi/docs/pdfs/directive/psi_directive_en.pdf
[202] INSPIRE, EU FP7 project, – Infrastructure for Spatial Information in Europe, online at http://inspire.jrc.ec.europa.eu/
[203] H. van der Veer, A. Wiles, "Achiveing Technical Interoperability – the ETSI Approach", ETSI White Paper No.3, 3rd edition, April 2008, http://www.etsi.org/images/files/ETSIWhitePapers/IOP%20whitepaper%20Edition%203%20final.pdf
[204] Ambient Assisted Living Roadmap, AALIANCE
[205] Atmel AVR Xmega Micro Controllers, http://it.mouser.com/atmel_xmega/
[206] Worldwide Cellular M2M Modules Forecast, Beecham Research Ltd, August 2010
[207] Future Internet Assembly Research Roadmap, FIA Research Roadmap Working Group, May 2011
[208] D. Scholz-Reiter, M.-A. Isenberg, M. Teucke, H. Halfar, "An integrative approach on Autonomous Control and the Internet of Things", 2010
[209] NIEHS on EMF, http://www.niehs.nih.gov/health/topics/agents/emf/
[210] R.H. Weber/R. Weber, "Internet of Things - Legal Perspectives", Springer, Berlin 2010
[211] "The Global Wireless M2M Market", Berg Insight, 2010, http://www.berginsight.com/ReportPDF/ProductSheet/bi-gwm2m-ps.pdf
[212] M. Hatton, "Machine-to-Machine (M2M) communication in the Utilities Sector 2010–2020", Machina Research, July 2011.
[213] G. Masson, D. Morche, H. Jacquinot, and P. Vincent, "A 1 nJ/b 3.2–4.7 GHz UWB 50 Mpulses/s Double Quadrature Receiver for Communication and Localization", in *ESSCIRC 2010*