Internet of Things

Strategic Research Roadmap

15 SEPTEMBER, 2009

The meaning of things lies not in the things themselves, but in our attitude towards them.

Antoine de Saint-Exupery

Table of content

Executive Summary

As a part of future trends and developments the coming Internet of Things will shape the world and the society – yet sound research work and applicable recommendations are necessary to guide Europe on its way and to make it beneficial for all citizens.

In order to reply to this challenge the Cluster of European Research Projects on the Internet of Things (CERP-IoT) developed in 2009 its Strategic Research Agenda (SRA), taking into account its experiences and the results from the ongoing exchange among European and international experts.

The present document proposes a list of research fields and a roadmap on future R&D until 2010, before 2015 and beyond 2020.

This initial CERP-IoT SRA version is part of a continuous IoT community dialogue initiated by the European Commission (EC) DG INFSO-D4 Unit for the European and international IoT stakeholders. The result is a lively one and will be updated with expert feedback from ongoing and next calls for proposals within the FP7 Framework Program on Research and Development in Europe.

The SRA for the Internet of Things is the result of a four-step collaboration between the members of the cluster research projects:

1. Elaboration of an IoT common definition about the meaning of "Things" and IoT visions, introducing the IoT concept and presenting the underlying vision
2. Identification of IoT Application Domains exploring the application domains for the future IoT
3. Identification of Technologies that will drive the IoT development and supporting the IoT vision
4. Formulation of an IoT Research Agenda, presenting the research challenges and priorities, the standardization issues and the security and privacy concerns that have to be addressed and solved over the next decade

As a result the main outcomes could be summarized as follows:

- The Internet of Things is an integrated part of Future Internet and could be defined as a dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual “things” have identities, physical attributes, virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.
- The vision of Future Internet based on standard communication protocols considers the merging of computer networks, Internet of Media (IoM), Internet of Services (IoS), and Internet of Things (IoT) into a common global IT platform of seamless networks and networked “things”. This future network of networks will be laid out as public/private infrastructures and dynamically extended and improved by terminals created by the “things” connecting to one another.
- We envisage that the Internet of Things will allow people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service.
- The concept of Internet of Things can be regarded as an extension of the existing interaction between humans and applications through the new dimension of “Things” communication and integration.
- The main identified IoT application domains are:
  - Aerospace and aviation,
  - Automotive,
  - Telecommunications,
  - Intelligent Buildings,
  - Medical Technology, Healthcare,
  - Independent Living,
  - Pharmaceutical,
  - Retail, Logistics, Supply Chain Management,
  - Manufacturing, Product Lifecycle Management,
  - Oil and Gas
  - Safety, Security and Privacy,
  - Environment Monitoring,
  - People and Goods Transportation,
  - Food traceability,
  - Agriculture and Breeding,
  - Media, entertainment and Ticketing,
  - Insurance,
  - Recycling

The main IoT technologies presented allow identifying the research and development challenges and outlining a roadmap for future research activities to provide practical and reliable solutions.

This roadmap forms the basis for the research priorities presented and these IoT enabling technologies are:

- Identification Technology,
- Internet of Things Architecture Technology,

- Communication Technology,
- Network Technology,
- Network Discovery,
- Software and algorithms,
- Hardware,
- Data and Signal Processing Technology,
- Discovery and Search Engine Technologies,
- Relationship Network Management Technologies,
- Power and Energy Storage Technologies,
- Security and Privacy Technologies,
- Standardisation

SRA Coordinators:

Patrick Guillemin, CERP-IoT Coordinator, ETSI
Peter Friess, CERP-IoT EC Coordinator, European Commission

SRA Core Authors and Editor Team:

Ovidiu Vermesan, NO, SINTEF, EPoSS
Mark Harrison, UK, University of Cambridge, Auto-ID Lab, BRIDGE, EPCglobal Data Discovery JRG
Harald Vogt, DE, SAP, SToP
Kostas Kalaboukas, GR, SingularLogic, EURIDICE
Maurizio Tomasella, UK, University of Cambridge, Auto-ID Lab , SMART, BRIDGE, Auto-ID Lab
Karel Wouters, BE, K.U.Leuven, PrimeLife
Sergio Gusmeroli, IT, TXT e-Solutions SpA, iSURF, COIN
Stephan Haller, CH, SAP, CoBIS

The authors would appreciate any sharing of thoughts from the interested reader and constructive feedback on the IoT Strategic Research Agenda.

Contact:

Patrick.guillemin@etsi.org
Peter.FRIESS@ec.europa.eu

Chapter 1
Internet of Things Vision

1.1 Internet of Things Common Definition

The meaning of "things"

Defining things and recognizing what a particular thing is and represents in the context of Future Internet requires a careful analysis of what philosophers like Aristotle and Philoponus had to say and how their philosophical thoughts can transcend into the future.

Aristotle, in his work "The Categories" gives a strikingly general and exhaustive account of the things that are (ta onta) - beings. According to this opinion, beings can be divided into ten distinct categories. They include substance, quality, quantity, and relation, among others. Of these categories of beings, it is the first, substance (ousia), to which Aristotle gives a privileged position.

Aristotle is distinguishing things that are by nature from those that are from other causes. Philoponus, commenting on this distinction, first divides things that are by nature into those that have soul and those that do not.

The proper nature of "besouled" things (i.e., plants and animals) is their form, which, Philoponus says is properly identified with soul, their intrinsic mover.

From the "philosophical definition" of "things" one can conclude that the word is not restricted to material things but can apply to virtual things and the events that are connected to "things".

In the context of "Internet of Things" a "thing" could be defined as a real/physical or digital/virtual entity that exists and move in space and time and is capable of being identified. Things are commonly identified either by assigned identification numbers, names and/or location addresses.

Internet of Things

Internet of Things (IoT) is an integrated part of Future Internet and could be defined as a dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.

In the IoT, "things" are expected to become active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment by exchanging data and information "sensed" about the environment, while reacting autonomously to the "real/physical world" events and influencing it by running processes that trigger actions and create services with or without direct human intervention.

Interfaces in the form of services facilitate interactions with these "smart things" over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues.

1.2 Internet of Things Vision

The vision of Future Internet based on standard communication protocols considers the merging of computer networks, Internet of Media (IoM), Internet of Services (IoS), and Internet of Things (IoT) into a common global IT platform of seamless networks and networked "things".

IoS is denoting a software based component that will be delivered via different networks and Internet. Research on SOA, Web/Enterprise 3.0/X.0, Enterprise Interoperability, Service Web, Grid Services and Semantic Web will address important bits of the IoS puzzle, while improving cooperation between service providers and consumers.

IoM will address the challenges in scalable video coding and 3D video processing, dynamically adapted to the network conditions that will give rise to innovative applications such as massive multiplayer mobile games, digital cinema and in virtual worlds placing new types of traffic demands on mobile network architectures.

This future network of networks will be laid out as public/private infrastructures and dynamically extended and improved by edge points created by the "things" connecting to one another. In fact, in the IoT communications will take place not only between people but also between people and their environment.

Communication will be seen more among terminals and data centres (e.g. home data centres, Cloud computing, etc) than among nodes as in current networks. Growth of storage capacity at lower and lower costs will result in the local availability of most information required by people or objects. This, coupled with the enhanced processing capabilities and always-on connectivity, will make terminals gain a main role in communications.

Terminals will be able to create a local communication network and may serve as a bridge between communication networks thus extending, particularly in urban environments, the overall infrastructure capacity. This will likely determine a different view of network architectures. The Future Internet will exhibit high levels of heterogeneity ("things" – physical/real, cyber physical, web enabled, digital and virtual, devices and device models, communication protocols, cognitive capabilities, etc.), as totally different things, in terms of functionality, technology and application fields are expected to belong to the same communication environment.

The Internet of Things will create a dynamic network of billions or trillions of wireless identifiable "things" communicating with one another and integrating the developments from concepts like Pervasive Computing, Ubiquitous Computing and Ambient Intelligence. Internet of Things hosts the vision of ubiquitous computing and ambient intelligence enhancing them by requiring a full communication and a complete computing capability among things and integrating the elements of continuous communication, identification and interaction. The Internet of Things fuses the digital world and the physical world by bringing different concepts and technical components together: pervasive networks, miniaturization of devices, mobile communication, and new models for business processes.

Applications, services, middleware components, networks, and endpoints will be structurally connected in entirely new ways. Recognising that initially there will be commercial and physical challenges to establishing global ubiquitous network connectivity and that initially the many connected things and devices may have limited ability to engage in 2-way network connectivity, it is important that the architectural design for the Internet of Things supports effective two-way caching and data synchronisation techniques, as well as network-connected endpoints for virtual representations of the connected things and devices, which can be used for monitoring their location, condition and state, as well as sending requests and instructions to them.

The Internet of Things will bring tangible business benefits, such as the high-resolution management of assets and products, improved life-cycle management, and better collaboration between enterprises; many of these benefits are achieved through the use of unique identification for individual things together with search and discovery services, enabling each thing to interact individually, building up an individual life history of its activities and interactions over time.

Improved sensor and device capabilities will also allow business logic to be executed on the edges of a network – enabling some existing business processes to be decentralized for the benefit of performance, scalability, and local decision-making. For example, algorithms could be used for intelligent decision-making based on real-time readings from sensors that are used to monitor the health of patients or the condition of vehicles, in order to detect the early signs of problems or deterioration of condition.

The Internet of Things allows people and things to be connected **A**nytime, **A**nyplace, with **A**nything and **A**nyone, ideally using **A**ny path/network and **A**ny service. This implies addressing elements such as **C**onvergence, **C**ontent, **C**ollections (Repositories), **C**omputing, **C**ommunication, and **C**onnectivity in the context where there is seamless interconnection between people and things and/or between things and things so the **A** and **C** elements are present and addressed.

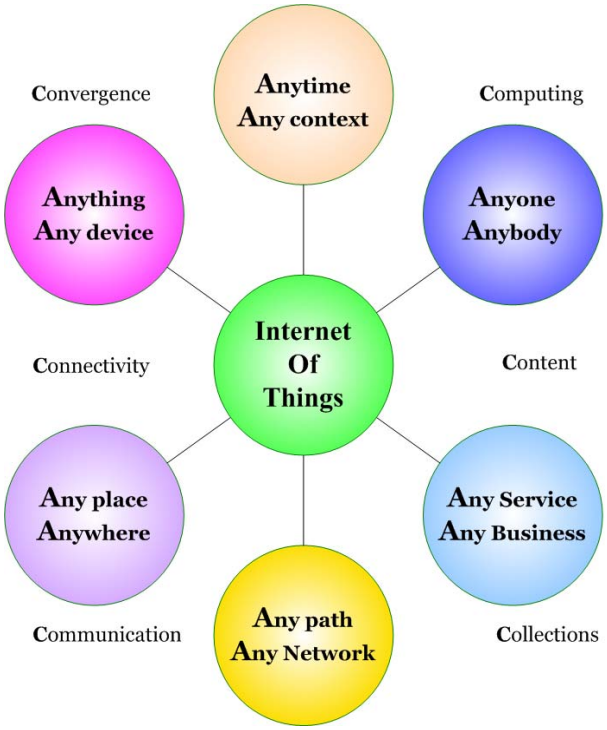

Figure 1 Internet of Things

The Internet of Things implies a symbiotic interaction among the real/physical, the digital/virtual worlds: physical entities have digital counterparts and virtual representation; things become context aware and they can sense, communicate, interact, exchange data, information and knowledge. Through the use of intelligent decision-making algorithms in software applications, appropriate rapid responses can be given to physical phenomena, based on the very latest information collected about physical entities and consideration of patterns in the historical data, either for the same entity or for similar entities. These create new opportunities to meet business requirements, create new services based on real time physical world data, gain insights into complex processes and relationships, handle incidents, address environmental degradation (pollution, disaster, global warming, etc), monitor human activities (health, movements, etc.), improve infrastructure integrity (energy, transport, etc.), and address energy efficiency issues (smart energy metering in buildings, efficient consumption by vehicles, etc.).

Everything from individuals, groups, communities, objects, products, data, services, processes will be connected by the IoT. Connectivity will become in the IoT a kind of commodity, available to all at a very low cost and not owned by any private entity. In this context, there will be the need to create the right situation-aware development environment for stimulating the creation of services and proper intelligent middleware to understand and interpret the information, to ensure protection from fraud and malicious attack (that will inevitably grow as Internet becomes more and more used) and to guarantee privacy.

Under this vision and making use of intelligence in the supporting network infrastructure, things will be able to autonomously manage their transportation, implement fully automated processes and thus optimise logistics; they might be able to harvest the energy they need; they

will configure themselves when exposed to a new environment, and show an "intelligent/cognitive" behaviour when faced with other things and deal seamlessly with unforeseen circumstances; and, finally, they might manage their own disassembly and recycling, helping to preserve the environment, at the end of their lifecycle.

The Internet of Things infrastructure allows combinations of smart objects (i.e. wireless sensors, mobile robots, etc), sensor network technologies, and human beings, using different but interoperable communication protocols and realises a dynamic multimodal/heterogeneous network that can be deployed also in inaccessible, or remote spaces (oil platforms, mines, forests, tunnels, pipes, etc.) or in cases of emergencies or hazardous situations (earthquakes, fire, floods, radiation areas, etc.,). In this infrastructure, these different entities or "things" discover and explore each other and learn to take advantage of each other's data by pooling of resources and dramatically enhancing the scope and reliability of the resulting services.

The "things" in the Internet of Things vision will influence each other depending their functional capabilities (e.g. computational processing power, network connectivity, available power, etc.) as well as on context and situations (time, space etc.) and will be actively involved in different processes. Some of their attributes, actions and involvements are clustered under five domains and presented in Table 1:

Table 1 Characteristics and attributes clustered under functional domains

Domain 1 - Fundamental characteristics	• "Things" can be "real world entities" or "virtual entities" • "Things" have identity; there are means for automatically identifying them • "Things" are environmentally safe • "Things" (and their virtual representations) respect the privacy, security and safety of other "things" or people with which they interact • "Things" use protocols to communicate with each other and the infrastructure • "Things" are involved in the information exchange between real/physical, digital and virtual worlds
Domain 2 – Common characteristics of all things, even the most basic (applies to all higher classes too)	• "Things" can use services that act as interfaces to "things" • "Things" would be competing with other "things" on resources, services and subject to selective pressures • "Things" may have sensors attached, thus they can interact with their environment
Domain 3 - Characteristics of social things (applies to all higher classes too)	• "Things" can communicate with other "things", computing devices and with people • "Things" can collaborate to create groups or networks • "Things" can initiate communication
Domain 4 - Characteristics of considerate autonomous things (applies to all higher classes too)	• "Things" can do many tasks autonomously • "Things" can negotiate, understand and adapt to their environment • "Things" can extract patterns from the environment or to learn from other "things" • "Things" can take decisions through their reasoning capabilities • "Things" can selectively evolve and propagate information
Domain 5 - Characteristics of things that are capable of self-replication or control	• "Things" can create, manage and destroy other "things"

In the IoT architecture, intelligent middleware will allow the creation of a dynamic map of the real/physical world within the digital/virtual space by using a high temporal and spatial resolution and combining the characteristics of ubiquitous sensor networks and other identifiable "things".

In the physical world, things respond to stimuli from the environment in a consistent manner. When white light is shone on a red object the dye absorbs nearly all the light except the red, which is reflected. At an abstract level, the coloured surface is an interface for the object, and

the light arriving at object can be a message sent to the thing, and accordingly its reflection is the response from the thing. The consistency in responses received from the interfaces for each message, enables things to interact with their surroundings. Hence to make the virtual world comprehensible, there needs to be consistency in messages and their responses. This is enabled through standard interfaces, which in turn facilitate interoperability.

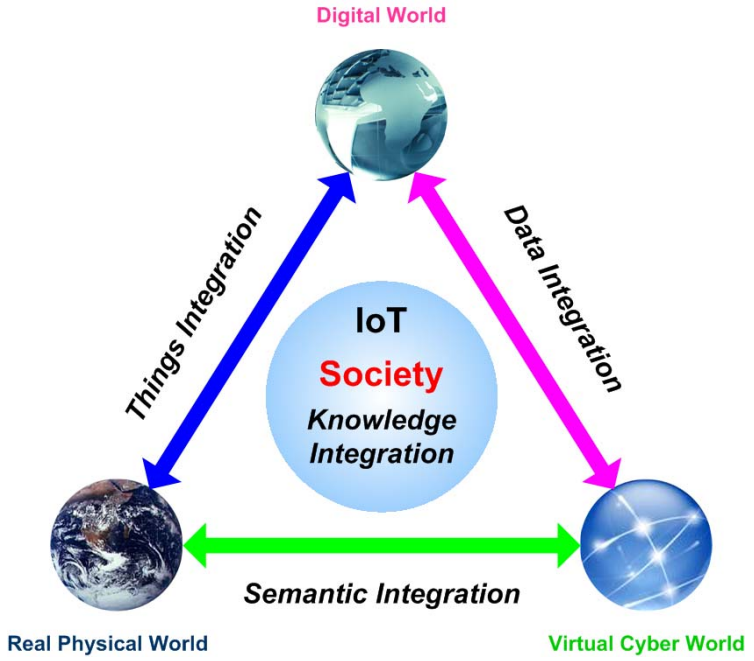

Figure 2 Internet of Things - a symbiotic interaction among the real/physical, the digital, virtual worlds and society

In the vision of Internet of Things, it is foreseeable that any "thing" will have at least one unique way of identification (directly by a "Unique Identifier" or indirectly by some "Virtual Identifier" techniques), creating an addressable continuum of "things" such as computers, sensors, people, actuators, refrigerators, TVs, vehicles, mobile phones, clothes, food, medicines, books, passports, luggage, etc. Having the capability of addressing and communicating with each other and verifying their identities, all these "things" will be able to exchange information and, if necessary, be deterministic. It is also desirable that some "things" have multiple virtual addresses and identities to participate in different contexts and situations under different "personalities".

Many "things" will be able to have communications capabilities embedded within them and will be able to create a local communication network in an ambient environment together with other "things". These ad-hoc networks will connect with other communication networks, locally and globally and the functionalities of the "things" will be influenced by the communications capabilities and by the context. "Things" could retrieve reference information and start to utilize new communication means based on their environment.

Chapter 2
Internet of Things Application Domains

The concept of Internet of Things can be regarded as an extension of the existing interaction between humans and applications through the new dimension of "Things" communication and integration. IoT will add value and extend the capabilities of traditional and localised exploitation of automatic identification and data capture (AIDC) and other interfacing 'edge' technologies and examples of envisioned IoT applications will be given in in the following sections.

The term "Things" can be perceived in a different way and depending on the domain in which it is used. In Industry, the "Thing" may typically be the product itself, the equipment, transportation means, etc; everything that participates in the product lifecycle. In Environment this might refer to the trees, a building, condition measurement devices, etc. Lastly, in the whole society the "Thing" may be related to devices within public spaces or devices for Ambient Assisted Living, etc. Hence, and in order to think of the possible applications for the Internet of Things, we need to identify the main application domains, a proposal of which is illustrated in Figure 3.

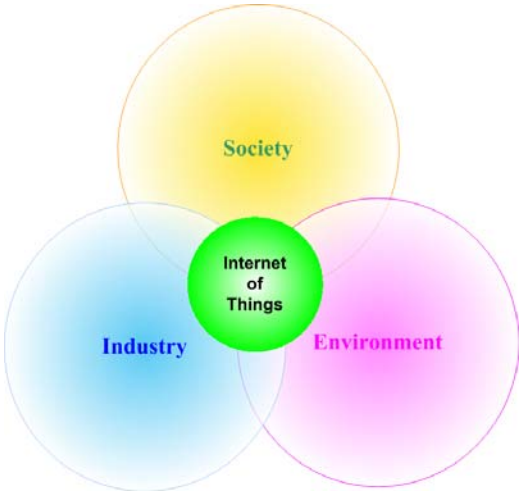

Figure 3 IoT Applications Domain

The characteristics of each domain and some indicative examples are presented the Table 2.

Table 2: IoT Application Domains - Description and Examples

Domain	Description	Indicative examples
Industry	Activities involving financial or commercial transactions between companies, organisations and other entities	Manufacturing, logistics, service sector, banking, financial governmental authorities, intermediaries, etc.
Environment	Activities regarding the protection, monitoring and development of all natural resources	Agriculture & breeding, recycling, environmental management services, energy management, etc.
Society	Activities/ initiatives regarding the development and inclusion of societies, cities, and people	Governmental services towards citizens and other society structures (e-participation), e-inclusion (e.g. aging, disabled people), etc.

Since we cannot isolate any of the above domains, we need to think in terms of developing new applications and services that apply at intra- and inter-domain level. For example, monitoring of the food chain, or dangerous goods, has not only to do with the industry itself, but also has societal implications that need to be taken into consideration.

Therefore, in the Internet of Things paradigm, we can refer to *Applications* (in the sense of a whole system/ framework/ tool that supports one or more of the above domains) and isolated *Services* that cater for a specific functionality/ need of the intra- inter domain level. While these applications domains have different objectives/goals, they don't have significantly different requirements with regard to IoT and applications that would be deployed on that platform.

2.1 Aerospace and aviation (systems status monitoring, green operations)

The Internet of Things can help to improve safety and security of products and services by protecting them from counterfeiting. The aviation industry, for example, is threatened by the problem of suspected unapproved parts (SUP). An SUP is an aircraft part that is not guaranteed to meet the requirements of an approved aircraft part (e.g., counterfeits, which do not conform to the strict quality constraints of the aviation industry). Thus, SUPs seriously violate the security standards of an aircraft. Aviation authorities report that at least 28 accidents or incidents in the United States have been caused by counterfeits [1]. Apart from time-consuming material analyses, verifying the authenticity of aircraft parts can be performed by inspecting the accompanying documents, which can be easily forged. This problem can be solved by introducing electronic pedigrees for certain categories of aircraft parts, which document their origin and safety-critical events during their lifecycle (e.g., modifications). By storing these pedigrees within a decentralised database as well as on RFID tags, which are securely attached to aircraft parts, an authentication (verification of digital signatures, comparison of the pedigree on RFID tags and within the database) of these parts can be performed, for example, prior to installing them within an aircraft. Thus, safety and security of an aircraft is significantly improved.

The 'on-condition' wireless monitoring of the aircraft by using intelligent devices with sensing capabilities available within the cabin or outside and connected to the aircraft monitoring systems is another emerging application area that forms the basis for ubiquitous sensor networks [19].

The nodes in such a network will be used for detecting various conditions such as pressure, vibrations, temperature etc. The data collected gives access to customized usage trends, facilitates maintenance planning, allows condition-based maintenance, reduces maintenance and waste and will be used as input for evaluating and reducing the energy consumption during aircraft operations.

Safety - the challenge of sustaining the confidence of both the passenger and society that commercial flying will not only remain extremely safe, notwithstanding greatly increased traffic, but will reduce the incidence of accidents and enhance efficency. In this context, wireless identifiable systems will be developed using:

- RFID tags correlated with luggage in containers, RFID tag based passenger/crew/luggage/cargo tracking concepts
- RFID tags and sensors on conveyors; cost effective reading systems linked to overarching security database; CCTV and data imaging software

2.2 Automotive (systems status monitoring, V2V and V2I communication)

Applications in the automotive industry include the use of "smart things" to monitor and report everything from pressure in tyres to proximity of other vehicles. RFID technology is used to streamline vehicle production, improve logistics, increase quality control and improve customer service. The devices attached to parts contain information related to the name of the manufacturer and when and where the product was made, its serial number, type, product code, and in some applications the precise location in the facility at that moment. RFID

technology provides real-time data in the manufacturing process, maintenance operations and offers a new way of managing recalls more effectively.

The use of wireless identifiable devices helps the stakeholders to gain insight into where everything is so it is possible to accelerate assembly processes and locate cars or components in a fraction of the time. Wireless technology is ideal in enabling real-time locating systems (RTLS) and connecting with other IoT sub networks, improving vehicle tracking and management and supporting automotive manufacturers better in managing the process of testing and verifying vehicles coming off the assembly line while tracking them as they go through quality control, containment and shipping zones.

Dedicated Short Range Communication (DSRC) will also give the possibility of higher bit rates and reduce the possibility of interference with other equipment. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications will significantly advance Intelligent Transportation Systems (ITS) applications such as vehicle safety services and traffic management and will be fully integrated in the IoT infrastructure.

The vehicle itself is also considered as a 'thing', enabling it to make automatic emergency calls or breakdown calls when appropriate, collecting as much data as possible from surrounding 'things', such as the vehicle parts itself, the supporting transportation infrastructure (road/rail/etc), other vehicles in the vicinity, sensors in the load it is carrying (humans, goods, etc).

There is an extensive range of complementary AIDC technologies (microdotting, matrix coding, etc) with attributes that can often be successfully matched to needs and applied to satisfy particular applications. Microdotting is a technology designed in the 40's for military use and has become a technology of choice in the automotive industry to prevent theft.

Today other techniques, such as the use of motes, which consists of a set of extremely small microprocessors with some communication capabilities are currently also being considered because they offer additional advantages. This is an emerging field [16], which might well replace classical microdotting technologies.

2.3 Telecommunications

IoT will create the possibility of merging of different telecommunication technologies and create new services. One example is the use of GSM, NFC (Near Field Communication), low power Bluetooth, WLAN, multi hop networks, GPS and sensor networks together with SIM-card technology. In these types of applications the Reader/tag is part of the mobile phone, and different applications share the SIM-card. NFC enables communications among objects in a simple and secure way just by having them close to each other. The mobile phone can therefore be used as a NFC-reader and transmit the read data to a central server. When used in a mobile phone, the SIM-card plays an important role as storage for the NFC data and authentication credentials (like ticket numbers, credit card accounts, ID information etc).

Things can join networks and facilitate peer-to-peer communication for specialized purposes or to increase robustness of communications channels and networks. Things can form ad-hoc peer-to-peer networks in disaster situations to keep the flow of vital information going in case of telecommunication infrastructure failures.

In the long term, the borders between IoT and classic telecommunication networks will blur: a situation-aware service environment will be pervasively exploited (crossing different domains) for supporting the creation of services and understanding of information, at the same time ensuring protection from frauds (that will inevitably going to grow as Internet becomes more and more used), guaranteeing privacy. In this context, services will be composed from different providers, stakeholders, and even end-users' terminals.

Services will cross different administrative domains and users will be able to compose and mash them up freely; moreover they will readily adapt in order to provide the better functions according to computing and communication environment.

2.4 Intelligent Buildings (automatic energy metering/home automation/wireless monitoring)

Building and home automation technologies have usually been deployed only in high-level offices and luxury apartments. Much research has been done on the benefits and possibilities of "smart homes" [15]. As the technologies mature and cheap wireless communication becomes abundant, the range of applications is becoming much broader. For example, smart metering is becoming more popular for measuring energy consumption and transmitting this information to the energy provider electronically. In conjunction with modern home entertainment systems, which are based on general-purpose computing platforms, they could easily be combined with other sensors and actors within a building, thus forming a fully interconnected, smart environment. Sensors for temperature, humidity provide the necessary data to automatically adjust the comfort level and to optimize the use of energy for heating or cooling. Additional value is provided by monitoring and reacting to human activity, such that exceptional situations could be detected and people can be assisted in everyday activities, thereby supporting the elderly in an aging society.

Autonomous networked wireless identifiable devices with physical sensors that combine advances in sensor miniaturisation, wireless communication, and micro-system technology will form the ubiquitous sensor networks that can make accurate measurements of environmental parameters (temperature, humidity, light etc.) in buildings and private homes. Building energy control systems are merely the next application of wireless identifiable devices by bringing the possibility of accurate climate control for all buildings down to the level of individual houses. Web-based smart energy metering and localisation and mapping of energy consumption will be one of the IoT applications.

In this scenario, autonomic technologies and architectures will represent the enabling solution: an autonomic home network will be intelligent and capable of sensing and adapting to environment changes whilst performing self-* capabilities (e.g. configuration, healing, optimization, protection). Autonomics will make home network architecture highly dynamic and distributed enabling the interworking of several devices and systems. Interworking of home networking systems and devices with other systems and devices external to the intranet will be achieved via Personal Virtual Private Networks (VPN). Use of Personal VPN also for home networking will become more and more popular due to inexpensive, high capacity Internet connectivity: secure, inexpensive, Personal VPN solutions will be used to share files between home, office computers, people on the move, etc.

Any device or thing that has human input controls can be used to securely interface with the building's services to monitor status and change its settings. Using home automation devices with wireless communication technologies (i.e. ZigBee, 6LoWPAN, etc.) all of building's "things" can have two-way communication with each other. For example the touch screen monitor on the fridge can be used to change the thermostat's settings. Or a mobile phone entering the building can activate that person's preference profile setting for the home. Or the washing machine can autonomously order replacement parts while under warranty. Personal mobile devices will be automatically detected and integrated when within range of the home network.

2.5 Medical Technology, Healthcare, (personal area networks, monitoring of parameters, positioning, real time location systems)

The IoT will have many applications in the healthcare sector, with the possibility of using the cell phone with RFID-sensor capabilities as a platform for monitoring of medical parameters and drug delivery. The enormous advantages are to be seen firstly in prevention and easy monitoring (and having therefore an essential impact on our social system) and secondly in case of accidents and the need for ad hoc diagnosis.

The combination of sensors, RFID, NFC (near field communication), Bluetooth, ZigBee, 6LoWPAN, WirelessHART, ISA100, WiFi will allow significantly improved measurement and monitoring methods of vital functions (temperature, blood pressure, heart rate, cholesterol levels, blood glucose etc). In addition, it is expected that the sensor technology will become

available and at much lower cost and with built-in support for network connectivity and remote monitoring.

Implantable wireless identifiable devices could be used to store health records that could save a patient's life in emergency situations especially for people with diabetes, cancer, coronary heart disease, stroke, chronic obstructive pulmonary disease, cognitive impairments, seizure disorders and Alzheimer's as well as people with complex medical device implants, such as pacemakers, stents, joint replacements and organ transplants and who may be unconscious and unable to communicate for themselves while in the operating theatre.

Edible, biodegradable chips could be introduced into the body and used for guided action. Paraplegic persons could have muscular stimuli delivered via an implanted “smart thing” controlled electrical simulation system in order to restore movement functions.

Things are more and more integrated within the human body. It is expected that body area networks can be formed and that they will communicate with treating physicians, emergency services, and humans caring elderly people. An example showing the current state is the completely automated internal Cardioverter-Defibrillator, which is built into the human heart, can autonomously decide on when to administer shocks to defibrillate, and is fully networked such that a MD can follow up on his patient.

2.6 Independent Living (wellness, mobility, monitoring of an aging population)

IoT applications and services will have an enormous impact on independent living and as support for an aging population by detecting the activities of daily living using wearable and ambient sensors, monitoring social interactions using wearable and ambient sensors, monitoring chronic disease using wearable vital signs sensors, and in body sensors.

With emergence of pattern detection and machine learning algorithms, the “things” in a patient’s environment would be able to watch out and care for the patient. Things can learn regular routines and raise alerts or send out notifications in anomaly situations. These services will be merged with the medical technology services, mentioned above.

Attention should be given to the nature of the problem that needs to be solved. Not all human needs can be met with technology alone. Caring for elders is a social issue; hence the technology should foster a community response, such as facilitating communication between individuals, instead of attempting to attend to the issue with technology alone.

2.7 Pharmaceutical

For pharmaceutical products, security and safety is of utmost importance to prevent compromising the health of patients. Attaching smart labels to drugs, tracking them through the supply chain and monitoring their status with sensors has many benefits: Items requiring specific storage conditions, e.g. maintenance of a cool chain, can be continuously monitored and discarded if conditions were violated during transport. Drug tracking and e-pedigrees allow for the detection of counterfeit products and keeping the supply chain free of fraudsters. Counterfeiting is a common practise in this area as illustrated by [20], and affects mostly developing countries.

The smart labels on the drugs can also directly benefit patients, e.g. by storing the package insert, informing consumers of dosages and expiration date, and being assured of the authenticity of the medication. In conjunction with a smart medicine cabinet, that reads information transmitted by the drug labels, patients can be reminded to take their medicine at appropriate intervals and patient compliance can be monitored.

2.8 Retail, Logistics, Supply Chain Management

Implementing the Internet of Things in Retail/Supply Chain Management has many advantages: With RFID-equipped items and smart shelves that track the present items in real time, a retailer can optimize many applications [2], like automatically checking of goods receipt, real time monitoring of stocks, tracking out-of-stocks or the detection of shoplifting.

The savings potential in a retail store is large. For example, sales losses that occur when shelves go empty are estimated to be 3.9% of sales worldwide [3]. Furthermore, the data from the retail store can be used to optimize the logistics of the whole supply chain: If manufacturers know the stock and sales data from retailers, they can produce and ship the right amount of products, thus avoiding over-production and under-production.

The logistic processes from supply chains in many industry sectors can profit from exchanging RFID data, not only those in the retail sector. Moreover, environmental issues can be better tackled, e.g. the carbon footprint of logistics - and supply chains more generally – processes can be optimized based on the availability of dynamic, fine-grained data, collected in the real world directly by (or also retrieved with the help of) some of the "things" (such as trucks, pallets, individual product items, etc., depending on the case).

In the shop itself, IoT offers many applications like guidance in the shop according to a pre-selected shopping list, fast payment solutions like automatically check-out using biometrics, detection of potential allergen in a given product, personalized marketing if accepted, verification of the cool chain, etc. Commercial buildings will of course benefit from smart building functionalities as described above.

2.9 Manufacturing, Product Lifecycle Management (from cradle to grave)

By linking items with information technology, either through embedded smart devices or through the use of unique identifiers and data carriers that can interact with an intelligent supporting network infrastructure and information systems, production processes can be optimized and the entire lifecycle of objects, from production to disposal can be monitored. By tagging items and containers, greater transparency can be gained about the status of the shop floor, the location and disposition of lots and the status of production machines. The fine grained information serves as input data for refined production schedules and improved logistics. Self-organizing and intelligent manufacturing solutions can be designed around identifiable items.

As an object and the attached information processing component may be inseparable, from production to the end of the lifecycle, the history of an item and its current status can be continuously monitored and stored on the tag or in the information system. The data reflects a product's usage history which includes valuable information for product design, marketing and the design of product related services, as well as end-of-life decision-making for safe and environmentally-friendly recycling, re-manufacture or disposal of the product.

2.10 Processing industries - Oil and Gas

The Oil and Gas industry is using scalable architectures that consider possibilities for plug-and-play new ID methods combined with sensing/actuating integrated with Internet of Things infrastructure and integrate the wireless monitoring of petroleum personnel in critical situations (onshore/offshore), container tracking, tracking of drill string components pipes, monitoring and managing of fixed equipment.

A review of high-cost chemical/petrochemical accidents in the UK [4] observed common features in these disasters, such as lack of understanding as well as poor management of storage, process, and chemical segregation. The Internet of Things could help to reduce accidents in the oil and gas industry. For example, containers with hazardous goods can be made *intelligent* by equipping them with wireless sensor nodes.

A possible scenario is that these nodes periodically send information messages about the chemical that is inside the container they are attached to as well as the maximum storage limit of this chemical in the current location. As the nodes have access to a list of incompatible chemicals, they can send out alert messages as soon as they receive an information message from another node that is attached to a container with an incompatible chemical. These alert messages can be then forwarded to a back-end system that, for example, informs the plant manager about the critical situation.

2.11 Safety, Security and Privacy

Wireless identifiable devices are used in different areas to increase safety and security. Some of these are:

- Environment surveillance: earth quakes, tsunami, forest fires, floods, pollution (water and air).
- Building monitoring: water leaks, gases, vibrations, fire, unauthorised entry, vandalism.
- Personnel: mugging alarm, equipment surveillance, payment systems, identity security

When using wireless identifiable smart devices, opportunities and threats could arise from the proliferation of data, the sharing of the data, and from the possibility of snooping via radio. Deciding a common strategy and a policy for future Internet of Things is a priority for the European Commission, which considers that each datum itself in its integral parts is not a threat but this could become a threat when associations are built via accessed databases such that sensitive relationships are revealed or discovered, resulting in damage or potential for damage.

The privacy of citizens has always been in sharp contrast with making humans traceable by tagging them. Despite this, we see some tendencies coming up, where people allow themselves to be tagged with implantable RFID tags in order to distinguish themselves from the crowd, such as illustrated by a implant for VIP customers of the Baja Beach Club in Barcelona. On the other side of the spectrum, we acknowledge that there exist valid usability reasons to implant such a chip, e.g., for chips that can determine the blood sugar level (diabetics), or internal cardioverter-defibrillators for certain patients, curfewed offenders, etc.

Another issue is the 'things' that a government imposes on its citizens to give them access to certain facilities, such as healthcare insurance (wireless medi-cards), the ability to travel (passports with built-in chips) or identification (eID cards or eID/RFID implants). For each of these technologies, the privacy and security impact should be evaluated. On a consumer level, it remains to be investigated how much information can be extracted from consumer electronics with sensors, and to which extent this can be regulated by law. In any case, there's an enormous potential for enhancing the user experience, based on the 'things' in his possession/surrounding.

2.12 Environment Monitoring

Wireless identifiable devices and the utilization of IoT technologies in green related applications and environmental conservation are one of the most promising market segments in the future, and there will be an increased usage of wireless identifiable devices in environmentally friendly programmes worldwide.

Standardisation efforts for RFID and WSNs are considering data rates of up to 1Mb/s, heterogeneous sensor integration and different frequencies. This will open up new applications with positive impacts on society, such as remote data monitoring in disaster scenarios, ubiquitous connectivity for health monitors in body area networks, and wireless broadband for rural areas. Secure communications are also a concern of end users. In the meantime, operators are looking beyond the capital expenditure costs of running RFID networks to minimising operational costs such as power consumption and site costs (installation, integration, maintenance).

2.12 People and Goods Transportation

The IoT offers solutions for fare collection and toll systems, screening passengers and bags boarding commercial carriers as well as the goods moved by the international cargo system that support the aim of governments and the transportation industry, to meet the increasing demand for security in the world.

Every day millions of people move using air, sea and ground transportation systems, taking millions of bags with them. Global trade transports huge quantities of goods through our seaports, airports and railroad stations

Monitoring traffic jams through cell phones of users and using intelligent transport systems (ITS) will improve and make the transportation of goods and people more efficient. Transportation companies would become more efficient in packing containers when those containers can self scan and weigh themselves. This would reduce resource consumption by optimizing the flow of goods in transport.

Applying IoT technologies for managing passenger luggage in airport and airline operations enables automated tracking and sorting, increases per-bag read rates, and increases security.

2.13 Food traceability

This means tracing food or ingredients across the partially or entirely reconstructed supply chain, so that recalls can be issued when quality problems arise. In Europe, food traceability is enforced through EU regulation 178/2002, and in the U.S. it is enforced by the Food and Drug Administration (FDA). Furthermore, efficient food traceability can save lives: In the U.S. for instance, food-borne pathogens are estimated to cause 76 million illnesses and 5,000 deaths each year [5] and societal costs are estimated between $2.9 and $6.7 billion per year [6].

The Internet of Things can aid implementing food traceability, e.g., if RFID is attached to items (item-level tagging) then tracing information can be stored and updated on the items itself. However, producers have concerns about their industrial privacy when using RFID, since competitors could use the information on the RFID tag to gain insight into the supply chain. Therefore, appropriate security methods have to be implemented. An example of such a method is given in [7].

2.14 Agriculture and Breeding

The regulations for traceability of agricultural animals and their movements require the use of technologies like IoT, making possible the real time detection of animals, for example during outbreaks of contagious disease. Moreover, in many cases, countries give subsidies depending on the number of animals in a herd and other requirements, to farms with cattle, sheep, and goats. As the determination of the number is difficult, there is always the possibility of fraud. Good identification systems can help minimize this fraud. Therefore, with the application of identification systems, animal diseases can be controlled, surveyed, and prevented. Official identification of animals in national, intra community, and international commerce is already in place, while at the same time, identification of livestock that are vaccinated or tested under official disease control or eradication is also possible. Blood and tissue specimens can be accurately identified, and the health status of herds, regions, and countries can be certified by using IoT.

With the Internet of Things, single farmers may be able to deliver the crops directly to the consumers not only in a small region like in direct marketing or shops but in a wider area. This will change the whole supply chain which is mainly in the hand of large companies, now, but can change to a more direct, shorter chain between producers and consumers.

2.15 Media, entertainment and Ticketing

Ad-hoc news gathering using the IoT, based on location. In a future scenario, it can be envisaged that news gathering could happen by querying the internet of things, to see which multi-media-capable devices are present at a certain location, and sending them a (financial) offer to collect multimedia footage about a certain event. Near field communication tags can be attached to posters and provide more information by connecting the reader to an URI address, which provides more information related to the poster.

2.16 Insurance

Often the introduction of IoT technology is perceived as a grave invasion of privacy. However, sometimes people are willing to trade privacy for a better service or a monetary benefit. One example is car insurance. If insurance clients are willing to accept electronic recorders in their car, which are able to record acceleration, speed, and other parameters, and communicate this information to their insurer, they are likely to get a cheaper rate or premium [8]. The insurer can save costs by being involved very early when an accident happens and can trigger the most

economic actions. A part of the savings can be given to the customers through discounts on insurance premiums.

The same applies for other assets such as buildings, machinery, etc. that are equipped with IoT technology. In these cases the technology mostly helps to prevent maintenance or allows for much cheaper predictive maintenance before an incident occurs.

2.17 Recycling

IoT and wireless technologies can be used to advance the efficiency and effectiveness of numerous important city and national environmental programmes, including the monitoring of vehicle emissions to help supervise air quality, the collection of recyclable materials, the reuse of packaging resources and electronic parts, and the disposal of electronic waste (RFID used to identify electronic subcomponents of PCs, mobile phones, and other consumer electronics products to increase the reuse of these parts and reduce e-waste). RFID continues to provide greater visibility into the supply chain by helping companies more efficiently track and manage inventories, thereby reducing unnecessary transportation requirements and fuel usage.

Chapter 3
Technologies supporting the Internet of Things vision

As the technology advances, communication and processing capabilities are becoming more and more accessible and versatile; the opportunity for even tighter interconnectivity is fuelling the desire to make use of these possibilities.

In this context, this Section will present the technology areas enabling the Internet of Things and will identify the research and development challenges and outline a roadmap for future research activities to provide practical and reliable solutions. This roadmap will form the basis for the research priorities presented in Chapter 4.

3.1 Identification Technology

The function of identification is to map a unique identifier or UID (globally unique or unique within a particular scope), to an entity so as to make it without ambiguity identifiable and retrievable. UIDs may be built as a single quantity or out of a collection of attributes such that the combination of their values is unique. In the vision of the Internet of Things, things have a digital identity (described by unique identifiers), are identified with a digital name and the relationships among things can be specified in the digital domain.

A unique identifier for an object can translate to a single permanent assigned name for the life of an object. However, IoT will face the need to accommodate multiple identifiers per objects, as well as changes to those identifiers. For example, many objects will have a unique identifier assigned by their manufacturer. Some may also have network addresses (such as IPv6 addresses), as well as temporary local identifiers within transient ad-hoc clusters of objects. Objects may also have sensors and actuators physically attached to them, with each of these sensors and actuators also being individually addressable; their identifiers may be constructed as extensions of the ID of the object or perhaps associated with the object's identifier via a lookup in a registry. Many objects may be composite objects or products that consist of replaceable parts that are exchanged during the usage phase or lifetime of the object. These parts may also have their own unique identifiers and it is important that the information models for the IoT allow changes of identifier, changes of configuration and associations between identifiers to be recorded and queried, both in terms of keeping track of changes to parent-child relationships as well as old-new relationships (e.g. where a new part is installed to replace an old part that is worn or faulty). Further examples of associations between identifiers include the breakdown of large quantities of bulk product (e.g. a specific batch of food product) into a number of individual products or packages for retail purposes, repackaging and re-labelling of products, aggregation of ingredients, components and parts to form composite products and assemblies or kits, such as medical kits.

Combinations of things will create “family tree” identification schemes where parts and components that are incorporated within composite/complex products such as computers, vehicles, and buildings have many different components, each with their own unique ID and life history. This is also referred to as a serialised Bill of Materials. This is necessary in order to track sets of different objects (e.g. parents or children of the original object) and the framework for expressing data sharing rules needs to be able to support this.

By assigning each thing participating in the Internet of Things a unique identity (UID) or potentially several unique identities, it is possible to refer to each thing as an individual, each having its own characteristics, life history and information trail, its own flow pattern through the real world and its own sequence of interactions with other things. It is important that such unique identifiers for things can be globally unique and can have significant consistency and longevity (ideally for the life of the thing), independent of the current location of the thing or

the current network connectivity available to the thing, in order that it is possible to gather information about a thing even when that information is collected and owned by a number of different entities and fragmented across a large number of databases and information systems.

Many things can be considered to be (at least at the time of their creation) near-identical replicas of each other, perhaps belonging to the same product type and sharing a number of properties common to all instances within the same class of things. Often, a request or order for a particular thing might not always specify the exact unique ID that must be retrieved; instead the request can be satisfied by any thing that is a member of a particular class. It is therefore important that the Internet of Things can support unique identifiers in a way that it is also possible to refer to a particular class of things as well as individual things within that class, in order to be able to retrieve or refer to class-level information and services provided for the class of things as well as serial-level information and services provided for each individual thing.

It is also important that citizens, companies and other organisations can construct unique identifiers for things as easily, affordably and autonomously as they can create unique identifiers for web pages and other internet resources, while ensuring that no two entities can claim to be the authoritative creator of the same unique ID. In the existing Internet, this is typically achieved through hierarchical identifier structures, in which each tier of the hierarchy is only responsible for ensuring uniqueness among the members of the tier below. Familiar examples of such hierarchically structured identifiers include telephone numbers, URIs, Internet hostnames and sub domains, handles, digital object identifiers etc. It would be important to accommodate more than a single hierarchical name space; perhaps some classes of “things” would have their own namespace, such as the World Wide Web using the class “IN” [17] whose namespace is managed by ICANN. Other ways that a namespace can be described would be as a dominion or a realm.

However, there can be good reasons why the Internet of Things should also support 'opaque' identifiers and pseudonyms, in which the internal structure of hierarchy is not readily apparent; this is particularly important when unauthorised parties are able to read the class information (e.g. product type or object type) and could jeopardise the privacy of a citizen or the safety and security of supply chains, subjecting them to discriminatory treatment or targeted attack, on the basis of what the identifier reveals about the things which are being worn, carried or transported. There could be an opaque identifier namespace that is not part of the hierarchical namespace structure and reveals absolutely no information about the object that it is identifying. For example, this could have applications in uniquely identifying the medication that a patient is carrying, especially when using wireless identification technologies that lack adequate privacy measures.

We recognise that many industry sectors have already begun assigning unique identifiers to objects and that significant investment has been made in information systems and collection of information about various kinds of things, using those existing unique identifiers as keys to lookup and retrieve that information. Such established UIDs are difficult to displace and it is therefore critical for successful deployment that IoT technology can support such existing UIDs, using mapping processes where necessary.

Furthermore, as indicated in ISO 15459, multiple established name issuing authorities exist and it is important that the Internet of Things recognises their legitimate but non-exclusive involvement in the construction of unique identifiers for things and in helping to manage delegation of uniqueness of the identifiers created by their members, each of whom is thereby granted the autonomy to create unique identifiers within their own namespace; it should also be possible for anyone to use Uniform Resource Identifiers (URI) as unique identifiers for things.

It is important to understand that identifiers can refer to names and addresses, but since there can be multiple addresses of information and services related to an individual thing, it is probably more helpful to ensure that each thing is given a unique name and to use lookup mechanisms and referral services to obtain addresses of information and services, including those provided authoritatively by the thing's creator and those contributed by others who have interacted with the thing at some time in its life. In the case of the existence of multiple identifiers for a single object due to different reasons a scheme for ID data translation and dynamic compatibility/interoperability check is necessary.

Furthermore, it is important that identifiers are not constrained by current choices of technology for storing and communicating unique identifiers or their current limitations, since we should expect that the data carrier technology will evolve over time and current limitations (such as those on memory capacity available for identifiers) will become more relaxed.

Today various unique identifier schemes exist and interoperability is required between applications using different schemes when those applications are operated in the Future Internet environment.

The traffic in the Internet of Things networks for queries about unique identifiers will be many times higher than that for DNS queries in the current Internet.

In this context the Internet of Things deployment will require the development of new technologies that need to address the global ID schemes, identity management, identity encoding/encryption, authentication and repository management using identification and addressing schemes and the creation of global directory lookup services and discovery services for Internet of Things applications with various unique identifier schemes.

3.2 Internet of Things Architecture Technology

In Service Oriented Architectures (SOA) it becomes imperative for the providers and requestors to communicate meaningfully with each other despite the heterogeneous nature of the underlying information structures, business artefacts, and other documents. This requirement is termed as semantic interoperability. Often technology is perceived to be the biggest impediment to effective collaboration and integration between requestors and providers; however it is usually the problem of semantic interoperability which is the root cause. Semantic interoperability can be achieved between heterogeneous information systems (service providers and service requestors) in a multitude of ways. On one extreme, development of comprehensive shared information models can facilitate semantic interoperability among the participant applications and businesses. However, the problem with this approach is its rigidity, which translates to inflexibility when it comes to business processes leveraging SOA. On the other extreme, semantic interoperability can be achieved by providing appropriate semantic mediators (translators) at each participant's end, to facilitate the conversion to the information format which the participant understands. Most often systems use a combination of context independent shared information models, coupled with context specific information specialization approaches to achieve semantic interoperability.

Scalability, modularity, extensibility and interoperability among heterogeneous things and their environments are key design requirements for the Internet of Things, in order to ensure an open playing field for solution providers and developers, while users also benefit from a competitive marketplace of solutions, from which applications can be assembled.

As things move and interact with their environment, events are automatically generated. These events can subsequently be enhanced with additional semantic information that expresses the context in which each event happened, to explain why something occurred, such as why a thing was observed at a location or how and why it interacted with another thing. There is considerable scope for further research and innovation regarding novel methods of automatically interpreting events, adding semantic annotation and even predicting what will happen next and what precautionary measures should be taken. Architecture standards for the IoT should support the unambiguous communication of events and additional semantic information, without prescribing the implementation details of how they are generated.

The decentralised and heterogeneous nature of things and the entities with which they interact requires a scalable, flexible, open, layered, event-driven architecture of standards that minimises or eliminates any bias towards any single programming language, operating system, information transport mechanism or other technology and makes efficient use of available network connectivity and energy, where required.

When architecting the Internet of Things, it is important to remember that many things will not have permanent network connectivity - indeed some things may have no intrinsic network connectivity, but rely on supporting intelligence in their local environment or in remote information systems. Things will therefore need the ability to communicate their location, state and requirements to information systems that have more permanent or more reliable

network connectivity. Through such information systems, a digital counterpart of the thing can be monitored or even displayed in a virtual representation, such that remote authorized entities could query or update the state of an individual thing or influence its destiny. There is therefore a need for the IoT architecture to provide effective caching and synchronisation of information updates in both directions, to support things and application scenarios that lack reliable permanent network connectivity. For example, there may be environments (such as the interior of an aircraft cabin) where network connectivity is not available either because of non-availability, electromagnetic interference or concerns about potential disruption to other mission-critical or safety-critical systems, such as the flight control system and internal communications infrastructure of an aeroplane.

Handheld devices might be used by maintenance mechanics and inspectors for retrieving lifecycle history information about an individual aircraft part, especially when it is mounted behind a panel or in an otherwise inaccessible plate. Handheld devices might also be used by cabin crew during aircraft turnaround operations, to rapidly check that all required safety equipment (life jackets, oxygen masks, fire extinguishers) are present and correct and not misplaced. In such scenarios, one can envisage pre-positioning onto the handheld device the information about the expected manifest of safety equipment or details about the complete maintenance history of each part known to be installed on that specific aircraft, such that the pre-cached information is immediately available at the time and place of interaction with the object. The memory of the handheld device can also be used to temporarily record any updates, such as modifications to the parts, symptoms observed, missing safety equipment, etc., so that those updates can be synchronised to the network as soon as the hand-held device returns within range of network connectivity, such as WiFi or a docking station.

The architecture for the IoT should support distributed ownership of data, in which entities (and things) can control which information to share with other things and entities. Subject to authorisation controls, the architecture should also support mechanisms for gathering fragments of distributed information from a variety of sources, even when those sources are not known a priori, in order to achieve comprehensive end-to-end traceability as far as is permitted.

In the context of SOA, many practical approaches to semantic interoperability have been proposed and used with different levels of success. We shall be concerned primarily with the following four practical approaches:

- Vertical domain cantered business vocabularies,
- Horizontal Canonical Cross-Vertical frameworks like ebXML, UBL etc.,
- Semantic Web based ontological frameworks, and
- Semantic mediators.

Each vertical domain of business applications has various types of peculiarities specific to the domain warranting the development of a specialized shared vocabulary of business processes and documents. At the same time, it is also observable that various types of business concepts and data types are common across multiple verticals necessitating the development of cross-domain vocabularies and processes so that they can be captured in a domain-independent manner. Common artefacts falling into this category are:

- Business concepts, data and documents like purchase orders, shipping notices/dispatch advice, etc.
- Process, workflow, choreography etc. including exception handling
- Contracts, trust, roles, permissions etc.

The third truly dynamic category of business processes in SOA fall under the dynamic category. Dynamic SOA based business processes operate on the “publish-find-bind” paradigm principle, where business processes may dynamically involve business partners and associated applications. The problem of semantic interoperability is far more acute in such dynamic situations involving service brokers, due to the lack of prior business relationships between the enterprises.

Industry practitioners have suggested leveraging work in the semantic web to devise comprehensive and open ontologies to address the issue of semantic interoperability for dynamic binding based SOA.

Issues to be addressed:

- Distributed open architecture with end to end characteristics, interoperability of heterogeneous systems, neutral access, clear layering and resilience to physical network disruption.
- Decentralized autonomic architectures based on peering of nodes.
- Cloud computing technology, event-driven architectures, disconnected operation and synchronization

3.3 Communication Technology

The applications of Internet of Things form an extensive design space with many dimensions that include:

- Deployment – onetime, incremental or random
- Mobility – occasional or continuous performed by either selected or all "things" in the selected environment.
- Cost, size, resources, and energy – very resource limited to unlimited
- Heterogeneity – a single type of "thing" or diverse sets of differing properties and hierarchies
- Communication modality – Electromagnetic communication - radio frequency, optical, acoustic, inductive and capacitive coupled communication have been used
- Infrastructure – different applications exclude, allow or require the use of fixed infrastructure
- Network topology – single hop, star, multihop, mesh and/or multitier
- Coverage – sparse, dense or redundant
- Connectivity – continuous, occasional or sporadic
- Network size – ranging from tens of nodes to thousands
- Lifetime – few hours, several months to many years
- Other quality of service requirements – real time constraints, tamper resistance, un obtrusiveness,

An extensive design space complicates IoT application development in various ways. One could argue that designing for the most restrictive point in the design space, e.g. minimum "thing" capabilities, highly mobile, etc. might be a solution. However, often there is no such global "minimum" and it will be desirable to exploit the characteristics of the various points in the design space. This implies that no single hardware and software platform will be sufficient to support the whole design space and heterogeneous systems will be used.

Issues to be addressed:

- Internet of Things energy efficient communications
- Multi frequency radio front ends and protocols,
- Communication spectrum and frequency allocation
- Software defined radios (SDRs)
- Cognitive radios (CRs)
- Energy efficient wireless sensor networks with inter protocol communication capabilities (hybrids i.e, ZigBee-6LoWPAN-WiFi, etc.)

3.4 Network Technology

The IoT deployment requires developments in network technology which is essential for implementing the vision reaching out to objects in the physical world and to bring them into the Internet. RFID, short-range wireless technologies and sensor networks are enabling this, while for example IPv6, with its expanded address space, allow that all things can be connected, and can be tracked.

In the IoT security, scalability, and cross platform compatibility between diverse networked systems will be essential. In this context the network technologies has to offer solutions that reduced costs that can offer the viability of connecting almost anything to the network, and this ubiquity of access will change the way information is processed. IP provides today end to end communication between devices, without intermediate protocol translation gateways.

Protocol gateways are inherently complex to design, manage, and deploy and with the end to end architecture of IP, there are no protocol translation gateways involved.

New scalable architectures designed specifically for the ubiquitous sensor networks communications will allow for networks of billions of devices. Improvements in techniques for secure and reliable wireless communication protocols will enable mission-critical applications for ubiquitous sensor networks based on wireless identifiable devices.

Issues to be addressed:

- Network technologies (fixed, wireless, mobile etc.),
- Ad-hoc networks

3.5 Network Discovery

In the IoT the network will dynamically change and continuously evolving and the things feature varying degrees of autonomy. New “things” will be added and existing network topologies will be moved around. In the context of IoT automated discovery mechanisms and mapping capabilities are essential to network management and needed for overall communication management. Without it the network management capabilities cannot scale, be accurate or efficient since ti needs to automatically assign roles to devices based on intelligent matching against pre-set templates and attributes, automatically deploy and start active, passive or performance monitors based on assigned roles and attributes, start, stop, manage and schedule the discovery process and make changes to any role or monitoring profile at any time or create new profiles as required

They enable interaction between devices that is not pre-configured and hard coded as far as the addresses or service end-points are concerned, but allows for dynamic, run-time configuration of connections. This allows the (potentially mobile) devices to form collaborative groups and adapt to changing context. Examples for protocols for discovery on LAN level are WS-Discovery [9] (as part of WS-DD), Bonjour [10] and SSDP [11] (as part of UPnP).

Passive or dynamic discovery mechanisms exist today and technologies are developed to implement both active and passive real time, dynamic network discovery data.

Discovery services must nevertheless be based on authentication mechanisms to address privacy or security issues.

3.6 Software and algorithms

One of the most promising micro operating systems for constrained devices is Contiki [12]. It provides a full IP stack (both IPv4 and IPv6), supports a local flash file system and features a large development community and a comprehensive set of development tools.

One of challenges in building IoT applications lies in the lack of a common software fabric underlying how the software in the different environments can be combined to function into a composite system and how to build a coherent application out of a large collection of unrelated software modules. Research and development is focusing on service oriented computing for developing distributed and federated applications to support interoperable machine to machine and “thing” to “thing” interaction over a network. This is based on the Internet protocols, and on top of that, defines new protocols to describe and address the service instance. Service oriented computing loosely organizes the Web services and makes it a virtual network.

Issues to be addressed:

- Open middleware platforms
- Energy efficient micro operating systems
- Distributed self adaptive software for self optimization, self configuration, self healing (e.g. autonomic)
- Lightweight and open middleware based on interacting components/modules abstracting resource and network functions;

- Bio-inspired algorithms (e.g. self organization) and game theory (to overcome the risks of tragedy of commons and reaction to malicious nodes)
- Self management techniques to overcome increasing complexities
- Password distribution mechanisms for increased security and privacy
- Energy-aware operating systems and implementations

3.7 Hardware

The research on nanoelectronics devices will be used for implementing wireless identifiable systems with the focus on miniaturization, low cost and increased functionality.

Polymers electronics technology will be developed and research is needed on developing cheap, non-toxic and even disposable electronics for implementing RFID tags and sensors that include logic and analogue circuits with n and p type Thin Film Transistors (TFTs), power converters, batteries, memories, sensors, active tags.

Figure 4 IoT Devices

Silicon IC technology will be used for systems with increased functionality and requirements for more non volatile memory used for sensing and monitoring ambient parameters. Research is needed on ultra-low power, low voltage and low leakage designs in submicron RF CMOS technologies, on high-efficiency DC-DC power-management solutions, ultra low power, low voltage controllable non-volatile memory, integration of RF MEMS and MEMS devices. The focus will be on highly miniaturised integrated circuits that will include:

- Multi RF, adaptive and reconfigurable Front Ends
- HF/UHF/SHF/EHF
- Memory –EEPROM/FRAM/Polymer
- ID 128/256 bits + other type ID
- Multi Communication Protocols
- Digital Processing
- Security, including tamper-resistance countermeasures, and technology to thwart side-channel attacks

Based on this development two trends are emerging for wireless identifiable devices for IoT applications:

- Increasing use of “embedded intelligence”
- Networking of embedded intelligence

IoT will create new services and new business opportunities for system providers to service the communication demands of potentially tens of billions of devices. Three main trends are seen today:

- Ultra low cost tags with very limited features. The information is centralized on data servers managed by service operators. Value resides in the data management.
- Low cost tags with enhanced features such as extra memory and sensing capabilities. The information is distributed both on centralized data servers and tags. Efficient network infrastructure. Value resides in communication and data management, including processing of data into actionable information.
- Smart fixed/mobile tags and embedded systems. More functions into the tag bringing local services. Smart systems (sensing/monitoring/actuating) on tags. The information is centralized on the data tag itself. Value resides in the communication management to ensure security and effective synchronisation to the network.

Smart devices enhanced with inter-device communication will result in smart systems with much higher degrees of intelligence and autonomy. This will enable the more rapid deployment of smart systems for IoT applications and creation of new services.

3.8 Data and Signal Processing Technology

Different industry bodies in vertical domains have realized the utility of XML as the underlying language for standardization of business artefacts. Each vertical industry has come up with standards bodies to develop XML standards for the specific vertical. The basic idea is to express the contract, trust, process, workflow, message, and other data semantics in terms of XML nodes and attributes for the nodes. These XML vocabularies are then published as generalized Document Type Definition (DTD) or XML Schema for consumption by members of that vertical industry. Since all members follow the same DTD or schema the semantic interoperability is achieved.

The OASIS (Organization for the Advancement of Structured Information Standards) site [13] or the XML cover pages [14] site provides a comprehensive list of XML vocabularies. Some of the prominent vertical vocabularies are ACORD for insurance, OTA for travel, GovML for Government, FpML for financial derivatives, HL7 for healthcare domain, STPML for financial straight-through processing, etc. Some of these standardized vocabularies are already in action and have seen widespread adoption. A case in point is the adoption of XBRL, the standard for business and financial reporting. It has been popularly adopted by many corporations in addition to financial and reporting software companies.

Initiatives such as International Standard for Metadata Registries (ISO/IEC 11179) and implementations of it, such as the Universal Data Element Framework (UDEF) from OpenGroup aim to support semantic interoperability between structured data that is expressed using different schema and data dictionaries of vocabularies, by providing globally unique cross-reference identifiers for data elements that are semantically equivalent, even though they may have different names in different XML markup standards.

ebXML is an end-to-end stack proposed under the aegis of UN/CEFACT (United Nations Centre for Trade Facilitation and Electronic Business) and OASIS, aimed at standardizing B2B collaborations. The stack of ebXML derives its fundamentals from Electronic Data Interchange (EDI), the existing de-facto technology for conducting e-business between multiple business partners. It is envisioned to enable enterprises of any size, anywhere, to find each other electronically and conduct business by exchanging XML messages. It builds on earlier semantic approaches to business vocabularies like XML Common Business Library (xCBL) from Commerce One, and business object documents (BODs) from Open Applications Group.

ebXML offers an open XML based framework for enterprises to conduct business electronically with other enterprises or with customers. In effect it is a collection of standards for conducting e-business. The semantics in ebXML stack are handled at two levels: Core Components at the data dictionary level and UBL for the standardized business documents level.

A Core Component (CC) is a generic term referring to a semantic data item that is used as a basis for constructing electronic business messages. The Core Components specification addresses the need for capturing data items common across multiple businesses and domains. A layered approach is taken with provision of specialization of components based on context (Context refers to the environment in which the data item is used). There are two basic types of Core Components: (a) Basic Core Component – A simple, singular Core Component that

has an indivisible semantic meaning like an item code, an ID, etc., and (b) Aggregate Core Component – A collection or packaged Core Component like an address.

On the other hand, Universal Business Language (UBL) is an output of OASIS to address the development of reusable semantic business documents for interoperability across multiple businesses and verticals. Core Components specifies two broad categories of elements, the Core Components and the Business Information Entities (BIE). UBL is concerned with only the BIEs (both Basic BIEs and Aggregate BIEs).

Finally, semantic web based standards from W3C like DAML (Darpa Agent Markup Language), RDF (Resource Description Framework) and OWL (Ontology Working Language) are useful in providing semantic foundations for dynamic situations involving dynamic discovery of businesses and services.

The intelligent decision-making algorithms will need to trigger activities not on the basis of a single event (such as an individual observation or sensor reading) but often also considering correlations among events and often requiring transformation of the raw sensor data. Toolkits and frameworks already exist for complex event processing, such as ESPER and DROOLS - and are likely to play a useful role in formulating machine-readable rules for how a particular sequence of events should trigger a particular activity or process.

It may be necessary to evaluate multiple rules in parallel, to consider various possible causes and appropriate responses or outcomes. Sensor data in particular may require some pre-processing, to reduce noise, assess whether or not to consider outlying data points, perform smoothing, averaging (possibly across moving time windows). Furthermore, certain kinds of sensor data may need to be transformed.

For example, from temperature data together with knowledge of the biological and chemical reactions of a perishable product, it may be possible to calculate whether the population of toxic micro-organisms has reached a safety-critical level; the growth rate of the microbe population may have non-linear temperature dependence. As another example, it is necessary to apply techniques such as Fourier transforms and complex cepstrums (the inverse Fourier transform of the complex logarithm of a Fourier transform) to vibration data in order to detect changes in the amplitude of vibrating components at particular resonant frequencies, as well as changes in the relative amplitudes of harmonics of such frequencies; by transforming the sensor data in such ways, it is possible to detect signs of degradation, instability or imbalance with much greater sensitivity, leading to a much earlier detection of possible problems.

Issues to be addressed:

- Semantic interoperability, service discovery, service composition, semantic sensor web,
- Data sharing and collaboration,
- Autonomous agents,
- Human machine interaction
- Edge processing, filtering and aggregation,
- Quality of service, stream processing

3.9 Discovery and Search Engine Technologies

Information and services about things will be fragmented across many entities and may be provided at class-level (i.e. common information and services for all instances of things having the same class) or at serial-level (i.e. unique to an individual thing), as well as being provided authoritatively by the creator of the thing or contributed by other entities such as those who have interacted with an individual thing at some stage in its life.

The Internet of Things requires the development of lookup / referral services to link things to such information and services and to support secure access to such information and services in a way that respects both the privacy of individuals and confidentiality of business information, such that matching between requesters and providers of information services can be founded on trust relationships. As a thing moves through the real world, it will encounter new environments and both the smart things and other agents that are monitoring the things will require lookup mechanisms in order to discover what capabilities are available within the local environment of the thing. Such capabilities may include availability of sensors and actuators, network communication interfaces, facilities for computation and processing of

data into information as well as facilities for onward transportation, handling, physical processing or alerting of a human operator about problems.

Things may also require the ability to discover the existence and identity of peer things within their environment in order to negotiate about shared goals (such as common requirements for transportations and destinations, specific handling or storage requirements, e.g. within particular temperature ranges), and in order to identify and resolve conflicts and achieve efficient, synergistic and considerate solutions with their peers for their co-location and co-transportation, especially when they plan to interact with actuators in their local environment or request transportation. Requesters of information, including the virtual counterparts of things will often need to be able to monitor the location of things. Locations might be expressed as abstract or 'logical' locations, perhaps within a hierarchy or federation of hierarchical locations. They can also be expressed as 3-dimensional terrestrial spatial location co-ordinates.

Some applications in the Internet of Things may need to be able to understand both concepts of location and to access mechanisms for relating logical locations to spatial locations and vice versa, as well as understanding geometric concepts such as intersection and overlap of locations and location boundaries. This is particularly important for the interpretation of sensor data when the available sensors are located at a distance from the thing that is being monitored, since properties such as temperature might not have reached equilibrium between the location of the thing and the location of ambient sensors in the environment.

The Internet of Things will also require the ability for things or the entities that are responsible for them to make assertions about the state of an object in such a way that other things and other entities can discover these assertions about the state of each individual object or the class to which it belongs. For example, an assertion might be made about an event relating to an individual thing such as whether it has been sold, destroyed, lost, found, marked for recall, returned. Assertions might also be made about a class of things, such as reviews, ratings, recommendations, helpful tips and advice or the availability of new services, updates and extensions/capabilities for the things, such as new software or firmware. Additionally assertions can be made about identity of a thing or its relationship with other things, such as assertions about being a peer within a federation of things.

Issues to be addressed:

- Device discovery, distributed repositories
- Positioning and localisation
- Mapping of real, digital and virtual entities
- Terrestrial mapping data

3.10 Relationship Network Management Technologies

The IoT requires managing networks that contains billons of heterogeneous “things”, and where a wide variety of software, middleware and hardware devices exists. Network management technologies cover a wide area of elements including, security, performance and reliability.

Network management involves distributed databases, repositories, auto polling of network devices, and real time graphical views of network topology changes and traffic. The network management service employs a variety of tools, applications, and devices to assist monitoring and maintaining the networks involved in the IoT applications.

Similar to the social network services that are flourishing today on the web, there would be a need for things to form relationships with one another on the networks. These relationships can be formal and official, such as membership within a federation, or they could be loosely based alliances brought upon by an incident or an event.

Issues to be addressed:

- Propagation of memes [18] by things
- Identity, relationship and reputation management

3.11 Power and Energy Storage Technologies

The autonomous “things” operating in the IoT applications and performing either the sensing or monitoring of required changes/events need power, to perform the required job.

Micro batteries with enough energy to power the “things” for their lifespan, and energy scavenging technologies that let the “things” collect power from their operating environment are used today.

Since that environment has wide variations, depending on where and how the “thing” is used, the power collection methods vary (RF, solar, sound, vibration, heat, etc.).

The “things” with local power may not use it to send the information, saving power by letting a reader power the transmission. For situations and locations where is it reasonable to have a lot of “things” with sensing capabilities, spaced fairly evenly, mesh networks become a way to increase the communication and power efficiency by including the ability to forward transmissions from the closest “thing”. The reader then only needs to be range of the edge of the network.

Power and energy storage technologies are enabalers for the deployment of IoT applications. These technologies has to provide high power density energy generation and harvesting solutions that, when used with today’s low power nanoelectronics, enables a self□powered intelligent sensor based wireless identifiable device.

To meet the IoT application’s power requirements, a typical energy generation/harvesting units contains four main building blocks the harvester, the conversion electronics, the energy storage, and the energy delivery.

Issues to be addressed:

- Battery and energy storage technologies
- Energy harvesting technologies
- Energy consumption mapping; the power technology should allow for fine-grained measurement/estimation of hardware components in the ‘thing’, such that energy-based priority scheduling software can work.

3.12 Security and Privacy Technologies

Two of the main issues in the IoT are privacy of humans and confidentiality of business processes. Because of the scale of deployment, their mobility and sometimes their relatively low complexity, the cloud of ‘things’ is hard to control.

For confidentiality, established encryption technology exists, and one of the challenges is to make encryption algorithms faster and less energy-consuming. Moreover, any encryption scheme will be backed up by a key distribution mechanism.

For small-scale systems, key distribution can happen in the factory or at deployment, but for ad-hoc networks, novel key distribution schemes have only been proposed in recent years.

For privacy, the situation is more serious; one of the reasons is the ignorance (regarding privacy) of the general public. Moreover, privacy-preserving technology is still in its infancy: the systems that do work are not designed for resource-restricted devices, and a holistic view on privacy is still to be developed (e.g, the view on privacy throughout one’s life).

The heterogeneity and mobility of ‘things’ in the IoT will add complexity to the situation. Also from a legal point of view, some issues remain far from clear and need legal interpretation; examples include the impact of location on privacy regulation, and the issue of data ownership in collaborative clouds of ‘things’.

Figure 5 IoT Security and Privacy

Network and data anonymity can provide a basis for privacy, but at the moment, these technologies are mainly supported by rather powerful equipment, in terms of computing power and bandwidth. A similar argument can be made for authentication of devices and establishing trust.

Issues to be addressed:

- Event-driven agents to enable an intelligent/self aware behaviour of networked devices
- Privacy preserving technology for heterogeneous sets of devices
- Models for decentralised authentication and trust
- Energy efficient encryption and data protection technologies
- Technologies for object and network authentication
- Anonymity mechanisms
- Security and trust for cloud computing
- Data ownership

3.13 Standardisation

Standards should be designed to support a wide range of applications and address common requirements from a wide range of industry sectors as well as the needs of the environment, society and individual citizens.

Through consensus processes involving multiple stakeholders, it will be possible to develop standardized semantic data models and ontologies, common interfaces and protocols, initially defined at an abstract level, then with example bindings to specific cross-platform, cross-language technologies such as XML, ASN.1, web services etc.

The use of semantic ontologies and machine-readable codification should help to overcome ambiguities resulting from human error or differences and misinterpretation due to different

human languages in different regions of the world, as well as assisting with cross-referencing to additional information available through other systems.

Standards are required for bidirectional communication and information exchange among things, their environment, their digital counterparts in the virtual cloud and entities that have an interest in monitoring, controlling or assisting the things.

In addition, the design of standards for the Internet of Things needs to consider efficient and considerate use of energy and network capacity, as well as respecting other constraints such as those existing regulations that restrict permitted frequency bands and power levels for radio frequency communications. As the Internet of Things develops, it may be necessary to review such regulatory constraints and investigate ways to ensure sufficient capacity for expansion, such as seeking additional radio spectrum allocation as it becomes available.

A particular challenge in this regard is ensuring global interoperability particularly for things and devices that make use of radio spectrum. Historically, various bands of radio spectrum have been allocated for various purposes, such as broadcast communications (AM, FM, digital audio broadcasting, analogue terrestrial television, digital terrestrial television), mobile telephony, citizen-band radio, emergency services communications, wireless internet, short-range radio. Unfortunately, the frequency band allocations are not exactly harmonised across all regions of the world and some bands that are available for a particular purpose in one region are not available for the same purpose in another region, often because they are being used for a different purpose.

Re-allocation of radio spectrum is a slow process, involving government agencies, regulators and international bodies such as the International Telecommunications Union (ITU) as well as regional bodies such as the European Telecommunications Standards Institute (ETSI) or the Federal Communications Commission (FCC). Careful discussions are needed to minimise disruption to existing users of radio spectrum and to plan for future needs. In the meantime, many IoT devices using radio spectrum will need to be capable of using multiple protocols and multiple frequencies. An example of this is the ISO 18000-6C/EPCglobal UHF Gen2 standard, which is implemented using slightly different frequencies within the 860-960 MHz band, depending on the region of operation, as well as different power levels and different protocols (at least initially in Europe, where the Listen-Before-Talk protocol was required).

Issues to be addressed:

- IoT standardisation
- Ontology based semantic standards
- Standards for communication within and outside cloud

Chapter 4
Internet of Things Research Agenda, Timelines and Priorities

4.1 Identification Technology

Further research is needed in the development, convergence and interoperability of technologies for identification and authentication that can operate at a global scale. This includes the management of unique identities for physical objects and devices, and handling of multiple identifiers for people and locations and possible cross-referencing among different identifiers for the same entity and with associated authentication credentials.

Frameworks are needed for reliable and consistent encoding and decoding of identifiers, irrespective of which data carrier technology that is used (e.g. whether linear or 2-D barcode, RFID, memory button or other technologies, including those that may be developed in the future. For some applications, it may be necessary to use encrypted identifiers and pseudonym schemes in order to protect privacy or ensure security. Identifiers play a critical role for retrieval of information from repositories and for lookup in global directory lookup services and discovery services, to discovery the availability and find addresses of distributed resources.

It is vital that identification technology can support various existing and future identifier schemes and can also interoperate with identifier structures already used in the existing Internet and World Wide Web, such as Uniform Resource Identifiers (URIs).

Further research is needed in development of new technologies that address the global ID schemes, identity management, identity encoding/encryption, pseudonimity, (revocable) anonymity, authentication of parties, repository management using identification, authentication and addressing schemes and the creation of global directory lookup services and discovery services for Internet of Things applications with various unique identifier schemes.

4.2 Internet of Things Architecture Technology

The Internet of Things needs an open architecture to maximise interoperability among heterogeneous systems and distributed resources including providers and consumers of information and services, whether they be human beings, software, smart objects or devices. Architecture standards should consist of well-defined abstract data models, interfaces and protocols, together with concrete bindings to neutral technologies (such as XML, web services etc.) in order to support the widest possible variety of operating systems and programming languages.

The architecture should have well-defined and granular layers, in order to foster a competitive marketplace of solutions, without locking any users into using a monolithic stack from a single solution provider. Like the internet, the IoT architecture should be designed to be resilient to disruption of the physical network and should also anticipate that many of the nodes will be mobile, may have intermittent connectivity and may use various communication protocols at different times to connect to the IoT.

IoT nodes may need to dynamically and autonomously form peer networks with other nodes, whether local or remote and this should be supported through a decentralised, distributed approach to the architecture, with support for semantic search, discovery and peer networking. Anticipating the vast volumes of data that may be generated, it is important that the architecture also includes mechanisms for moving intelligence and capabilities for

filtering, pattern recognition, machine learning and decision-making towards the very edges of the network to enable distributed and decentralised processing of the information, either close to where data is generated or remotely in the cloud. The architectural design will also need to enable the processing, routing, storage and retrieval of events and allow for disconnected operations (e.g. where network connectivity might only be intermittent). Effective caching, pre-positioning and synchronisation of requests, updates and data flows need to be an integral feature of the architecture. By developing and defining the architecture in terms of open standards, we can expect increased participation from solution providers of all sizes and a competitive marketplace that benefits end users.

Issues to be addressed:

- Distributed open architecture with end to end characteristics, interoperability of heterogeneous systems, neutral access, clear layering and resilience to physical network disruption.
- Decentralized autonomic architectures based on peering of nodes.
- Architectures moving intelligence at the very edge of the networks, up to users' terminals and things.
- Cloud computing technology, event-driven architectures, disconnected operations and synchronization.
- Use of market mechanisms for increased competition and participation

4.3 Communication Technology

Billions of connected devices are pushing current communication technologies, networks and services approaches to their limits and require new technological investigations. Research is required in the field of Internet architecture evolution, wireless system access architectures, protocols, device technologies, service oriented architecture able to support dynamically changing environments, security and privacy. Research is required in the field of dedicated applications integrating these technologies within a complete end to end system.

In the Internet of Things the following topics related to communication technology have to be considered:

- Communication to enable information exchange between "things" and between "things" and Internet
- Communication with sensors for capturing and representing the physical world in the digital world
- Communication with actuators to perform actions in the physical world triggered in the digital world
- Communication with distributed storage units for data collection from sensors, identification and tracking systems
- Communication for interaction with humans in the physical world
- Communication and processing to provide data mining and services
- Communication for localization and tracking for physical world location determination and tracking
- Communication for identification to provide unique physical object identification in the digital world

In the IoT the range of connectivity options will increase exponentially and the challenges of scalability, interoperability and ensuring return on investment for network operators will remain.

In this context the communication needs will change and new radio and service architectures will be required to cater for the connectivity demands of emerging devices. The frequency spectrum will have to be adapted to the new bandwidth requirements.

Issues to be addressed:

- Internet of Things energy efficient communication multi frequency protocols, communication spectrum and frequency allocation.
- Software defined radios to remove need for hardware upgrades when new protocols emerge.
- Connectionless communications, even beyond IP.

- High performance, scalable algorithms and protocols

4.4 Network Technology

The evolution and pervasiveness of present communication technologies has promised to revolutionize the way humans interact with their environment. The Internet of Things is born from this vision in which objects form an integral part of the communication infrastructures that wire today's world. For this vision to be realized, the Internet of Things architecture needs to be built on top of a network structure that integrates wired and wireless technologies in a transparent and seamless way. Wireless network technologies have gained more focus due to their ability to provide unobtrusive wire-free communication. They have also become the leading area of research when combined with data collecting technologies used for environmental and object monitoring.

In this regard, wireless sensor networks promise low power, low cost object monitoring and networking, constituting a fundamental technology for the evolution towards a truly embedded and autonomous Internet of Things.

Research is needed on networks on chip technology considering on chip communication architectures for dynamic configurations design time parameterized architecture with a dynamic routing scheme and a variable number of allowed virtual connections at each output).

Scalable communication infrastructure on chip to dynamically support the communication among circuit modules based on varying workloads and/or changing constraints.

Power aware networks that turned on and off the links in response to bursts and dips of traffic on demand.

IP provides today the protocol for implementing IoT applications. More research is required for IP technology and eventually the development of different post IP protocols optimized for IoT, compatible and interoperable with the exiting IP technologies.

Issues to be addressed:

- Network technologies (fixed, wireless, mobile etc.),
- Ad-hoc and wireless sensor networks
- Autonomic computing and networking
- Development of the infrastructure for "Network of Networks" capable of supporting dynamically small area and scale free connections and characteristics (typical social communities).
- Password and identity distribution mechanisms at the network level
- Anonymous networking
- IP and post IP technologies

4.5 Software, Services and Algorithms

Only with appropriate software will it be possible that the Internet of Things comes to life as imagined, as an integral part of the Future Internet. It is through software that novel applications and interactions are realized, and that the network with all its resources, devices and distributed services becomes manageable. For manageability, the need for some sort of self-configuration and auto-recovery after failures is foreseen.

Services play a key role: They provide a good way to encapsulate functionality – e.g., abstracting from underlying heterogeneous hardware or implementation details – , they can be orchestrated to create new, higher-level functionality, and they can be deployed and executed in remote locations, in-situ on an embedded device if necessary. Such distribution execution of service logic, sometimes also called distributed intelligence, will be key in order to deal with the expected scalability challenges.

Issues to be addressed include:

- Service discovery and composition

- Semantic interoperability, semantic sensor web etc.
- Data sharing, propagation and collaboration
- Autonomous agents
- Human machine interaction
- Self management techniques to overcome increasing complexities and save energy
- Distributed self adaptive software for self optimization, self configuration, self healing
- Lightweight and open middleware based on interacting components/modules abstracting resource and network functions;
- Energy efficient micro operating systems
- Software for virtualisation
- Language for object interaction
- Bio-inspired algorithms (e.g. self organization) and solutions based on game theory (to overcome the risks of tragedy of commons and reaction to malicious nodes)
- Algorithms for optimal assignment of resources in pervasive and dynamic environments
- Mathematical models and algorithms for inventory management, production scheduling, and data mining.

4.6 Hardware

The developments in the area of IoT will require research for hardware adaptation and parallel processing in ultra low power multi processor system on chip that handle non predictable situations at design time with the capability of self adaptiveness and self organization. Research and development is needed in the area of very low power field-programmable gate array hardware where the configuration (or parts of it) is changed dynamically from time to time to introduce changes to the device. Context switching architectures, where a set of configurations are available and the device between switch between them depending on the defined using context.

Research is needed for very large scale integrated (VLSI) circuits containing scalable cognitive hardware systems that are changing the topology mapped on the chip using dedicated algorithms.

Self adaptive networks on chip that analyzes itself during run time and self adapts are required for IoT applications. Such run time adaptive network on chip will adapt the underlying interconnection infrastructure on demand in response to changing communication requirements imposed by an application and context.

Issues to be addressed:

- Nanotechnologies- miniaturization
- Sensor technologies – embedded sensors, actuators
- Solutions bridging nano and micro systems.
- Communication – antennas, energy efficient RF front ends
- Nanoelectronics – nanoelectronics devices and technologies, self configuration, self optimization, self healing circuit architectures.
- Polymer electronics
- Embedded systems - micro energy microprocessors/microcontrollers, hardware acceleration
- Spintronics
- Low cost, high performance secure identification/authentication devices
- Low cost manufacturing techniques
- Tamper-resistant technology, side-channel aware designs

4.7 Data and Signal Processing Technology

In the context of Internet of Things the devices that are operating at the edge are evolving from embedded systems to cyber physical and web enabled “things” that are integrating computation, physical and cognitive processes. Cognitive devices, embedded computers and networks will monitor and control the physical processes, with feedback loops where physical processes affect computations and cognitive processes and contrariwise. This convergence of physical computing and cognitive devices (wireless sensor networks, mobile phones, embedded systems, embedded computers, micro robots etc.) and the Internet will provide

new design opportunities and challenges and requires new research that addresses the data and signal processing technology.

A typical feature of to cyber physical and web enabled “things” will the heterogeneity of device models, communication and cognitive capabilities. This heterogeneity concerns different execution models (synchronous, asynchronous, vs. timed and real-timed), communication models (synchronous vs. asynchronous), and scheduling of real time processes.

Issues to be addressed:

- Semantic interoperability, service discovery, service composition, semantic sensor web, data sharing, propagation and collaboration, autonomous agents, human machine interaction

4.8 Discovery and Search Engine Technologies

The Internet of Things will consist of many distributed resources including sensors and actuators, as well as information sources and repositories. It will be necessary to develop technologies for searching and discovering such resources according to their capabilities (e.g. type of sensor / actuator / services offered), their location and/or the information they can provide (e.g. indexed by the unique IDs of objects, transactions etc.). Search and discovery services will be used not only by human operators but also be application software and autonomous smart objects, in order to help gather complete sets of information from across many organisations and locations, as well as discovering what ambient infrastructure is available to support smart objects with their needs for transportation and handling, heating/cooling, network communication and data processing. These services play a key role in the mapping between real entities such as physical objects and in the assembly of their digital and virtual counterparts from a multitude of fragments of information owned and provided by different entities. Universal authentication mechanisms will be required, together with granular access control mechanisms that allow owners of resources to restrict who can discover their resources or the association between their resource and a specific entity, such as a uniquely identified physical object.

For efficient search and discovery, metadata and semantic tagging of information will be very important and there are significant challenges in ensuring that the large volumes of automatically generated information can be automatically and reliably without requiring human intervention. It will also be important that terrestrial mapping data is available and cross-referenced with logical locations such as postcodes and place names and that the search and discovery mechanisms are able to handle criteria involving location geometry concepts, such as spatial overlap and separation.

Issues to be addressed:

- Device discovery, distributed repositories
- Positioning and localisation
- Mapping of real, digital and virtual entities
- Terrestrial mapping data
- Semantic tagging and search
- Universal authentication mechanisms

4.9 Relationship Network Management Technologies

With many of Internet of Things and Internet of Services applications moving to a distributed seamless architecture the future application manager needs to monitor more than just the infrastructure. The Internet of Things must incorporate traffic and congestion management. This will sense and manage information flows, detect overflow conditions and implement resource reservation for time-critical and life-critical data flows. The network management technologies will need depth visibility to the underlying seamless networks that serves the applications and services and check the processes that run on them, regardless of device, protocol, etc. This will require identifying sudden overloads in service response time and resolving solutions, monitoring IoT

and web applications and identify any attacks by hackers, while getting connected remotely and managing all “things” involved in specific applications from remote “emergency” centres.

Issues to be addressed:

- Propagation of memes by things
- Identity, relationship and reputation management

4.10 Power and Energy Storage Technologies

Objects require a digital “self” in order to be part of the Internet of Things. This participation is obtained by combining electronic, embedded and wireless communication technologies into the physical objects themselves. Simple digitalization alternatives, such as bar code and passive RFID, do not require a power source on the embedded devices. More complex alternatives, such as those that provide active communications and object condition monitoring, need batteries to power the electronics that make the objects first class citizens of the IoT.

Energy storage has become one of the most important obstacles to the miniaturization of electronic devices, and today’s embedded wireless technologies such as Wireless Sensor Networks and Active RFID suffer from either bulky packaging to support large batteries or from short life times, that will require recharging or replacement of the integrated batteries. In order for the IoT to succeed in providing truly embedded and digital object participation, it is necessary to continue with the research on miniature high-capacity energy storage technologies. A solution that could bypass the shortcomings of energy storage is the harvesting of energy from the environment, which would automatically recharge small batteries contained in the objects.

Energy harvesting is still a very inefficient process that would require a large amount of research. Sources for energy harvesting in embedded devices could include, among others, vibration, solar radiation, thermal energy, etc.

Micro power technologies have emerged as a new technology area that can provide many development opportunities for IoT devices.

Research topics and issues that need to be addressed include:

- Energy harvesting/scavenging for MEMS devices and microsystems
- Electrostatic, piezoelectric and electromagnetic energy conversion schemes
- Thermoelectric systems and micro coolers
- Photovoltaic systems
- Micro fuel cells and micro reactors
- Micro combustion engines for power generation and propulsion
- Materials for energy applications
- Micro power ICs and transducers
- Micro battery technologies
- Energy storage and micro super capacitor technologies

4.11 Security and Privacy Technologies

Internet of Things needs to be built in such a way as to ensure an easy and safe user control. Consumers need confidence to fully embrace the Internet of Things in order to enjoy its potential benefits and avoid any risks to their security and privacy.

In the IoT every ‘thing’ is connected to the global Internet and ‘things’ are communicating with each other, which results in new security and privacy problems, e. g., confidentiality, authenticity, and integrity of data sensed and exchanged by ‘things’. Privacy of humans and things must be ensured to prevent unauthorized identification and tracking. In this context, the more autonomous and intelligent “things” get, problems like the identity and privacy of things, and responsibility of things in their acting will have to be considered.

The Internet of Things will challenge the traditional distributed database technology by addressing very large numbers of "things" that handle data, in a global information space and a universal data space. This poses challenges. In this context the information map of the real world of interest is represented across billions of "things", many of which are updating in real-time and a transaction or data change is updated across hundreds or thousands of "things" with differing update policies, opens up for many security challenges and security techniques across multiple policies. In order to prevent the unauthorized use of private information and permit authorized use, research is needed in the area of dynamic trust, security, and privacy management.

Issues to be addressed:

- Event-driven agents to enable an intelligent/self aware behaviour of networked devices
- Privacy preserving technology for heterogeneous sets of devices
- Models for decentralised authentication and trust
- Energy efficient encryption and data protection technologies
- Security and trust for cloud computing
- Data ownership
- Legal and liability issues
- Repository data management
- Access and use rights, rules to share added value
- Responsibilities, liabilities
- Artificial immune systems solutions for IoT
- Secure, low cost devices
- Integration into, or connection to, privacy-preserving frameworks, with evaluation privacy-preserving effectiveness.
- Privacy Policies management

4.12 Standardisation

The Internet of Things will support interactions among many heterogeneous sources of data and many heterogeneous devices though the use of standard interfaces and data models to ensure a high degree of interoperability among diverse systems. Although many different standards may co-exist, the use of ontology based semantic standards enables mapping and cross-referencing between them, in order to enable information exchange. From an architectural perspective, standards have an important role to play both within an organisation or entity and across organisations; adoption of standards promotes interoperability and allows each organisation or individual to benefit from a competitive marketplace of interoperable technology solutions from multiple providers; when those organisations or individuals which to share or exchange information, standards allow them to do so efficiently, minimising ambiguity about the interpretation of the information they exchange. Standards regarding frequency spectrum allocation, radiation power levels and communication protocols ensure that the Internet of Things co-operates with other users of the radio spectrum, including mobile telephony, broadcasting, emergency services etc. These can be expected to develop, as the Internet of Things increases in scale and reach and as additional radio spectrum becomes available through digital switchover etc.

As greater reliance is placed on the Internet of Things as the global infrastructure for generation and gathering of information, it will be essential to ensure that international quality and integrity standards are deployed and further developed, as necessary to ensure that the data can be trusted and also traced to its original authentic sources.

Issues to be addressed:

- IoT standardisation
- Ontology based semantic standards
- Spectrum energy communication protocols standards
- Standards for communication within and outside cloud
- International quality/integrity standards for data creation, data traceability

4.13 Future Technological Developments

		Before 2010	2010-2015	2015-2020	Beyond 2020
Development	**Identification Technology**	• Different schemes • Domain Specific IDs • ISO, GS1, u-Code, IPv6, etc	• Unified framework for unique identifiers • Open framework for the IoT • URIs	• Identity management • Semantics • Privacy-awareness	• "Thing DNA" identifier
	Internet of Things Architecture Technology	• IoT architecture specifications • Context-sensitive middleware • Intelligent reasoning platforms	• IoT architectures developments • IoT architecture in the FI • Network of networks architectures • F-O-T platforms interoperability	• Adaptive, context based architectures • Self-* properties	• Cognitive architectures • Experiential architectures
	Communication Technology	• RFID, UWB, Wi-Fi, WiMax, Bluetooth, ZigBee, RuBee, ISA 100, WirelessHart, 6LoWPAN	• Ultra low power chip sets • On chip antennas • Millimetre wave single chips • Ultra low power single chip radios • Ultra low power system on chip	• Wide spectrum and spectrum aware protocols	• Unified protocol over wide spectrum
	Network Technology	• Sensor networks	• Self aware and self organizing networks • Sensor network location transparency • Delay tolerant networks • Storage networks and power networks • Hybrid networking technologies	• Network context awareness	• Network cognition • Self learning, self repairing networks
	Software and algorithms	• Relational database integration • IoT-oriented RDBMS • Event-based platforms • Sensor middleware • Sensor Networks middleware • Proximity / Localization algorithms	• Large scale, open semantic software modules • Composable algorithms • Next generation IoT-based social software • Next generation IoT-based enterprise applications	• Goal oriented software • Distributed intelligence, problem solving • Things-to-Things collaboration environments	• User oriented software • The invisible IoT • Easy-to-deploy IoT sw • Things-to-Humans collaboration • IoT 4 All
	Hardware	• RFID Tags and some sensors • Sensors built in to mobile devices • NFC in mobile phones • Smaller and cheaper • MEMs technology	• Multi protocol, multi standards readers • More sensors and actuators • Secure, low-cost tags (e.g. Silent Tags)	• Smart sensors (bio-chemical) • More sensors and actuators (tiny sensors)	• Nano-technology and new materials

	Data and Signal Processing Technology	• Serial data processing • Parallel data processing • Quality of services	• Energy, frequency spectrum aware data processing, • Data processing context adaptable	• Context aware data processing and data responses	• Cognitive processing and optimisation
	Discovery and Search Engine Technologies	• Sensor network ontologies • Domain specific name services	• Distributed registries, search and discovery mechanisms • Semantic discovery of sensors and sensor data	• Automatic route tagging and identification management centres	• Cognitive search engines • Autonomous search engines
	Power and Energy Storage Technologies	• Thin batteries • Li-Ion • Flat batteries • Power optimized systems (energy management) • Energy harvesting (electrostatic, piezoelectric) • Short and medium range wireless power	• Energy harvesting (energy conversion, photovoltaic) • Printed batteries • Long range wireless power	• Energy harvesting (biological, chemical, induction) • Power generation in harsh environments • Energy recycling • Wireless power •	• Biodegradable batteries • Nano-power processing unit
	Security and Privacy Technologies	• Security mechanisms and protocols defined • Security mechanisms and protocols for RFID and WSN devices	• User centric context-aware privacy and privacy policies • Privacy aware data processing • Virtualisation and anonymisation	• Security and privacy profiles selection based on security and privacy needs • Privacy needs automatic evaluation • Context centric security	• Self adaptive security mechanisms and protocols
	Material Technology	• Silicon, Cu, Al Metallization • 3D processes	• SiC, GaN • Silicon • Improved/new semiconductor manufacturing processes/technologies for higher temperature ranges	• Diamond	
	Standardisation	• Standardization efforts for RFID security • Standardization of passive RFID tags with expanded memory and read/write capability for product serial numbers, repair and warranty information.	• IoT standardisation • M2M standardisation • Interoperability profiles	• Standards for cross interoperability with heterogeneous networks	• Standards for automatic communication protocols

4.14 Internet of Things Research Needs

Research Needs		Before 2010	2010-2015	2015-2020	Beyond 2020
	Identification Technology	• Different ID schemes customised for application domains • Convergence of IP and RFID IDs and addressing schemes	• Unique ID • Multiple IDs for specific cases • Extend the ID concept (more than ID number) • Electro Magnetic Identification - EMID	• Beyond EMID	• Multi methods-one ID
	IoT Architecture	• Intranet (Intranet of Things) (single controlling administrative entity of the IoT infrastructure, controlled environment and business cases, thousands/millions of things)	• Extranet (Extranet of Things) (partner to partner applications, basic interoperability, billions-of-things)	• Internet (Internet of Things) (global scale applications, global interoperability, many trillions of things)	
	SOA Software Services for IoT	• Basic IoT services (Services over Things)	• Composed IoT services (IoT Services composed of other Services, single domain, single administrative entity)	• Process IoT services (IoT Services implementing whole processes, multi/cross domain, multi administrative entities, totally heterogeneous service infrastructures)	
	Internet of Things Architecture Technology	• Low cost crypto primitives – hash functions, random number generators, etc. • Low cost hardware implementation without computational loss • Smaller and cheaper tags • Higher frequency tags • RFID tags for RF-unfriendly environments (i.e. water and metal) • 3-D localisation	• Adaptation of symmetric encryption and public key algorithms from active tags into passive tags • Universal authentication of objects • Graceful recovery of tags following power loss • More memory • Less energy consumption • 3-D real time location/position embedded systems • IoT Governance scheme	• Code in tags to be executed in the tag or in trusted readers. • Global applications • Adaptive coverage • Object intelligence • Context awareness	• Intelligent and collaborative functions
	Communication Technology	• Sensor networks, ZigBee, RFID, Bluetooth, WirelessHart, IAA100, UWB	• Long range (higher frequencies –tenth of GHz) • Protocols for interoperability	• On chip networks and multi standard RF architectures • Plug and play tags	• Self configuring, protocol seamless networks

			• Protocols that make tags resilient to power interruption and fault induction. • Collision-resistant algorithms	• Self repairing tags	
	Network Technology	• Broadband • Different networks (sensors, mobile phone, etc.,) • Interoperability framework (protocols and frequencies) • Network security (e.g. access authorization, data encryption, standards etc.)	• Grid/Cloud network • Hybrid networks • Ad hoc network formation • Self organising wireless mesh networks • Multi authentication • Networked RFID-based systems – interface with other networks – hybrid systems/networks	• Service based network • Integrated/universal authentication • Brokering of data through market mechanisms	• Need based network • Internet of **Everything** • Robust security based on a combination of ID metrics • Autonomous systems for non stop information technology service
	Software and algorithms	• Service oriented architectures • Embedded software • Generation of domain specific events • "Things" Semantics / Ontologies • Filtering • Probabilistic and non-probabilistic track and trace algorithms, based upon the analysis of tracking data concerning some kind of unique ID.	• Self management and control • Micro operating systems • Context aware business event generation • Interoperable ontologies of business events • Scalable autonomous software • Software for coordinated emergence • (Enhanced) Probabilistic and non-probabilistic track and trace algorithms, run directly by individual "things". • Software and data distribution systems	• Evolving software • Self reusable software • Autonomous things: o Self configurable o Self healing o Self management • Platform for object intelligence	• Self generating "molecular" software • Context aware software
	Hardware Devices	• MEMS • Low power circuits • Silicon devices • Smart multi band antennas • Beam steerable phased array antennas • Low power chip sets • Low cost tags • Small size, low cost passive functions • High-Q inductors • High density capacitors, tuneable capacitors	• Paper thin electronic display with RFID • Ultra low power EPROM/FRAM • NEMS • Polymer electronics tags • Antennas on chip • Coil on chip • Ultra low power circuits • Electronic paper • Devices capable of tolerating harsh environments (extreme temperature variation, vibration and shocks conditions and contact with different chemical substances)	• Polymer based memory • 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

		• Low loss switches • RF filters	• Nano power processing units • Silent Tags • Biodegradable antennae		
	Hardware Systems, Circuits and Architectures	• Integration of hybrid technologies sensor, actuator, display, memory • Power optimised hardware-software design • Power control of system on chip (SoC) • Development of high performance, small size, low cost passive functions e.g. high-Q inductors, tight tolerance capacitors, high density capacitors, low loss switches, RF filters, tuneable capacitors • Mobile RFID readers with increased functionality and computing power while reducing the size and cost • Miniaturised and embedded readers (SiP)	• Multi protocol front ends • Multi standard mobile readers • Extended range of tags and readers • Transmission speed • Distributed control and databases • Multi-band, multi-mode wireless sensor architectures • Smart systems on tags with sensing and actuating capabilities (temperature, pressure, humidity, display, keypads, actuators, etc.) • Ultra low power chip sets to increase operational range (passive tags) and increased energy life (semi passive, active tags). • Ultra low cost chips with security • Collision free air to air protocol	• 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	• Heterogeneous architectures. • “Fluid” systems, continuously changing and adapting.
	Data and Signal Processing Technology	• Grid computing • Heterogeneous modelling of sensor data • Virtual Things identification (i.e. things identified based on A/V signal processing) • Sensor virtualization (vendor/technology independent modules)	• Common sensor ontologies (cross domain) • Distributed energy efficient data processing	• Autonomous computing • Tera scale computing	• Cognitive computing
	Discovery and Search Engine Technologies	• Simple ID based object lookup • Local registries • Discovery services	• Scalable Discovery services for connecting things with services while respecting security, privacy and confidentiality • “Search Engine” for Things	• On demand service discovery/integration • Universal authentication	• Cognitive registries

			• IoT Browser • Multiple identities per object		
	Power and Energy Storage Technologies	• Thin batteries • Energy management • RF • Thermal • Solar	• Printed batteries • Photovoltaic cells • Super capacitors • Energy conversion devices • Grid power generation • Multiple power sources	• Paper based batteries • Wireless power everywhere, anytime. • Power generation for harsh environments	• Biodegradable batteries
	Security and Privacy Technologies	• Power efficient security algorithms	• Adaptation of symmetric encryption and public key algorithms from active tags into passive tags • Low cost, secure and high performance identification/authentication devices	• Context based security activation algorithms • Service triggered security • Context-aware devices • Object intelligence	• Cognitive security systems
	Material Technology	• Polymer • Assembly and packaging techniques for RFID tags (protection against high/low temperature, mechanical, chemical substances, etc)	• Carbon • Conducting Polymers and semi-conducting polymers and molecules • Conductive ink • Flexible substrates • Modular manufacturing techniques	• Carbon nanotube	
	Standardisation	• RFID • M2M • WSN • H2H	• Privacy and security cantered standards • Adoption of standards for “intelligent” IoT devices • Language for object interaction	• Dynamic standards • Adoption of standards for interacting devices	• Evolutionary standards • Adoption of standards for personalised devices

Chapter 5
References

[1] CTV: Deadly Fakes, http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20020306/ctvnews848463

[2] B. C. Hardgrave, M. Waller, and R. Miller. RFID's Impact on Out of Stocks: A Sales Velocity Analysis. Research Report from the Univ. of Arkansas, 2006.

[3] T. W. Gruen, D. S. Corsten, and S. Bharadwaj. Retail Out of Stocks. Technical report, 2002.

[4] P.Fewtrell, I. L Hirst, A Review of High-Cost Chemical/Petrochemical Accidents since Flixborough 1974. In: *Loss Prevention Bulletin* (1998), April, Nr. 140. - http://www.hse.gov.uk/comah/lossprev.pdf

[5] P. Mead, L. Slutsker, V. Dietz, L. McCaig, J. Bresee, C. Shapiro, P. Griffin and R. Tauxe. Food-related illness and death in the Unites States. Emerging Infectious Diseases, 1999.

[6] J. Buzby, T. Roberts, C.-T. Jordan Lin and J.M. MacDonald. Bacterial foodborne disease: Medical costs & productivity losses. USDA-ERS Agricultural Economic Report 741, 1996.

[7] L. Weiss Ferreira Chaves, F. Kerschbaum. Industrial Privacy in RFID-based Batch Recalls. In Proceedings of InSPEC'09, 2009.

[8] V. Coroama. The Smart Tachograph – Individual Accounting of Traffic Costs and its Implications. Proceedings of Pervasive 2006. pp. 135-152, Dublin, Ireland, May 07-10, 2006

[9] http://docs.oasis-open.org/ws-dd/discovery/1.1/wsdd-discovery-1.1-spec.html

[10] http://developer.apple.com/networking/bonjour/

[11] http://quimby.gnus.org/internet-drafts/draft-cai-ssdp-v1-03.txt

[12] http://www.sics.se/contiki/

[13] http://www.oasis-open.org

[14] http://xml.coverpages.org/

[15] A. Taylor, R. Harper, L. Swan, S. Izadi, A. Sellen, M. Perry. Homes that make us smart. Personal and Ubiquitous Computing, Vol. 11, Number 5, June 2007

[16] Joshua R. Smith, David Wetherall, Revisiting Smart Dust with RFID Sensor Networks; Michael Buettner, Ben Greenstein, Alanson Sample, Seventh ACM Workshop on Hot Topics in Networks (HotNets-VII), 2008, Calgary, Alberta, Canada. To appear.

[17] http://www.rfc-editor.org/rfc/rfc2929.txt

[18] http://en.wikipedia.org/wiki/Meme

[19] A. Brintrup, D.C. Ranasinghe, S. Kwan, A. Parlikad, K. Owens, “Roadmap to Self-Serving Assets in Civil Aerospace” in *Proc. Of CIRP IPS2 Conference*, Cranfield, UK, April 1st-2nd 2009, pp. 323–331.

[20] T. Kelesidis, I. Kelesidis, P. Rafailidis, and M. Falagas. “Counterfeit or substandard antimicrobial drugs: a review of the scientific evidence”. Journal of Antimicrobial Chemotherapy, 60(2):214-236, August 2007.

[21] C. Troncoso, G. Danezis, E. Kosta, and B. Preneel, "PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance," In *Proceedings of the 6th ACM workshop on Privacy in the electronic society (WPES 2007)*, T. Yu (ed.), ACM, pp. 99-107, 2007.

[22] Rumble SM, Stutsman R, Levis P, Mazières D, Zeldovich N. "Apprehending Joule Thieves with Cinder". In *Proceedings of the First ACM SIGCOMM Workshop on Networking, Systems, Applications on Mobile Handhelds (MobiHeld 2009)*.

[23] O. Vermesan, D. Grosso, F. Dell'Ova, C. Prior, “Quo Vadis RFID Technology. Emerging RFID Technology “ In *Proceedings of EU RFID Forum 2007 Conference,* Brussels, Belgium, March .2007

Acknowledgements

Many colleagues have assisted with their views on this Internet of Things strategic research agenda document. Their contributions are gratefully acknowledged.

Ali Rezafard, IE, Afilias, EPCglobal Data Discovery JRG

Andras Vilmos, HU, Safepay, StoLPaN

Anthony Furness, UK, AIDC Global Ltd & AIM UK, CASAGRAS, RACE networkRFID

Antonio Manzalini, IT, Telecom Italia, CASCADAS

Carlo Maria Medaglia , IT, University of Rome 'Sapienza'

Daniel Thiemert, UK, University of Reading, HYDRA

David Simplot-Ryl, FR, INRIA/ERCIM, ASPIRE

Dimitris Kiritsis, CH, EPFL, IMS2020

Florent Frederix, EU, EC, EC

Franck Le Gall , FR, Inno, WALTER

Frederic Thiesse , CH, University of St. Gallen, Auto-ID Lab

Harald Sundmaeker, DE, ATB GmbH , CuteLoop

Humberto Moran, UK, Friendly Technologies, PEARS Feasibility

Jean-Louis Boucon, FR, TURBOMECA, SMMART

John Soldatos, GR, Athens Information Technology, ASPIRE

Mario Hoffmann, DE, Fraunhofer-Institute SIT, HYDRA

Markus Eisenhauer, DE, Fraunhofer-Institute FIT, HYDRA

Neeli Prasad, DE, CTIF, University of Aalborg, ASPIRE

Paolo Paganelli , IT, Insiel, EURIDICE

Wang Wenfeng, CN, CESI/MIIT, CASAGRAS

Zsolt Kemeny, HU, Hungarian Academy of Sciences, TraSer

For further information:

Information Desk
European Commission - Information Society and Media DG
Office: BU31 01/18 B-1049 Brussels
Email: infso-desk@ec.europa.eu
Tel: +32 2 299 93 99
Fax: +32 2 299 94 99
http://europa.eu/information_society