UNIT 1

INTRODUCTION TO INTERNET OF THINGS

1.1 INTERNET OF THINGS (IOT)

IoT comprises things that have unique identities and are connected to internet. By 2020 there will be a total of 50 billion devices /things connected to internet. IoT is not limited to just connecting things to the internet but also allow things to communicate and exchange data.

Internet of Things (IoT) is a concept which enables communication between internetworking devices and applications, whereby physical objects or 'things' communicate through the Internet. The concept of IoT began with things classified as identity communication devices. Radio Frequency Identification Device (RFID) is an example of an identity communication device. Things are tagged to these devices for their identification in future and can be tracked, controlled and monitored using remote computers connected through the Internet.

The concept of IoT enables, for example, GPS-based tracking, controlling and monitoring of devices; machine-to-machine (M2M) communication; connected cars; communication between wearable and personal devices and Industry 4.0. The IoT concept has made smart cities a reality and is also expected to make self-driving cars functional very soon.

1.1.1 IOT Vision

Internet of Things (IoT) is a concept and a paradigm that considers pervasive presence in the environment of a variety of things/objects that through wireless and wired connections and unique addressing schemes are able to interact with each other and cooperate with other things/objects to create new applications/services and reach common goals. In this context the research and development challenges to create a smart world are enormous. A world where the real, digital and the virtual are converging to create smart environments that make energy, transport, cities and many other areas more intelligent.The goal of the Internet of Things is to enable things to be connected anytime, anyplace, with anything and anyone ideally using any path/ network and any service.

Internet of Things is a vision where things (wearable watches, alarm clocks, home devices, surrounding objects) become 'smart' and function like living entities by sensing, computing and communicating through embedded devices which interact with remote objects (servers, clouds, applications, services and processes) or persons through the Internet or Near-Field Communication (NFC) etc. The vision of IoT can be understood through Examples 1 and 2.

Example 1

Through computing, an umbrella can be made to function like a living entity. By installing a tiny embedded device, which interacts with a web-based weather service and the devices owner through the Internet the following communication can take place. The umbrella, embedded with a circuit for the purpose of computing and communication connects to the Internet. A website regularly publishes the weather report.

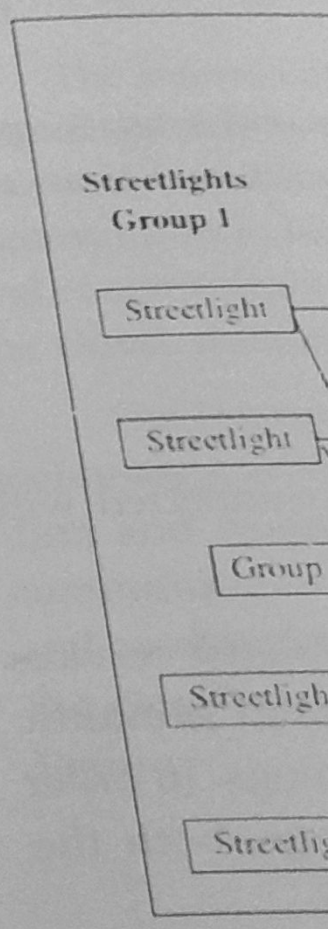
The umbrella receives these reports each morning, analyses the data and issues reminders to the owner at intermittent intervals around his/her office-going time. The reminders can be distinguished using differently coloured LED flashes such as red LED flashes for hot and sunny days, yellow flashes for rainy days. A reminder can be sent to the owner's mobile at a pre-set time before leaving for office using NFC, Bluetooth or SMS technologies. The message can be—(i) Protect yourself from rain. It is going to rain. Don't forget to carry the umbrella; (ii) Protect yourself from the sun. It is going to be hot and sunny. Don't forget to carry the umbrella. The owner can decide to carry or not to carry the umbrella using the Internet connected umbrella.

Example 2

Streetlights in a city can be made to function like living entities through sensing and computing using tiny embedded devices that communicate and interact with a central control-and-command station through the Internet. Assume that each light in a group of 32 streetlights comprises a sensing, computing and communication circuit. Each group connects to a group-controller (or coordinator) through Bluetooth or ZigBee. Each controller further connects to the central command-and-control station through the Internet.

The station receives information about each streetlight in each group in the city at periodic intervals. The information received is related to the functioning of the 32 lights, the faulty lights, about the presence or absence of traffic in group vicinity, and about the ambient conditions, whether cloudy, dark or normal daylight.

The station remotely
an appropriate action as p
remedial actions in case a
group in the city is contro
the IoT concept for street



Figu

Interne

Ten "cri
laid out by G
IP address a
consumer it
technology
are not ope
models tha

-
-
-
-

The station remotely programs the group controllers, which automatically take an appropriate action as per the conditions of traffic and light levels. It also directs remedial actions in case a fault develops in a light at a specific location. Thus, each group in the city is controlled by the 'Internet of streetlights'. Figure shows the use of the IoT concept for streetlights in a city.

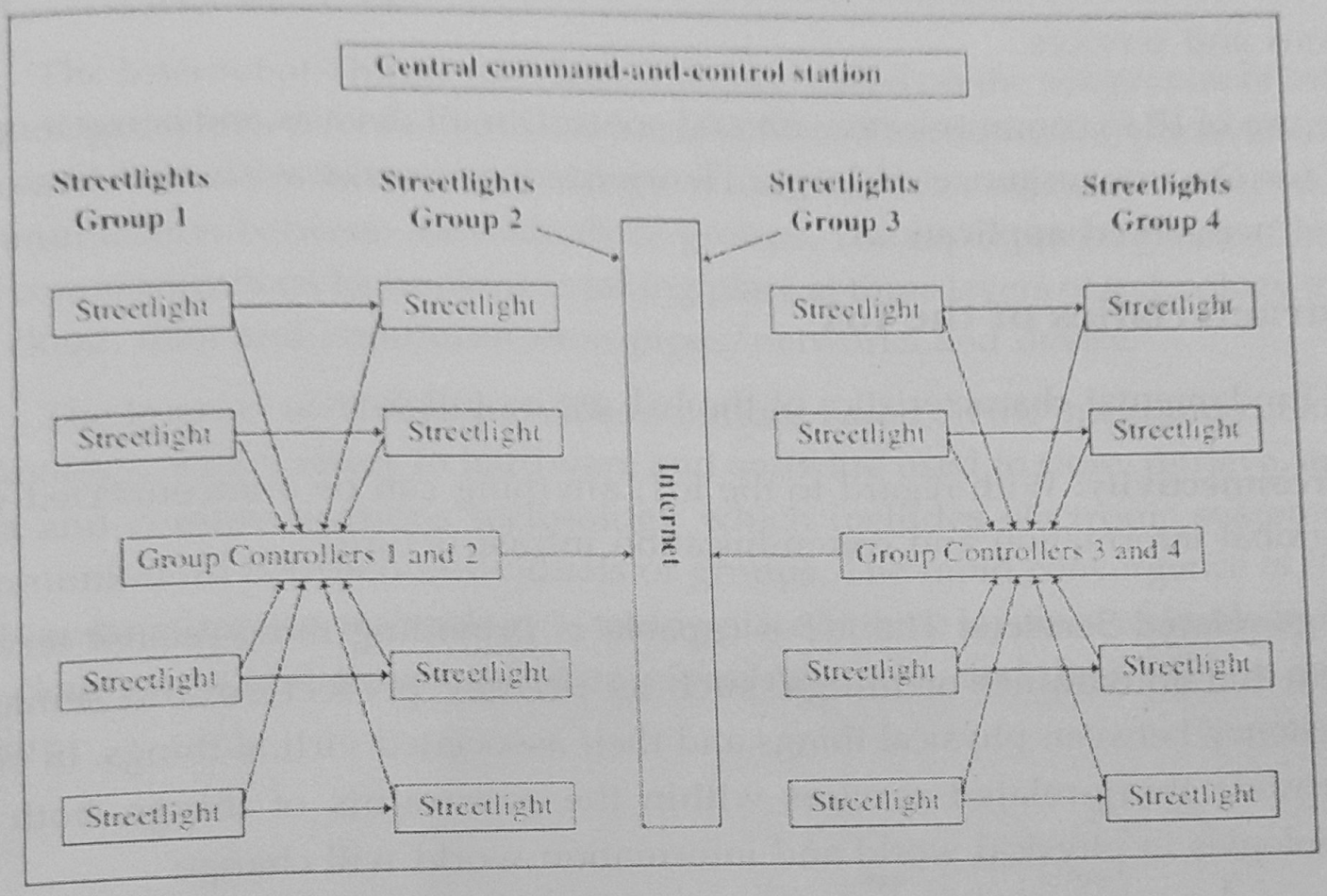


Figure : Use of Internet of Things concept for streetlights in a city

Internet of Things Common Definition

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

- Manage
- Monetize
- Operate
- Extend

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

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

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

Characteristics of the IoT

The fundamental characteristics of the IoT are as follows :

1. **Interconnectivity:** With regard to the IoT, anything can be interconnected with the global information and communication infrastructure.

2. **Things-related Services:** The IoT is capable of providing thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual things. In order to provide thing-related services within the constraints of things, both the technologies in physical world and information world will change.

3. **Heterogeneity:** The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks.

4. **Dynamic Changes:** The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically.

5. **Enormous Scale:** The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet. The ratio of communication triggered by devices as compared to communication triggered by humans will noticeably shift towards device-triggered communication. Even more critical will be the management of the data generated and their interpretation for application purposes. This relates to semantics of data, as well as efficient data handling.

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

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

The Internet of Things provides solutions based on the integration of information technology, which refers to hardware and software used to store, retrieve, and process data and communications technology which includes electronic systems used for communication between individuals or groups. The rapid convergence of information and communications technology is taking place at three layers of technology innovation: the cloud, data and communication pipes/networks, and device [8], as presented in Figure .

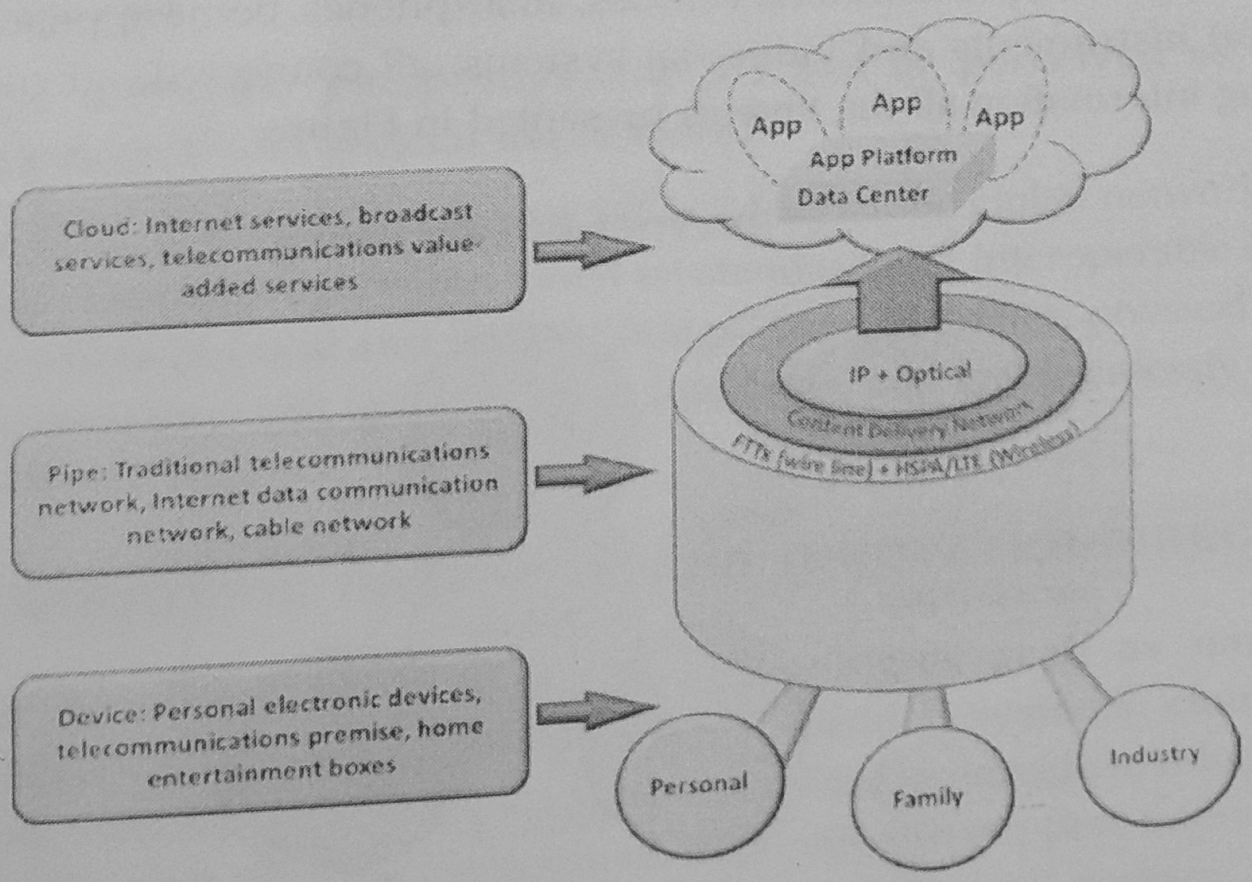


Figure: Factors driving the convergence and contributing to the integration and transformation of cloud, pipe, and device technologies

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

By 2020, over 30 billion connected things, with over 200 billion with intermitt connections are forecast. Key technologies here include embedded sensors, ima recognition and NFC. By 2015, in more than 70% of enterprises, a single executab will oversee all Internet connected things. This becomes the Internet of Everything.

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

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

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

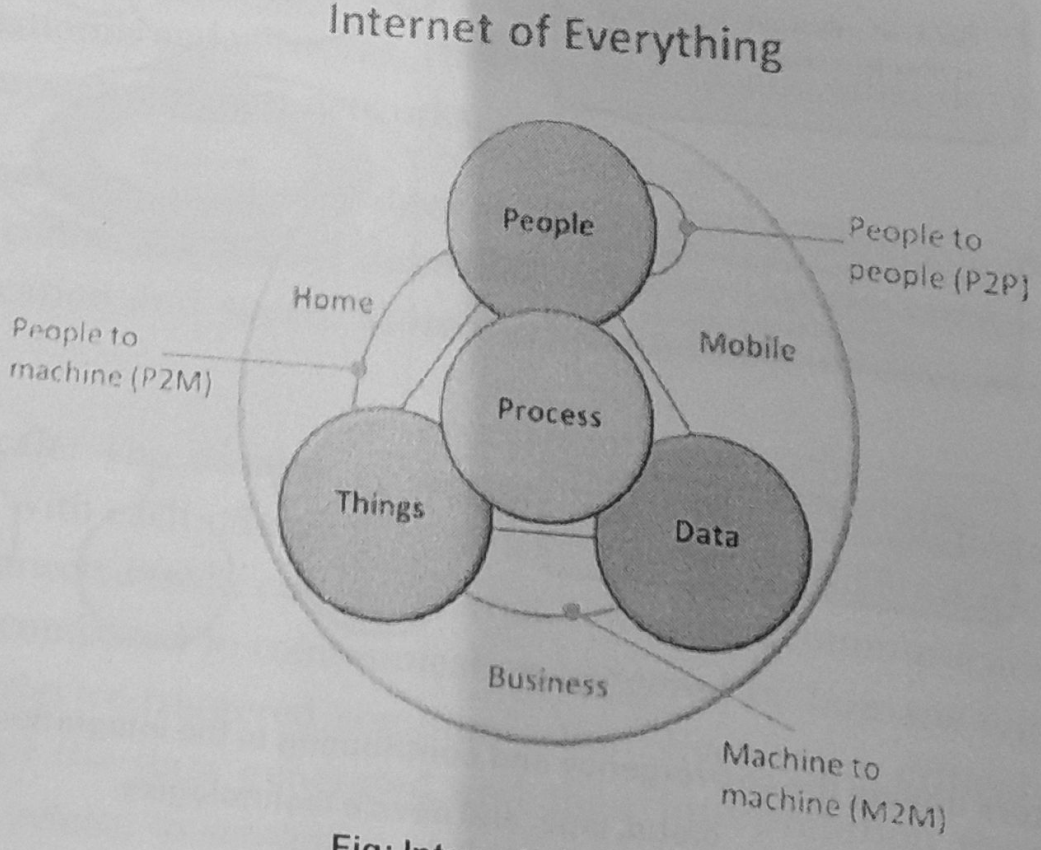


Fig: Internet of everything

The Internet of Things had until recently different means at different levels of abstractions through the value chain, from lower level semiconductor through the service providers. The Internet of Things is a "global concept" and requires a common definition. Considering the wide background and required technologies, from sensing device, communication subsystem, data aggregation and pre-processing to the object instantiation and finally service provision, generating an unambiguous definition of the "Internet of Things" is non-trivial.

The IERC is actively involved in ITU-T Study Group 13, which leads the work of the International Telecommunications Union (ITU) on standards for next generation networks (NGN) and future networks and has been part of the team which has formulated the following definition [18]: "Internet of things (IoT): A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

NOTE:

1. Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.
2. From a broader perspective, the IoT can be perceived as a vision with technological and societal implications."

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

1.2 STRATEGIC RESEARCH AND INNOVATIONDIRECTIONS

The development of enabling technologies such as nanoelectronics, communications, sensors, smart phones, embedded systems, cloud networking, network virtualization and software will be essential to provide to things the capability to be connected all the time everywhere. This will also support important future IoT product innovations affecting many different industrial sectors. Some of these technologies such as embedded or cyber-physical systems form the edges of the "Internet of Things" bridging the gap between cyber space and the physical world of

real "things", and are crucial in enabling the "Internet of Things" to deliver on its vision and become part of bigger systems in a world of "systems of systems". An example of technology convergence is presented in Figure .

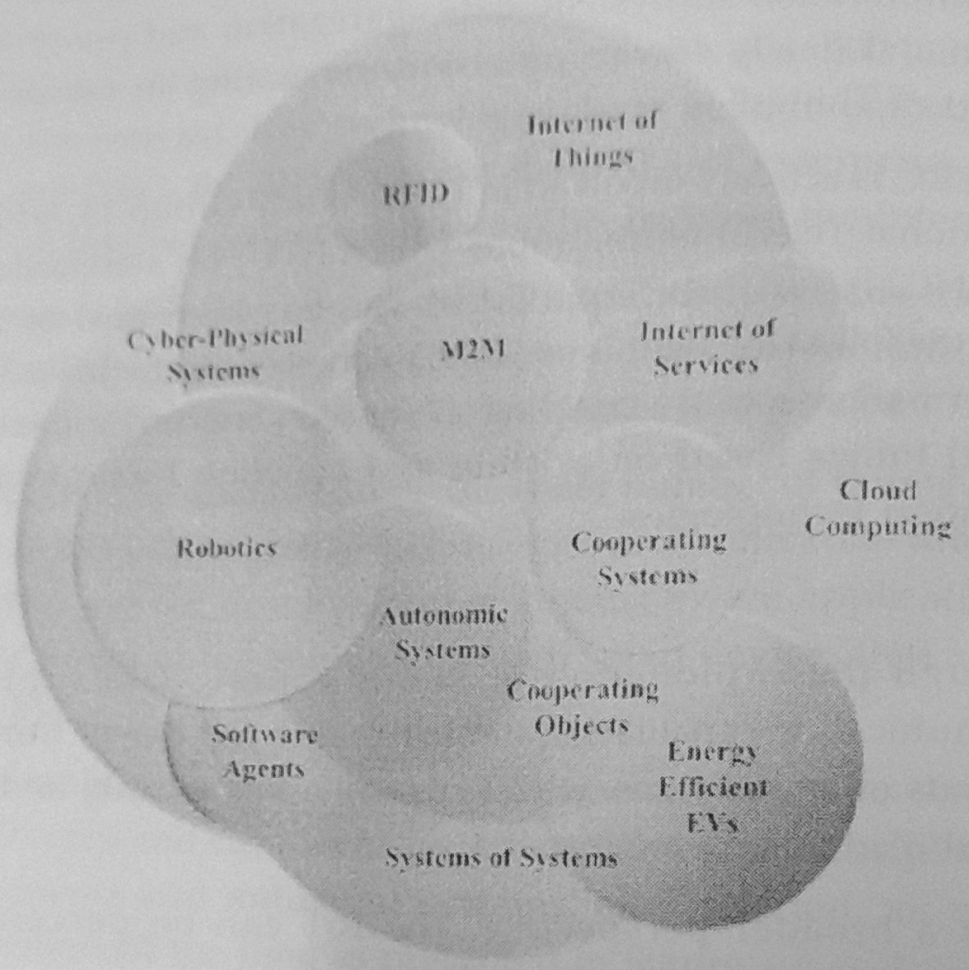


Figure: Technology convergence.

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

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

As such, IoT creates intelligent applications that are based on the supporting KETs identified, as IoT applications address smart environments either physical or at cyber-space level, and in real time. To this list of key enablers, we can add the global

deployment of IPv6 across the World enabling a global and ubiquitous addressing of any communicating smart thing.

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

The International Technology Roadmap for Semiconductors has emphasized in its early editions the "miniaturization" and its associated benefits in terms of performances, the traditional parameters in Moore's Law. This trend for increased performances will continue, while performance can always be traded against power depending on the individual application, sustained by the incorporation into devices of new materials, and the application of new transistor concepts. This direction for further progress is labelled "More Moore"

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

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

Integrated networking, information processing, sensing and actuation capabilities allow physical devices to operate in changing environments. Tightly coupled cyber and physical systems that exhibit high level of integrated intelligence are referred to as cyber-physical systems. These systems are part of the enabling technologies for Internet of Things applications where computational and physical processes of such systems are tightly interconnected and coordinated to work together effectively, with or without the humans in the loop. Robots, intelligent buildings, implantable medical devices, vehicles that drive themselves or planes that automatically fly in a controlled airspace, are examples of cyber-physical systems that could be part of Internet of Things ecosystems.

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

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

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

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

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

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

Since the release of the first version of the Strategic Research and Innovation Agenda, we have witnessed active research on several IoT topics. On the one hand this research filled several of the gaps originally identified in the Strategic Research and Innovation Agenda, whilst on the other it created new challenges and research questions.

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

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

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

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

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

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

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

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

IoT Functional View

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

1. Module for interaction with local IoT devices (for example embedded in a mob phone or located in the immediate vicinity of the user and thus contactable via short range wireless interface). This module is responsible for acquisition observations and their forwarding to remote servers for analysis and permane storage.
2. Module for local analysis and processing of observations acquired by IoT devic
3. Module for interaction with remote IoT devices, directly over the Internet or mo likely via a proxy. This module is responsible for acquisition of observations an their forwarding to remote servers for analysis and permanent storage.
4. Module for application specific data analysis and processing. This module i running on an application server serving all clients. It is taking requests fro mobile and web clients and relevant IoT observations as input, execute appropriate data processing algorithms and generates output in terms o knowledge that is later presented to users.
5. Module for integration of IoT-generated information into the business processe of an enterprise. This module will be gaining importance with the increased us of IoT data by enterprises as one of the important factors in day-to-day busines or business strategy definition.

6. User interface (web or mobile): visual representation of measurements in a given context (for example on a map) and interaction with the user, i.e. definition of user queries.

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

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

Research Challenges

1. Design of open APIs on all levels of the IoT ecosystem

2. Design of standardized formats for description of data generated by IoT devices to allow mashups of data coming from different domains and/or providers.

1.2.1 IoT Applications

The IoT finds application in various private and public aspects of life.

1. **Agriculture**: The ever-increasing world population drives up the demand for agricultural products. However, the migration of young people to big cities destabilizes the human resource required for agricultural development. IoT and related technologies can be pivotal in automating farming processes and fulfilling food demand.

2. **Consumer Applications**: The **Internet of Things** makes people's lives easier by monitoring and managing their lifestyles. There is a massive market for intelligent electronics, watches, television systems, health tracking, and virtual reality. In addition, IoT is leading the market with applications such as home security and personal asset tracking.

3. **Healthcare**: Wearable IoT devices provide a range of benefits to patients and healthcare providers alike. By extension, IoT enables healthcare professionals to monitor patients remotely. The devices can automatically collect patients' health vitals like blood pressure, heart rate, temperature, and more.

4. **Insurance:** IoT is altering traditional business models like insurance. It simplifies and accelerates the claim and underwriting process. Besides reducing costs, digital networking via IoT generates additional revenues. Cross-selling and more significant customer interaction become a strategic component for insurers.

5. **Manufacturing:** The Internet of Things creates a more technically-driv environment for manufacturing industries. It can automatically track develop cycles, facilitate the production flow, and manage inventories.

6. **Retail:** IoT devices can collect vital data on a product's shopping lifecycle. On this data is processed and analyzed, retail managers can make valuable decisio to improve retail operations and the customer experience.

7. **Transportation:** IoT applications integrate personal and commercial vehicles b improving communication and information distribution. Besides connecting consumers and goods, it offers benefits such as route optimization, automobil tracking, weather monitoring, distance coverage, and more.

8. **Utilities/Energy:** A grid can have IoT capabilities with intelligent meters, receivers, sensors, and energy boxes communicating. **IoT applications** in utilities generate revenue, improve efficiency, and conserve resources. Utility providers can keep up with the rising demand by optimizing energy and distribution with the help of IoT.

9. **Traffic Monitoring:** Intelligent traffic monitoring helps improve decision-making and achieve urban growth. An IoT-based system collects, processes, and analyzes real-time traffic data to provide updates on traffic incidents and congestion. In addition, early warning messages save commute time during peak hours.

10. **Hospitality:** Many hotels allow guests to control air conditioning, heating, or ventilation from a central location. Television control and greeting devices are also common. Moreover, Internet of Things devices alert the staff about various appliances' operating status. As a result, technicians can fix critical appliances even before any major functionality loss occurs.

11. **Water Supply:** Water scarcity is a reality. IoT applications have a potential solution to monitor, control, and regulate the quality and usage of water. Besides, it also maintains associated equipment such as pumps, pipes, etc. Smart water technology connects water systems with people.

12. **Fleet Management:** IoT enables predictive fleet maintenance by boosting visibility, efficiency, and manageability. It helps to monitor cargo better and improves driver operation. In addition, IoT devices can predict maintenance and help replace parts before the issue gets too expensive.

13. **Smart Pollution Control:** IoT devices and attached sensors are stationed at key city locations. They monitor pollution levels and periodically upload data to the IoT cloud. The system then processes the information to trigger public actions such as diversions or road closures.

14. **Smart Cities:** A smart city has better public utilities, infrastructure, services, and more. Smart meters allow utility companies to regulate energy flow efficiently, while connected vehicles make public transit tremendously efficient. In addition, smart grids are coming up to conserve resources and lower peak hour stress.

Applications and Use Case Scenarios

The IERC vision is that "the major objectives for IoT are the creation of smart environments/spaces and self-aware things (for example: smart transport, products, cities, buildings, rural areas, energy, health, living, etc.) for climate, food, energy, mobility, digital society and health applications". The outlook for the future is the emerging of a network of interconnected uniquely identifiable objects and their virtual representations in an Internet alike structure that is positioned over a network of interconnected computers allowing for the creation of a new platform for economic growth.

1. Smart products have a real business case, can typically provide energy and efficiency savings of up to 30 per cent, and generally deliver a two- to three-year return on investment. This trend will help the deployment of Internet of Things applications and the creation of smart environments and spaces.

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

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

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

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

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

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

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

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

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

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

1.3 INTERNET TECHNOL

The Internet of

1. Cloud Comput

Since the publi one of the major bui progressively foster paradigms known "Infrastructure and cost of ownership market entry thre With the virtuali convergence of cl opportunities in t

As part of t be delivered on- to virtualize sens connected objec (such as Sensin

Moreover the "sensing se into the fabric projecting an domains) at m the creation o

2. IoT and

The 20 discovering the past yea data (web-o Future rese could build infrastructu

1.3 INTERNET OF THINGS AND RELATED FUTURE INTERNET TECHNOLOGIES

The Internet of Things and Related Future Internet Technologies are as follows:

1. Cloud Computing

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

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

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

2. IoT and Semantic Technologies

The 2010 SRA has identified the importance of semantic technologies towards discovering devices, as well as towards achieving semantic interoperability. During the past years, semantic web technologies have also proven their ability to link related data (web-of-data concept) , while relevant tools and techniques have just emerged . Future research on IoT is likely to embrace the concept of Linked Open Data. This could build on the earlier integration of ontologies (e.g., sensor ontologies) into IoT infrastructures and applications.

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

3. Autonomy

Spectacular advances in technology have introduced increasingly complex and large scale computer and communication systems. Autonomic computing , inspired by biological systems, has been proposed as a grand challenge that will allow the systems to self-manage this complexity, using high-level objectives and policies defined by humans. The objective is to provide some self-x properties to the system, where x can be adaptation, organization, optimization, configuration, protection, healing, discovery, description, etc. The Internet of Things will exponentially increase the scale and the complexity of existing computing and communication systems. Autonomy is thus an imperative property for IoT systems to have. However, there is still a lack of research on how to adapt and tailor existing research on autonomic computing to the specific characteristics of IoT, such as high dynamicity and distribution, real-time nature, resource constraints, and lossy environments.

Properties of Autonomic IoT Systems

The following properties are particularly important for IoT systems and need further research:

1. **Self-adaptation:** In the very dynamic context of the IoT, from the physical to the application layer, self-adaptation is an essential property that allows the communicating nodes, as well as services using them, to react in a timely manner to the continuously changing context in accordance with, for instance, business policies or performance objectives that are defined by humans. IoT systems should be able to reason autonomously and give self-adapting decisions. Cognitive radios at physical and link layers, self-organising network protocols, automatic service discovery and (re-)bindings at the application layer are important enablers for the self-adapting IoT.
2. **Self-organization:** In IoT systems – and especially in WS&ANs – it is very common to have nodes that join and leave the network spontaneously. The network should therefore be able to re-organize itself against this evolving

topology. Self organizing, energy efficient routing protocols have a considerable importance in the IoT applications in order to provide seamless data exchange throughout the highly heterogeneous networks. Due to the large number of nodes, it is preferable to consider solutions without a central control point like for instance clustering approaches. When working on self-organization, it is also very crucial to consider the energy consumption of nodes and to come up with solutions that maximize the IoT system lifespan and the communication efficiency within that system.

3. **Self-optimisation:** Optimal usage of the constrained resources (such as memory, bandwidth, processor, and most importantly, power) of IoT devices is necessary for sustainable and long-living IoT deployments. Given some high-level optimisation goals in terms of performance, energy consumption or quality of service, the system itself should perform necessary actions to attain its objectives.

4. **Self-configuration:** IoT systems are potentially made of thousands of nodes and devices such as sensors and actuators. Configuration of the system is therefore very complex and difficult to handle by hand. The IoT system should provide remote configuration facilities so that self-management applications automatically configure necessary parameters based on the needs of the applications and users. It consists of configuring for instance device and network parameters, installing/uninstalling/upgrading software, or tuning performance parameters.

5. **Self-protection:** Due to its wireless and ubiquitous nature, IoT will be vulnerable to numerous malicious attacks. As IoT is closely related to the physical world, the attacks will for instance aim at controlling the physical environments or obtaining private data. The IoT should autonomously tune itself to different levels of security and privacy, while not affecting the quality of service and quality of experience.

6. **Self-healing:** The objective of this property is to detect and diagnose problems as they occur and to immediately attempt to fix them in an autonomous way. IoT systems should monitor continuously the state of its different nodes and detect whenever they behave differently than expected. It can then perform actions to fix the problems encountered. Encounters could include re-configuration parameters or installing a software update.

7. **Self-description:** Things and resources (sensors and actuators) should be able to describe their characteristics and capabilities in an expressive manner in order to allow other communicating objects to interact with them. Adequate device and service description formats and languages should be defined, possibly at the

semantic level. The existing languages should be re-adapted in order to
trade-off between the expressiveness, the conformity and the size
descriptions. Self-description is a fundamental property for implementing
and play resources and devices.

8. **Self-discovery:** Together with the self-description, the self-discovery feature
an essential role for successful IoT deployments. IoT devices/services shou
dynamically discovered and used by the others in a seamless and transp
way. Only powerful and expressive device and service discovery proto
(together with description protocols) would allow an IoT system to be
dynamic (topology-wise).

9. **Self-matchmaking :** To fully unlock the IoT potential, virtual objects will
to:

   (i) Be reusable outside the context for which they were originally deployed

   (ii) Be reliable in the service they provide.

   On the one hand, IoT services will be able to exploit enriched availabilit
underlying objects. They will also have to cope with their unreliable nature
be able to find suitable "equivalent object" alternatives in case of failu
unreachability etc. Such envisaged dynamic service-enhancement environme
will require self-matchmaking features (between services and objects and
versa) that will prevent users of IoT future services from having to (re-)config
objects themselves.

10. **Self-energy-supplying:** Finally, self-energy-supplying is a tremendou
important (and very IoT specific) feature to realize and deploy sustainable
solutions. Energy harvesting techniques (solar, thermal, vibration, etc.) sho
be preferred as a main power supply, rather than batteries that need to be repla
regularly, and that have a negative effect on the environment.

Research Directions for Self-manageable IoT Systems

we propose the following research directions to progress towards self-manageab
IoT systems:

Already existing fundamental research results from domains including artifici
intelligence, biological systems, control theory, embedded systems and softwa
engineering are necessary to build scientifically-proven, solid, robust and reliab
solutions. It may be necessary to tailor existing research to the IoT context. In additio
multidisciplinary conferences and workshops should be organised to foster th
interaction level between experts in those domains.

1. Novel methodologies, architectures, algorithms, technologies, and protocols should be developed taking into account IoTspecific characteristics such as resource constraints, dynamic, un-predictive, error prone and lossy environments, distributed and real-time data handling and decision-making, requirements, etc. Characterisation of self-x properties in IoT context should be done based on real-life cross-domain use cases.

2. Autonomic issues should be considered from the very early phases of IoT system implementations, from conception to deployment of devices, infrastructures and services. The self-awareness property should be included to any software module, however separated from the functional code. Hardware should be designed to be reconfigurable.

3. Devices should either be able to provide management data to autonomic managers, or to have embedded intelligence to reason and act locally. Automated tools for development, deployment, and supervision of IoT devices and services should be developed.

4. Prototypes should be developed at early stages in order to validate the theoretical results by measuring the overhead that autonomy can bring to IoT systems.

5. IoT is expected to be composed of very heterogeneous networks, thus standard interfaces should be defined for interoperability. Specific working groups on self-management issues should be created in standardisation organisations, industrial alliances and fora on IoT. A self-organising network (SON) for LTE of 3GPP is a good initiative that should be followed by other next generation network standards.

6. Model-driven approaches are solid ways to provide correctness, robustness, reliability, and dependability properties, and they have already proven their importance for the conception and development of embedded systems. In the context of IoT, they should be extended to obtain these properties not only during design and development but also at deployment and run-time for self-adaptation.

7. New modes of interaction with autonomic IoT systems that would increase the quality and experience of users are necessary, e.g., user assistance with intuitive multimodal interfaces: to monitor and control autonomic systems, to define rules and policies, and to receive important feedback in real-time.

8. Various stakeholders (users, manufacturers, integrators, service providers, telecom operators, etc.) will be dynamically and concurrently involved in IoT systems; particular attention should thus be paid for resource sharing and policy conflict

resolution between different actors. In addition to many existing concepts fr
the distributed systems domain, fundamentals of economics can also be appl
to resolve these issues

9. New programming paradigms should be proposed for creating self-awa
applications with the ability of self-adaption on-the-fly. The flexibility, dynamicit
modularity of the service-oriented approach (SOA) is particularly interestin
An integration of SOA with new device-oriented approaches can be useful f
programming cyber-physical environments.

10. Security and privacy issues should be considered very seriously since IoT deal
not only with huge amounts of sensitive data (personal data, business data, etc
but also has the power of influencing the physical environment with its contro
abilities. Cyber-physical environments must thus be protected from any kind o
malicious attacks.

11. Addressing scalability for a large scale IoT deployment is another key issue.
Integration with IPv6 and global resource directories should be further researched,
including collateral issues such as authentication and privacy management with
distributed IoT across global networks.

In order to make the smart objects paradigm come true (objects with perception
capabilities, embedded intelligence and high level of autonomy and
communication) much research is needed in order to fit sensors/actuators, CPU,
memory, energy, etc. into tiny chips. The challenge is quite high, assuming that
autonomy requires complex algorithms which themselves require high CPU power
and therefore also a comfortable amount of available energy.

12. Self-management systems should be designed with particular attention in contexts
where the safety of the user can be impacted (e.g., driving cars). In some cases,
policies should be embedded in the system to prevent safety risk in case of
malfunction of the self-management system.

4 Situation Awareness and Cognition

Integration of sensory, computing and communication devices (e.g. smart phones,
GPS) into the Internet is becoming common. This is increasing the ability to extract
"content" from the data generated and understand it from the viewpoint of the wider
application domain (i.e. meta-data). This ability to extract content becomes ever more
crucial and complex, especially when we consider the amount of data that is generated.
Complexity can be reduced through the integration of self-management and automatic
learning features (i.e. exploiting cognitive principles). The application of cognitive

principles in the extraction
towards creating overall aw
ability to respond to chang
instruction from users an
service creation.

1.4 INFRASTRUC

The Internet of Th
become part of our overa
most recently the Intern
computers, the Internet
objects with a strong in

1. Plug and Play In

If we look at IoT-
It is typically deploy
significant technical k
of Things we need t
towards a horizonta
simultaneously.

This is only po
simple as plugging i
an infrastructure tha
it to the application
on autonomy. On t
communication, fea
this process. Suitab
the integration into
provided, such as

2. Infrastructu

The infrast
An application m
is not limited to
whenever relev
status of things
changes and th

principles in the extraction of "content" from data can also serve as a foundation towards creating overall awareness of a current situation. This then gives a system the ability to respond to changes within its situational environment, with little or no direct instruction from users and therefore facilitate customised, dependable and reliable service creation.

1.4 INFRASTRUCTURE

The Internet of Things will become part of the fabric of everyday life. It will become part of our overall infrastructure just like water, electricity, telephone, TV and most recently the Internet. Whereas the current Internet typically connects full-scale computers, the Internet of Things (as part of the Future Internet) will connect everyday objects with a strong integration into the physical world

1. Plug and Play Integration

If we look at IoT-related technology available today, there is a huge heterogeneity. It is typically deployed for very specific purposes and the configuration requires significant technical knowledge and may be cumbersome. To achieve a true Internet of Things we need to move away from such small-scale, vertical application silos, towards a horizontal infrastructure on which a variety of applications can run simultaneously.

This is only possible if connecting a thing to the Internet of Things becomes as simple as plugging it in and switching it on. Such plug and play functionality requires an infrastructure that supports it, starting from the networking level and going beyond it to the application level. This is closely related to the aspects discussed in the section on autonomy. On the networking level, the plug & play functionality has to enable the communication, features like the ones provided by IPv6 are in the directions to help in this process. Suitable infrastructure components have then to be discovered to enable the integration into the Internet of Things. This includes announcing the functionalities provided, such as what can be sensed or what can be actuated.

2. Infrastructure Functionality

The infrastructure needs to support applications in finding the things required. An application may run anywhere, including on the things themselves. Finding things is not limited to the start-up time of an application. Automatic adaptation is needed whenever relevant new things become available, things become unavailable or the status of things changes. The infrastructure has to support the monitoring of such changes and the adaptation that is required as a result of the changes.

3. Semantic Modelling of Things

To reach the full potential of the Internet of Things, semantic information regarding the things, the information they can provide or the actuations they can perform need to be available. It is not sufficient to know that there is a temperature sensor or an electric motor, but it is important to know which temperature the sensor measures: the indoor temperature of a room or the temperature of the fridge, and that the electric motor can open or close the blinds or move something to a different location. As it may not be possible to provide such semantic information by simply switching on the thing, the infrastructure should make adding it easy for users. Also, it may be possible to derive semantic information, given some basic information and additional knowledge, e.g. deriving information about a room, based on the information that a certain sensor is located in the room. This should be enabled by the infrastructure.

1. **Physical Location and Position:** As the Internet of Things is strongly rooted in the physical world, the notion of physical location and position are very important, especially for finding things, but also for deriving knowledge. Therefore, the infrastructure has to support finding things according to location (e.g. geo-location-based discovery). Taking mobility into account, localization technologies will play an important role for the Internet of Things and may become embedded into the infrastructure of the Internet of Things.

2. **Security and Privacy:** In addition, an infrastructure needs to provide support for security and privacy functions including identification, confidentiality, integrity, non-repudiation authentication and authorization. Here the heterogeneity and the need for interoperability among different ICT systems deployed in the infrastructure and the resource limitations of IoT devices (e.g., Nano sensors) have to be taken into account.

3. **Infrastructure-related Research Questions:** Based on the description above of what an infrastructure for the Internet of Things should look like, we see the following challenges and research questions:

   (i) How can the plug and play functionality be achieved taking into account the heterogeneity of the underlying technology?

   (ii) How should the resolution and discovery infrastructure look to enable finding things efficiently?

   (iii) How can monitoring and automatic adaptation be supported by the infrastructure?

(iv) How can semantic information be easily added and utilized within the infrastructure?

(v) How can new semantic information be derived from existing semantic information based on additional knowledge about the world, and how can this be supported by the infrastructure?

(vi) How can the notion of physical location be best reflected in the infrastructure to support the required functionalities mentioned above?

(vii) How should the infrastructure support for security and privacy look?

(viii) How can the infrastructure support accounting and charging as the basis for different IoT business models?

(ix) How we can provide security and privacy functions at infrastructure level on the basis of heterogeneous and resource limited components of the infrastructure?

1.5 NETWORKS AND COMMUNICATIONS

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

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

Networking Technology

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

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

1. **Complexity of the Networks of the Future:** A key research topic will be to understand the complexity of these future networks and the expected growth of complexity due to the growth of Internet of Things. The research results of this topic will give guidelines and timelines for defining the requirements for network functions, for network management, for network growth and network composition and variability [91]. Wireless networks cannot grow without such side effects as interference.

2. **Growth of Wireless Networks:** Wireless networks especially will grow largely by adding vast amounts of small Internet of Things devices with minimum hardware, software and intelligence, limiting their resilience to any imperfections in all their functions. Based on the research of the growing network complexity, caused by the Internet of Things, predictions of traffic and load models will have to guide further research on unfolding the predicted complexity to real networks, their standards and on-going implementations.

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

3. **Mobile Networks:** Applications such as body area networks may develop into an autonomous world of small, mobile networks being attached to their bearers and being connected to the Internet by using a common point of contact.

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

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

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

   The Internet and the Internet of Things will have access to large parts of these networks. Further sections may be only represented by a top access node or may not be visible at all globally. Some networks will by intention be shielded against external access and secured against any intrusion on multiple levels.

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

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

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

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

Disruptive developments are to be expected by analysing the energy re
of current solutions and by going back to principles of communicatio
optical and wireless information transfer. Research done by Bell Labs
years shows that networks can achieve an energy efficiency increase o
of 1,000 compared to current technologies .

The results of the research done by the Green Touch consortium [96]
integrated into the development of the network technologies of the futu
network technologies have to be appropriate to realise the Internet o
and the Future Internet in their most expanded state to be anticipate
imagination of the experts.

Communication Technology

The communication technology are as follows:

1. **Unfolding the Potential of Communication Technologies:** The researc
at communication technology to be undertaken in the coming decade w
to develop and unfold all potential communication profiles of Internet of
devices, from bit-level communication to continuous data streams, from s
connections to connections being always on, from standard services to eme
modes, from open communication to fully secured communication, sp
applications from local to global, based on single devices to globally-dist
sets of devices.

   Based on this research the anticipated bottlenecks in communications
networks and services will have to be quantified using appropriate theo
methods and simulation approaches. Communications technologies for the
Internet and the Internet of Things will have to avoid such bottlenec
construction not only for a given status of development, but for the whol
to fully developed and still growing nets.

2. **Correctness of Construction:** Correctness of construction [100] of the
system is a systematic process that starts from the small systems running
devices up to network and distributed applications. Methods to prov
correctness of structures and of transformations of structures will be requ
including protocols of communication between all levels of communications
used in the Internet of Things and the Future Internet.

   These methods will be essential for the Internet of Things devices and system
the smallest devices will be implemented in hardware and many types wi
be programmable. Interoperability within the Internet of Things will be a
even if such proof methods are used systematically.

3. An Un
betwee
multico
compu
in the I
shall b
includi

   In this
best
comm

4. Energ
types
time;
have
throu
expe
appli
mini
all la

5. Chal
solu
mini
with
dom
corr

6. Dis
alre
exis
wit
dev
poi

1.6

Th
way ente

3. **An Unified Theoretical Framework for Communication:** Communication between processes [101] running within an operating system on a single or multicore processor, communication between processes running in a distributed computer system [102], and the communication between devices and structures in the Internet of Things and the Future Internet using wired and wireless channels shall be merged into a unified minimum theoretical framework covering and including formalized communication within protocols.

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

4. **Energy-Limited Internet of Things Devices and their Communication:** Many types of Internet of Things devices will be connected to the energy grid all the time; on the other hand a significant subset of Internet of Things devices will have to rely on their own limited energy resources or energy harvesting throughout their lifetime. Given this spread of possible implementations and the expected importance of minimum-energy Internet of Things devices and applications, an important topic of research will have to be the search for minimum energy, minimum computation, slim and lightweight solutions through all layers of Internet of Things communication and applications.

5. **Challenge the Trend to Complexity:** The inherent trend to higher complexity of solutions on all levels will be seriously questioned – at least with regard to minimum energy Internet of Things devices and services. Their communication with the access edges of the Internet of Things network shall be optimized cross domain with their implementation space and it shall be compatible with the correctness of the construction approach.

6. **Disruptive Approaches:** Given these special restrictions, non-standard, but already existing ideas should be carefully checked again and be integrated into existing solutions, and disruptive approaches shall be searched and researched with high priority. This very special domain of the Internet of Things may well develop into its most challenging and most rewarding domain – from a research point of view and, hopefully, from an economical point of view as well.

1.6 PROCESSES OF IOT

The deployment of IoT technologies will significantly impact and change the way enterprises do business as well as interactions between different parts of the society, affecting many processes. To be able to reap the many potential benefits that have

been postulated for the IoT, several challenges regarding the modelling and execution of such processes need to be solved in order to see wider and in particular commercial deployments of IoT . The special characteristics of IoT services and processes have to be taken into account and it is likely that existing business process modelling and execution languages as well as service description languages such as USDL , will need to be extended.

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

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

2. **Processes Dealing with Unreliable Data**

   When dealing with events coming from the physical world (e.g., via sensors or signal processing algorithms), a degree of unreliability and uncertainty is introduced into the processes. If decisions in a business process are to be taken based on events that have some uncertainty attached, it makes sense to associate each of these events with some value for the quality of information (QoI). In simple cases, this allows the process modeller to define thresholds: e.g., if the degree of certainty is more than 90%, then it is assumed that the event really happened. If it is between 50% and 90%, some other activities will be triggered to determine if the event occurred or not. If it is below 50%, the event is ignored. Things get more complex when multiple events are involved: e.g., one event with 95% certainty, one with 73%, and another with 52%.

   The underlying services that fire the original events have to be programmed to attach such QoI values to the events. From a BPM perspective, it is essential that

such information can be captured, processed and expressed in the modelling notation language, e.g. BPMN. Secondly, the syntax and semantics of such QoI values need to be standardized. Is it a simple certainty percentage as in the examples above, or should it be something more expressive (e.g., a range within which the true value lies)? Relevant techniques should not only address uncertainty in the flow of a given (well-known) IoT-based business process, but also in the overall structuring and modelling of (possibly unknown or unstructured) process flows. Techniques for fuzzy modelling of data and processes could be considered.

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

4. **Highly Distributed Processes:** When interaction with real-world objects and devices is required, it can make sense to execute a process in a decentralized fashion. As stated in [107], the decomposition and decentralization of existing business processes increases scalability and performance, allows better decision making and could even lead to new business models and revenue streams through entitlement management of software products deployed on smart items.

For example, in environmental monitoring or supply chain tracking applications, no messages need to be sent to the central system as long as everything is within the defined limits. Only if there is a deviation, an alert (event) needs to be generated, which in turn can lead to an adaptation of the overall process. From a business process

modelling perspective though, it should be possible to define the process centr
including the fact that some activities (i.e., the monitoring) will be done remot
Once the complete process is modelled, it should then be possible to deploy the rel
services to where they have to be executed, and then run and monitor the compl
process. Relevant research issues include tools and techniques for the synthesis,
verification and the adaptation of distributed processes, in the scope of a volat
environment (i.e. changing contexts, mobility, internet connected objects/devices th
join or leave).

1.7 DATA MANAGEMENT

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

There are many technologies and factors involved in the "data management" within the IoT context. Some of the most relevant concepts which enable us to understand the challenges and opportunities of data management are:

1. Data Collection and Analysis
2. Big Data
3. Semantic Sensor Networking
4. Virtual Sensors

1. Data Collection and Analysis (DCA)

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

2. Big Data

Big data is about the processing and analysis of large data repositories, so disproportionately large that it is impossible to treat them with the conventional tools of analytical databases. Some statements suggest that we are entering the "Industrial Revolution of Data," [108], where the majority of data will be stamped out by machines. These machines generate data a lot faster than people can, and their production rates will grow exponentially with Moore's Law. Storing this data is cheap, and it can be mined for valuable information.

3. Semantic Sensor Netwo

The information collecte
resources and services on th
intelligence, enabling the c
services which could revolu
services and applications in
and also the network resou
networks that are often re
allow software agents and
data.

There are currently o
to apply semantic Web t
(SSW) proposes annotati
metadata. This approach
to extend them with ser
facilitate access to senso
also working on develo
sensor, observation an
for this purpose, are fu

However, associa
the data is also an imp
applications, front-er
interpret links and re
also other resources.
of the data as netw
information (i.e., se
networks.

Emergence o
data consumers to
the Web. By relati
measurement feat
integrate physical
business intellige
making systems

3. Semantic Sensor Networks and Semantic Annotation of Data

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

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

However, associating this data to the existing concepts on the Web and reasoning the data is also an important task to make this information widely available for different applications, front-end services and data consumers. Semantics allow machines to interpret links and relations between different attributes of a sensor description and also other resources. Utilising and reasoning this information enables the integration of the data as networked knowledge. On a large scale this machine interpretable information (i.e., semantics) is a key enabler and necessity for the semantic sensor networks.

Emergence of sensor data as linked-data enables sensor network providers and data consumers to connect sensor descriptions to potentially endless data existing on the Web. By relating sensor data attributes such as location, type, observation and measurement features to other resources on the Web of data, users will be able to integrate physical world data and the logical world data to draw conclusions, create business intelligence, enable smart environments, and support automated decision-making systems among many other applications.

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

4. Virtual Sensors

A virtual sensor can be considered as a product of spatial, temporal and/ thematic transformation of raw or other virtual sensor producing data with necess provenance information attached to this transformation. Virtual sensors and actuat are a programming abstraction simplifying the development of decentralized WS applications [117]. The data acquired by a set of sensors can be collected, process according to an application-provided aggregation function, and then perceived as t reading of a single virtual sensor. Dually, a virtual actuator provides a single ent point for distributing commands to a set of real actuator nodes.

Complex Event Processing

A concept linked with the notion and appearance of "Virtual Sensors" is th Complex Event Processing, in the sense that Virtual Sensors can be used to implemen "single sensors" from complex and multiple (actual) sensors or various data sources thus providing a seamless integration and processing of complex events in a sensor (o Data Collection and Analysis) platform or system.

Complex event processing (CEP) is an emerging network technology that creates actionable, situational knowledge from distributed message-based systems, databases and applications in real time or near real time. CEP can provide an organization with the capability to define, manage and predict events, situations, exceptional conditions, opportunities and threats in complex, heterogeneous networks. Many have said that advancements in CEP will help advance the state-of-the-art in end-to-end visibility for operational situational awareness in many business scenarios (The CEP Blog) . These scenarios range from network management to business optimization, resulting in enhanced situational knowledge, increased business agility, and the ability to more accurately (and rapidly) sense, detect and respond to business events and situations.

CEP is a technology for extracting higher level knowledge from situational information abstracted from processing sensory information and for low-latency filtering, correlating, aggregating, and computing on real-world event data. It is an emerging network technology that creates actionable, situational knowledge from distributed message-based systems, databases and applications in real-time or near real-time.

Types of CEP

Most CEP solutions and concepts can be classified into two main categories:

1. **Computation-oriented CEP:** Focused on executing on-line algorithms as a response to event data entering the system. A simple example is to continuously calculate an average based on data from the inbound events
2. **Detection-oriented CEP:** Focused on detecting combinations of events called event patterns or situations. A simple example of detecting a situation is to look for a specific sequence of events.

Some of the research topics for the immediate future in the context of CEP are:

(i) **Distributed CEP:** Since CEP core engines usually require powerful hardware and complex input data to consider, it is not easy to design and implement distributed systems capable of taking consistent decisions from non-centralised resources.

(ii) **Definition of Standardised Interfaces:** Currently, most of the CEP solutions are totally proprietary and not compliant with any type of standard format or interface. In addition, it is not easy to integrate these processes in other systems in an automated way. It is essential to standardise input and output interfaces in order to make CEP systems interoperable among themselves (thus enabling exchanging of input events and results) and to ease integration of CEP in other systems, just as any other step in the transformation or processing of data.

(iii) **Improved Security and Privacy Policies:** CEP systems often imply the handling of "private" data that are incorporated to decision taking or elaboration of more complex data. It is necessary that all processes and synthetic data can be limited by well-defined rules and security constraints (that must be measurable, traceable and verifiable).

1.8 SECURITY

As the IoT becomes a key element of the Future Internet and a critical national international infrastructure, the need to provide adequate security for the IoT infrastructure becomes ever more important. Large-scale applications and services based on the IoT are increasingly vulnerable to disruption from attack or information theft. Advances are required in several areas to make the IoT secure from those with malicious intent, including.

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

1.9 DEVICE LEVEL ENERGY ISSUES

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

1. Low Power Communication

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

(i) IEEE 802.15.4 has developed a low-cost, low-power consumption, low complexity, low to medium range communication standard at the link and the physical layers [122] for resource constrained devices.

(ii) Bluetooth low energy (Bluetooth LE, [123]) is the ultra-low power version of the Bluetooth technology [124] that is up to 15 times more efficient than Bluetooth.

(iii) Ultra-Wide Bandwidth (UWB) Technology [125] is an emerging technology in the IoT domain that transmits signals across a much larger frequency range than conventional systems. UWB, in addition to its communication capabilities, it can allow for high precision ranging of devices in IoT applications.

(iv) RFID/NFC proposes a variety of standards to offer contact less solutions. Proximity cards can only be read from less than 10 cm and follows the ISO 14443 standard [126] and is also the basis of the NFC standard. RFID tags or vicinity tags dedicated to identification of objects have a reading distance which can reach 7 to 8 meters.

Nevertheless, front-end architectures have remained traditional and there is now a demand for innovation. Regarding the ultra-low consumption target, super-regenerative have proven to be very energetically efficient architectures used for Wake-Up receivers. It remains active permanently at very low power consumption, and can trigger a signal to wake up a complete/standard receiver [127, 128]. In this field, standardisation is required, as today only proprietary solutions exist, for an actual gain in the overall market to be significant.

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

2. Energy Harvesting

Four main ambient energy sources are present in our environment: mechanical energy, thermal energy, radiant energy and chemical energy. These sources are characterized by different power densities (Figure). Energy harvesting (EH) must be chosen according to the local environment. For outside or luminous indoor environments, solar energy harvesting is the most appropriate solution. In a closed environment thermal or mechanical energy may be a better alternative. It is mainly

the primary energy source power density in the considered environment that de
the electrical output power that can be harvested and not the transducer itself

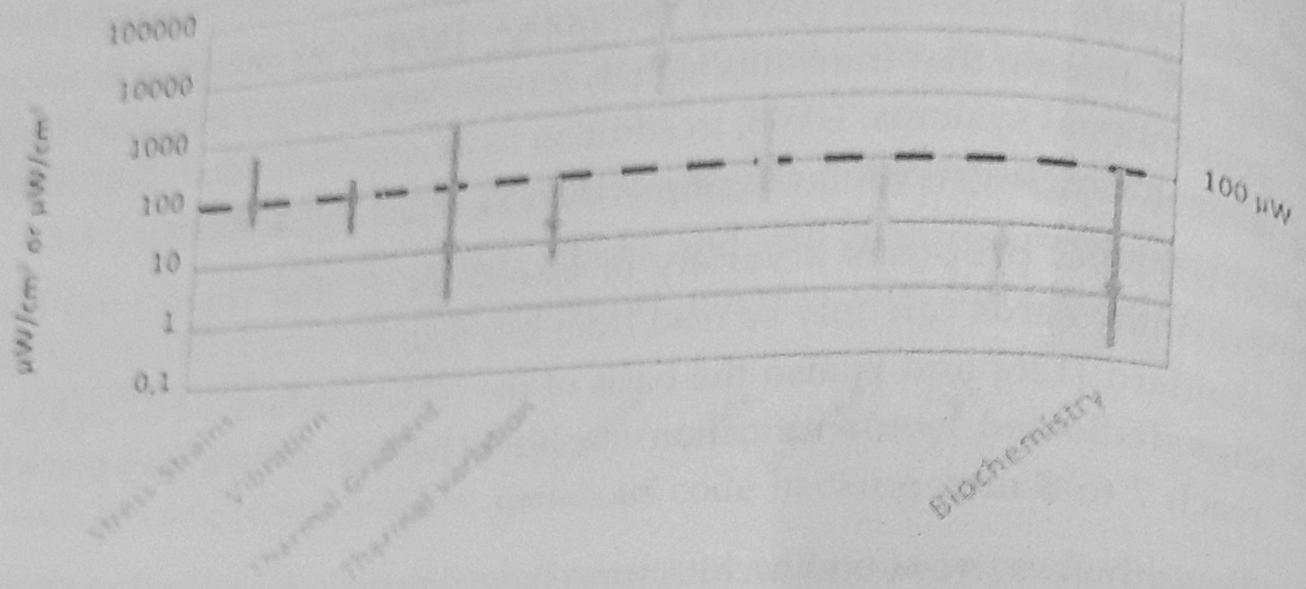


Figure: Ambient sources' power densities before conversion.

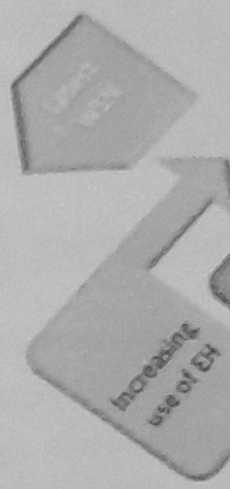
The figure also shows that, excluding "sun-outside", 10–100ìW is a fair order of magnitude for 1 cm2 or 1 cm3-EH output power.

Low power devices are expected to require 50 mW in transmission mode and less in standby or sleep modes. EH devices cannot supply this amount of energy in a continuous active mode, but instead intermittent operation mode can be used in EH-powered devices. The sensor node's average power consumption corresponds to the total amount of energy needed for one measurement cycle multiplied by the frequency of the operation

3. Future Trends and Recommendations

In the future, the number and types of IoT devices will increase, therefore interoperability between devices will be essential. More computation and yet less power and lower cost requirements will have to be met. Technology integration will be an enabler along with the development of even lower power technology and improvement of battery efficiency. The power consumption of computers over the last 60 years was analysed in [133] and the authors concluded that electrical efficiency of computation has doubled roughly every year and a half. A similar trend can be expected for embedded computing using similar technology over the next 10 years. This would lead to a reduction by an order of 100 in power consumption at same level of computation. Allowing for a 10 fold increase in IoT computation, power consumption

should still be reduced b
requirements for different



Figur

On the other h
to the energy cons
harvesters, we exp
g to 30ìW/g) and
energy harvesters

Actually, th
and Play (PnP) de
the same time, w
a factor of 10. A
new markets,
thermoelectric s
order to convert
improvement w
superlattices o

For solar
and robust sol
today's soluti
the photovol
energy in eve

should still be reduced by an order of 10. An example of power consumption requirements for different devices is given in Figure.

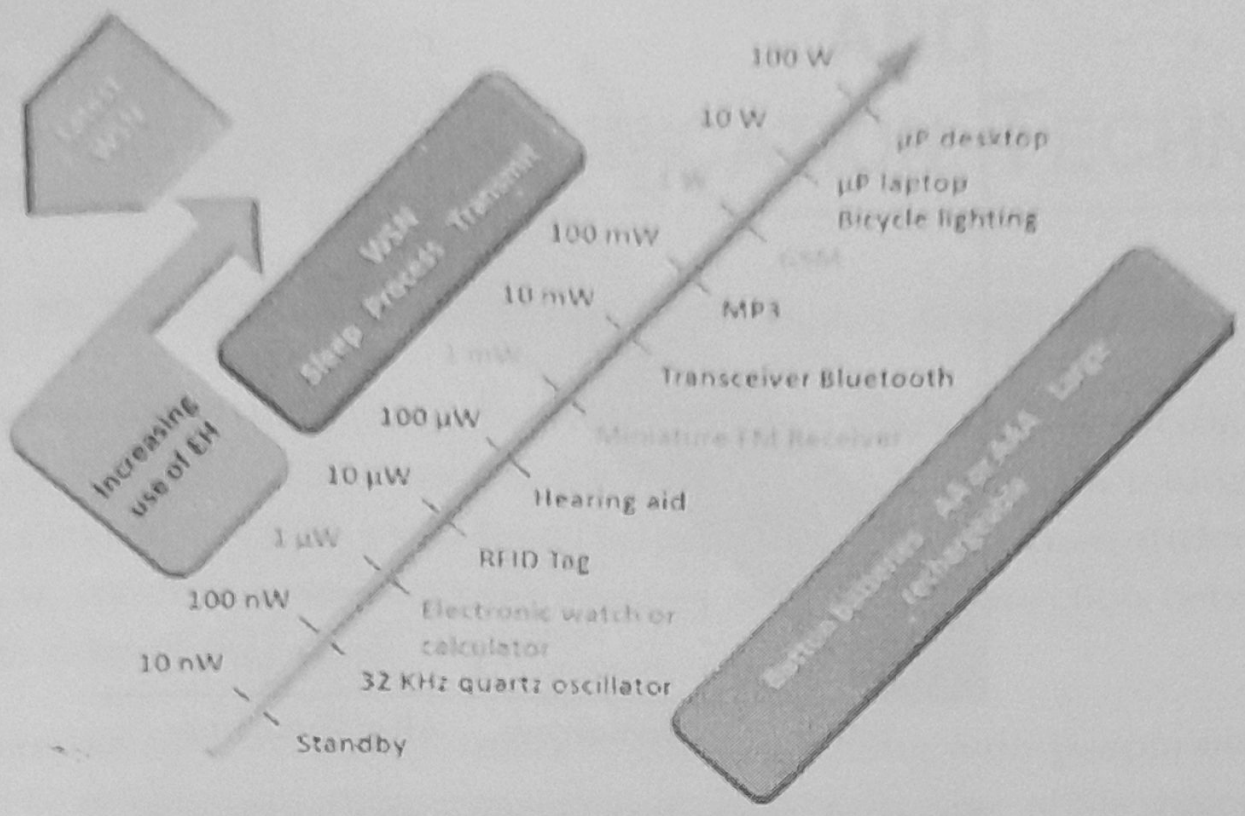


Figure : Power Consumption requirements for different devices

On the other hand, energy harvesting techniques have been explored to respond to the energy consumption requirements of the IoT domain. For vibration energy harvesters, we expect them to have higher power densities in the future (from 10iW/g to 30iW/g) and to work on a wider frequency bandwidth. A roadmap of vibration energy harvesters is provided in Figure.

Actually, the goal of vibration energy harvesters' researchers is to develop Plug and Play (PnP) devices, able to work in any vibrating environment, within 10 years. In the same time, we expect basic functions' energy consumption to decrease by at least a factor of 10. All these progresses will allow vibration energy harvesters to attract new markets, from industry to healthcare or defence. The main challenge for thermoelectric solutions is to increase thermoelectric materials' intrinsic efficiency, in order to convert a higher part of the few mW of thermal energy available. This efficiency improvement will be mainly performed by using micro and nanotechnologies (such as superlattices or quantum dots).

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

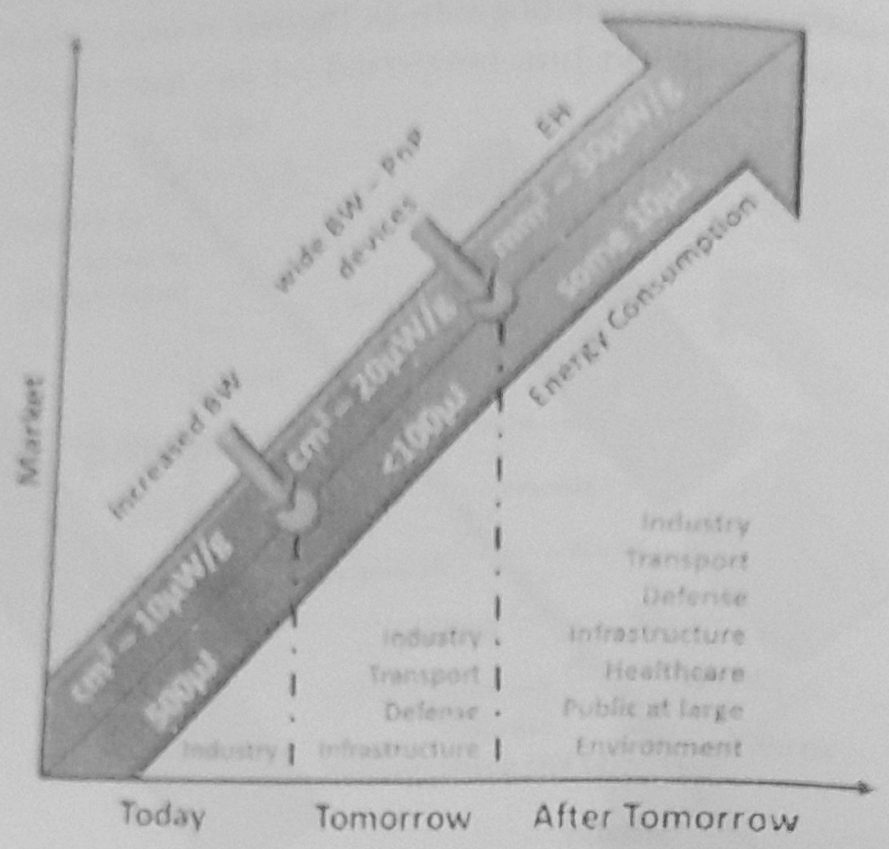


Figure : Roadmap for vibration energy harvesters.

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

IMPORTANT QUESTIONS

1. Define Internet of Things (IOT). Explain about IOT vision.
2. Explain about Strategic research and innovation directions.
3. What are the Iot Applications?
4. Explain about IOT Related future technologies and Infrastructure.
5. Discuss briefly about Networks and communications technology.
6. Explain the Networks and communications Processes.
7. What is Data Management? Explain about Security of IOT andDevice level energy issues.

UNIT 2

2.1 INT

The wo
it is changing
Today, com
Moreover, i
opposite sic

Inter
It could be
internet c
addition,
Skype, G
custome

In
Faceboo
blogs a

2.1.1

and a
pack
to re
was

wit
an
w

TA