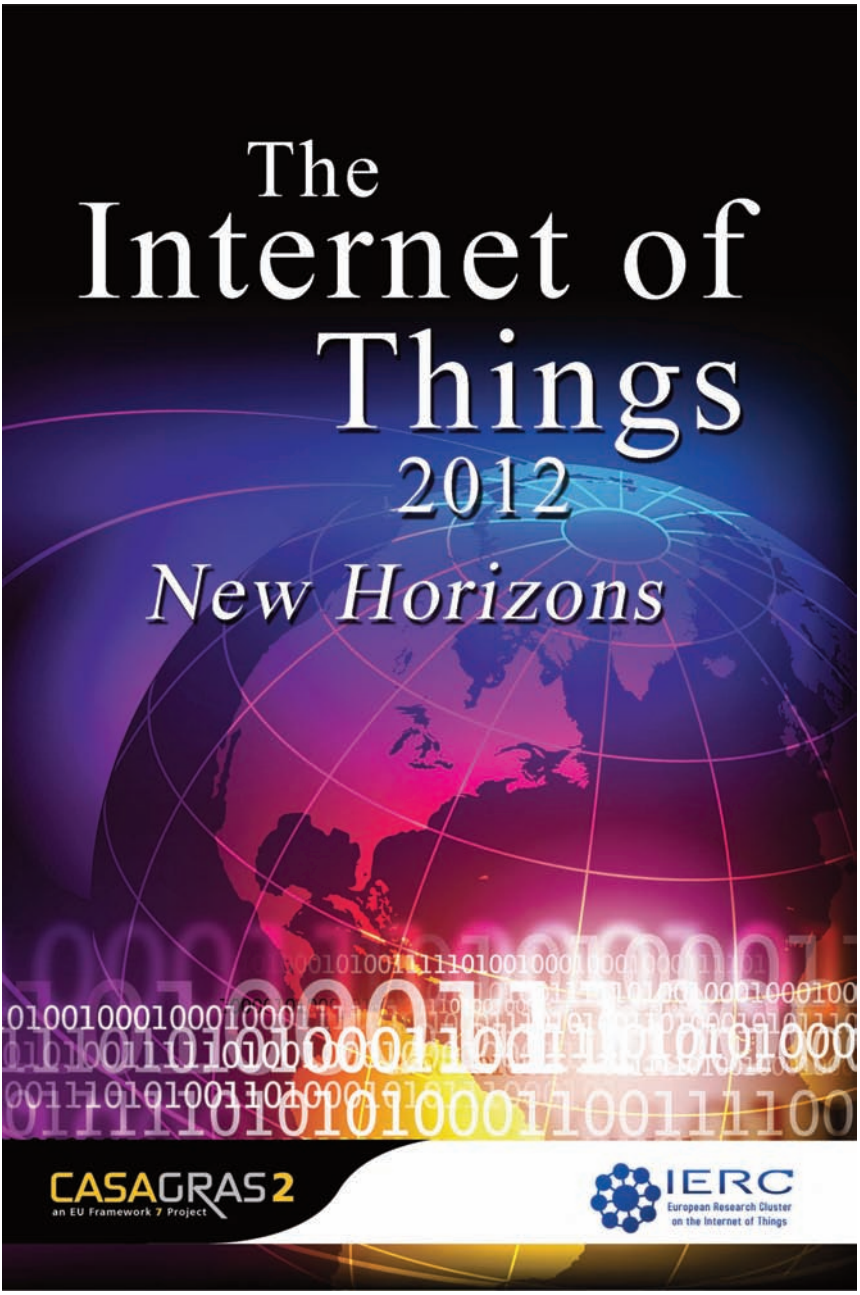


"I am neither an optimist nor pessimist, but a possibilist."
Max Lerner

The Internet of Things 2012

New Horizons

Edited by:

Ian G Smith

Technical Editors:

Ovidiu Vermesan Peter Friess Anthony Furness

ISBN hard cover: **978 - 0 - 9553707 - 9 - 3**

Design and layout: Martin Pitts
studio@smartidentification.org

Printed by Platinum **www.platinumprint.com**

published in Halifax, UK

2012©

IERC - Internet of Things
European Research Cluster

3rd edition of the Cluster Book

This year's Cluster Book is a landmark achievement for scientists and engineers working to carry forward the development of knowledge in the domain of the Internet of Things. It is the place where internationally renowned experts join together to celebrate a breathtaking record of achievement and to call for action from industry, academia, government, and civil society to create and sustain a culture of responsible innovation and social responsibility for the people of the world.

There are multiple dimensions to this Cluster Book: it is about the complex interrelationship between objects and networks – how we interact with objects, how the Internet influences the way we 'sense' reality, and how technology both helps and hinders us from knowing ourselves; it is about power and knowledge, insight and inspiration, culture and experience, physics and metaphysics.

The Cluster is assuming its responsibilities in contributing to wider public policy and innovation issues by having a permanent seat in the Commission's IoT Expert Group, backing the work of bi-lateral international expert groups and national advisory boards while linking to European Technology Platforms and providing input in the context of preparations for the Horizon 2020 Programme on European Research and Innovation.

The book is published in partnership with the EU FP7 CASAGRAS2 project which concludes its activities this year.

www.internet-of-things-research.eu

Partners:	• Smart Identification Ltd.	UK
	• Praxis Consultants	UK
	• Stiftelsen SINTEF	Norway
	• FEIG Electronic GmBH	Germany
	• China Electronics Standardization Institute	China (People's Republic of)
	• Sitronics Labs	Russia
	• Fundacio de Apoio as Universidade de Sao Paulo	Brazil
	• Custommedia Sdn Bhd	Malaysia
	• High Tech Aid USA	USA
	• Global ICT Standardisation Forum for India	India
	• Electronics And Telecommunications Research Institute	Korea (Republic of)
	• Yokusuka Telecom Research Park Kabu Shiki Gaisha	Japan
	• European Telecommunications Standards Institute	France
	• Birkbeck College - University of London	UK
	• University of Bradford	UK

Co-ordinator: Ian Smith Smart Identification, UK
Email:ian@smartidentification.org
www.iot-casagras.org

contents

"The two words information and communication are often used interchangeably, but they signify quite different things. Information is giving out; communication is getting through."
Sydney Harris

Internet of Things

Connected! All the time! Everywhere!

The world as we have created it is a process of our thinking. It cannot be changed without changing our thinking."
Albert Einstein

Ethical implications of tomorrow's digital society

By Neelie Kroes

The digital society raises questions not just technological or political – but philosophical, social, legal, ethical and psychological.

The ethical implications of tomorrow's internet are complex, and require broad public debate, with an active role of all stakeholders including public policy makers, business and civil society. While ICT offers opportunities like a platform for freedom of speech, social contact and enhanced democratic accountability, there are also ethical problems online: for example important questions like privacy and data protection. As ICT becomes ever more important, pervasive and useful, we need to raise and discuss these ethical questions.

The European Group on Ethics in Science and Technology (EGE) have presented a very useful reflection on the ethics of the digital economy and it's impacts on society. I'm glad that in particular they looked at the ethical implications of the 'Internet of Things': in no other area are the implications of the future of the Internet quite so vivid.

The Internet of Things promises to bring smart devices everywhere, from the fridge in your home, to sensors in your car; even in your body. Those applications offer significant benefits: helping users save energy, enhance comfort, get better healthcare and increased independence: in short meaning happier, healthier lives. But they also collect huge amounts of data, raising privacy and identity issues. That's why our Horizon 2020 programme proposes to invest in research for education and research into the ethical, legal, social and environmental areas of ICT.

For the Internet of Things to take off people need to feel a degree of comfort and control, and business needs stability and predictability to invest. That is why the issue of ethics and understanding needs, concerns and desires of people and businesses is so important. I hope we will make progress together in building a conducive environment for the Internet of Things and the future Internet.

Neelie Kroes,

Vice President of the European Commission and Commissioner Digital Agenda Europe

Towards Connectobjectome: The age when the totality of all objects become connected

By Gérald Santucci

This year's Cluster Book is a landmark achievement for scientists and engineers working to carry forward the development of knowledge in the domain of the Internet of Things. It is the place where internationally renowned experts join together to celebrate a breathtaking record of achievement and to call for action from industry, academia, government, and civil society to create and sustain a culture of responsible innovation and social responsibility for the people of the world.

Yes, the challenge of the next decade is to see that the benefits of the Internet of Things revolution are shared by all the citizens of the world, not just those fortunate enough to live in the most developed and emerging economies. This is why the European Commission has been consulting widely through a structured process with key stakeholders, since 2010, to devise a regulatory framework which puts in place the conditions to maximise the use of IoT potential whilst minimising risks. At the heart of the new framework is the vision of an Internet of Things that enables not only large corporations to thrive in ever-competitive environments, but also users, citizens, ordinary people without money and without power, to start up platforms, products, open source soft- and hardware, to develop good practices of sharing 'things', and to reap the full benefits of social networks, including micro- and supermicro-size social networks, as these networks get closer to the objects through, for instance, smartphone apps.

History will judge us.

We can either continue down the perilous path of considering the Internet of Things as the mere application of current core technologies, in particular Radio Frequency Identification, or insist on a new direction. If we don't

change course, if we look to the challenges ahead with the concepts of today, if we let ourselves be dominated by selfishness or easiness, or pulled into turf battles, we know what lies ahead – less economic growth, less sustainability, less jobs, and a society fragmented along sectarian, irreconcilable lines. We must be beyond ideological debates – the outer ends of privacy upholders and 'I-have-nothing-to-hide' defenders will never meet in a harmonious way, and hence, in the complex era of the Internet of Things, the only constructive approach requires the establishment of a new "social contract" whereby as many stakeholders as possible cooperate to define shared values and whereby acceptance is a process.

The wrong way to respond to the challenge of the Internet of Things is through a race to the bottom, where nations and organisations compete to see who can provide IoT applications, platforms and services with the lowest protection for citizens and the cheapest costs. The right way is through an ambitious global strategy, pursued with commitment and energy over several years. This strategy should recognise the important benefits of the Internet of Things for society as a whole, such as in smart transportation systems, smart cities, pollution control, natural hazards monitoring, and sustainable consumption, and it should foster public-private partnerships to invest in ethics-, privacy- and security-by-design IoT systems that enhance innovation, entrepreneurship, and user empowerment.

"May you live in interesting times."

There's an old blessing that I love to quote – "May you live in interesting times." We certainly find ourselves in difficult, complex, and, yes, interesting times today, with the many IoT challenges facing Europe. None of these challenges is beyond our capacity to solve. To take only one example, we start to understand that the public debate on the Internet of Things should not be framed in the context of today's discussions regarding identification technologies where human agency is still possible (match-on-card biometrics, RFID tag deactivation on retail goods, 'silence of the chips', privacy impact assessments, 'right to be forgotten', etc.), but should take the full measure of objects taking decisions autonomously without any user intervention, without possible user awareness, and "on user behalf". Such an approach opens a promising possibility for a collective reflection on challenging ethical values like the sense of identity, user consent, fairness and equity.

The awesome task then is not simply to innovate – and that is challenging enough – but to innovate in ways that reconcile the complex nodes of technology and society around new ethics.

Now, by itself, the simple recognition that we are all in this together won't usher in a new era of cooperation. What comes of this moment is up to us; it will be determined not by whether we can write and publish papers together today, but whether we can work together tomorrow. After four years of work within the IoT European Research Cluster, I believe we can. And of course I believe we must. That's what the people who will read this Cluster Book expect of us.

The world has changed

The world has changed, and for many in Europe, the change has been, and still is, painful, especially since the 2008 financial crisis caused by widespread failures in government regulation, corporate mismanagement and heedless risk-taking by stock exchanges. We see it in the shuttered windows of once booming factories, and the vacant storefronts of once busy streets. We see it in the frustrations of citizens who have lost their jobs or seen their pay slips dwindle – people who feel like the rules have been changed in the middle of the game. They're right, the rules have changed. ICT revolutions since the invention of the first single-chip microprocessor in 1971 have transformed the way we live, work and do business. By giving autonomy to objects, and by blurring the line between bits and atoms, the Internet of Things will produce another quantum leap forward on both the technological and societal levels by erasing boundaries between information entities and moving the reality across traditional legal, business, social and cultural concepts towards a single environment.

The scale of the challenge is unprecedented and Europe's response must match the aspirations of people across territories, lifestyles and social classes. The first step in winning the future is enhancing technological innovation. The second step is taking social innovation to scale, i.e. providing leeway for the renewal of services (commercial or public) and of the main socio-economic forces that drive our societies. The third step is fostering global standards, and in particular to achieve full interoperability of networks and services.

There are multiple dimensions to this Cluster Book: it is about the complex interrelationship between objects and networks – how we interact with

objects, how the Internet influences the way we 'sense' reality, and how technology both helps and hinders us from knowing ourselves; it is about power and knowledge, insight and inspiration, culture and experience, physics and metaphysics.

> The book sets the European and global scene of the Internet of Things, explains what Europe is doing on key issues like addressing, identification and resolution, architecture and standards, presents a model of IoT Governance, describes the Cluster's Strategic Research Roadmap, and provides a bunch of interesting updates on business developments. It takes us forward to the time when all the objects on Earth become connected to the Internet - welcome at *connectobjectome*!

I commend the Editors for convening such an impressive group of authors to address the challenging topic of the Internet of Things and also the Authors for their detailed, balanced, and thoughtful approach to the issues.

Gérald Santucci

Towards Dynamism and Self-Sustainability

By Dr. Peter Friess

"For people working in the field of the Internet of Things, the future is the present"

Opportunities and challenges

The Internet of Things (IoT), is a concept which has its roots in various network, sensing and information processing approaches. It is seriously gathering momentum and taking up speed. Today it is irrelevant whether stakeholders and opportunists adopt the IoT term or similar ones like Sensor Networks, Sensor Clouds or infinitively large concepts like Smart Planet. What does matter is that an increasing number of researchers, business evangelists and governmental decision makers feel the potential of stronger context-aware systems including lower or higher forms of decentralised reasoning.

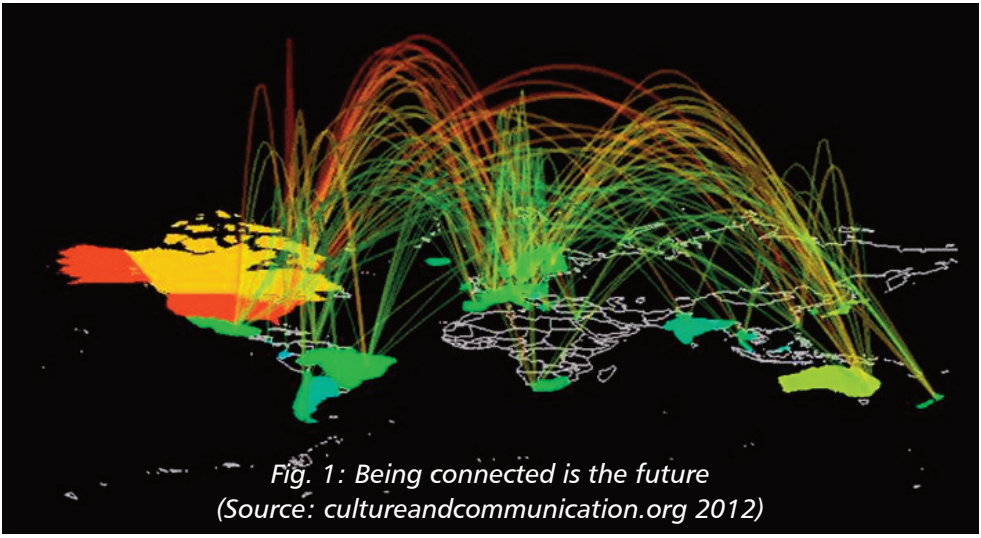


Fig. 1: Being connected is the future (Source: cultureandcommunication.org 2012)

It is also critical that at this very same moment early-adopters and smart followers, in their individual and collective analyses, are sharp enough to embrace on one hand the advantages of new ways of sensing and reasoning, and on the other hand be realistic and convinced about the necessary accompanying measures. The latter will need to ensure safety, trust and liability. At a higher abstract level, smart people must be able to cope with future complexity and new ways of living.

It is certainly not by accident that numerous fields of small and large applications nurture themselves from Internet of Things principles. Two reasons stand out: an increasing push for reduced energy consumption and increased safety in several fields of intervention (energy and construction, transport, catastrophe prevention etc.), the fact that many individuals both in their professional and private spheres are increasingly using multiple electronic personal devices.

The latter is also true for corporate and political executives. Decision making processes have resulted in a stronger push for a new era of connected devices and applications with all possible variations.

"Connected Any-time, Any-place, with Any-thing and Any-one Ideally using Any-path/network and Any-service"

Fig. 2: Dominance of the "Any" paradigm (Source: SINTEF 2011)

In this context the research and development challenges to create a smart world, where physical, digital and virtual worlds would rather converge than diverge, are enormous.

Not only the technical complexity impacts significantly on drawing concise and coherent development lines, it is also the factor of exponential connectivity and thus complexity increase which leads to unnecessary sub-optima solutions and spaces of chaos. In addition, as sincere researchers, leaders and policy makers tend to be concerned with various aspects of social responsibility, research and development efforts need to go hand in hand with communication, exchange, innovation stimulus, self-regulation and regulation.

Fig. 3: Europe's Internet of Things action plan (Source: EC 2011)

The following list of aspects provides a wide but certainly not exhaustive compilation of the current Internet of Things issues at stake:

- Architecture: development and refinement of structural reference frameworks for the arrangement of physical and logical hard - and software components, including questions of object identification, virtualisation and decentralisation; also ensuring interoperability across application sectors.
- Security and Trust issues: development of mechanisms and frameworks (by design) for ensuring that all users in business

and private contexts trust the applications and maintain a certain power of control on their data across the full data and information life cycle.

- Software and middleware platforms: support for analysis and processing of data flows from sensing devices and a high quantity of object instances, complemented with event filtering and management capabilities and including complexity management considerations.
- Interfaces: integration of multi-modal interface approaches for enriching all kinds of man-machine interaction for both changing the user experience and coping with the information density.
- Smart sensors: integration of sensing and reasoning capabilities into networked and energy-harvesting devices.
- Testing and Standardisation: current IoT dispositions are still on-going and effects on mass deployments need to be much better understood. Testing and large-scale pilots are absolutely crucial and should also lead subsequently to standardisation for ensuring interoperability and reducing complexity.
- Business models: a sound exploitation of the IoT business potential is still missing and new business models for the existing incumbents but also new and innovative players need to be developed.
- Societal and ethical implications: the Internet of Things has already started to change our lives virtually but questions about the physical and logical usage coupled with considerations of needs for privacy, inclusiveness of the society and evolution of social behaviour remain very valid and only partly addressed.
- IoT Governance: often misunderstood, IoT Governance is, in particular about the governance of the Things and their context of usage rather than Internet aspects. New models, mechanisms and frameworks covering legal aspects too are necessary for guaranteeing proper trust, identity and liability management.
- International Cooperation: the Internet of Things is a truly global subject which shows interesting application cases in different parts of the world. Moreover, as it will only work if a certain level of

interoperability is maintained, a common understanding among the different nations involved is pivotal.

- Integration of results from other disciplines: basic ICT, robotics, nanotechnology, biomedicine and cognitive sciences provide a rich source of inspiration and applications for developing the Internet of things further on.

Finally it should be mentioned that IoT connects largely to other fields of activities like Cloud approaches, Future Internet, Big data, Smart Cities, and specific European Member State initiatives such as Cyber-Physical Systems.

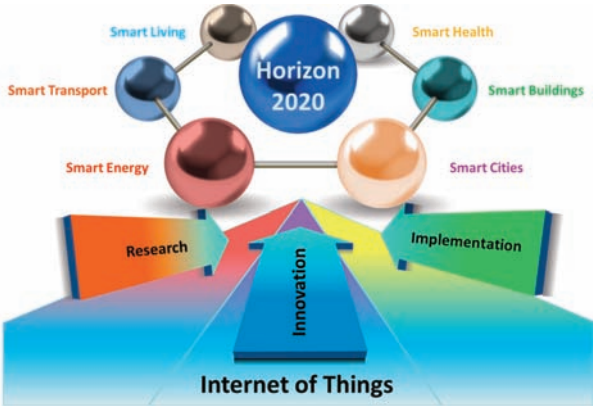


Fig. 4: The Internet of Things innovation arena (Source: IERC 2011)

The Cluster's reply

In this dynamic environment, a few years ago the European Commission created the IERC - Internet of Things European Research Cluster, which today comprises around 40 projects. The role of the Cluster, which has established an excellent reputation, is to provide a light-weight portfolio management approach for overcoming isolated, redundant research and knowledge barriers.

The latter often result due to structural and organization boundaries where the actors are confronted with disperse competencies and conflicting interests. It can be recognized that with the overarching vision of a future

Internet of Things and the present research and policy community, the IERC could take a significant step forward in this regard.

A further vehicle proposed by the IoT European Research Cluster is to link its activities with value creation networks or clusters and innovation/ research incubators to be established in every European Member State of the European Union and associated states. This form of co-research and innovation with the IERC will allow a better coordination of knowledge-producing projects in the area of IoT at the national level with inter-linkages among different countries and cooperation at the European level.

This is expected to generate more cooperation and new business networks, innovative projects by SMEs with universities and technology centres, as well as funding of innovation, investments, venture capital, start-ups and spin-offs.

In the past months the IoT European Research Cluster has maintained its dedication to act as a hub between researchers, business creators, standardization bodies, public authorities and international representatives. Membership is relatively open for interested partners who are willing to engage in the Cluster's activity chains and to provide further linkage for common goals which will enable the IoT vision to happen, establish common research strategic agendas, create final market demand, etc.

Fig. 5: IoT European Research Cluster working structure (Source: IERC 2012)

The working structure of the Cluster is organised around 14 activity chains (ACs) to favour integration in various dimensions. Although this concept has already been presented it is important to say that the structure is reviewed on a yearly basis with the activity chains being confirmed, modified or discarded. The present work structure comprises the following modules:

- **AC01-Architecture approaches and models:** collection and exchange of requirements, creation and implementation of an architecture reference model
- **AC02-Naming, addressing, search, discovery:** analysis and documentation of the (main) naming, addressing and discovery schemes used in the scope of IoT applications and services
- **AC03-Governance issues and models:** development support of an IoT Governance model which respects peculiarities on an international level
- **AC04-Service openness and interoperability:** identification of issues to ensure service openness and to improve semantic and overall IoT technologies' interoperability
- **AC05-Privacy and security issues:** identification of privacy and security issues and corresponding requirements for different IoT applications
- **AC06-Pre-normative and/or pre-regulatory (research):** definition of a standardisation strategy for IoT technology and applications, gap analysis
- **AC07-Cluster support:** adaption of the Strategic Research Agenda, cluster communication (newsletter, IERC blog, websites, overall communication and organisation)
- **AC08-Link to Future Internet initiatives:** liaison with the Future Internet Public Private Partnership (FI-PPP) initiative and the Future Internet Assembly (FIA)
- **AC09-National Cluster Liaison:** contact to and follow-up of IoT Initiatives in the 27 EU Member States and associated European states
- **AC10-International cooperation:** International cooperation and bilateral IoT working groups and initiatives (China, Japan, South Korea, US and more)

- **AC11-Application scenarios and Pilots:** definition of application scenarios for IoT technology, identification of industry needs for IoT applications
- **AC12-Dissemination activities:** support of IoT dissemination activities with focus on the research community in order to enable knowledge sharing
- **AC13-IoT Enabling technologies:** monitoring of present and future enabling technologies to be used in the context of the Internet of Things
- **AC14-Cognitive Technologies for IoT:** identification of opportunities and challenges, definition of cognitive management functionalities and building blocks for the IoT

In addition the IoT European Research Cluster collaborates strongly with the recently established Global IoT Forum, an initiative receiving start-up support from the European Commission. The IoT International Forum is a one-stop shop, a not-for-profit organisation for actors to come together from both the global IoT community and from domains which could benefit from IoT.

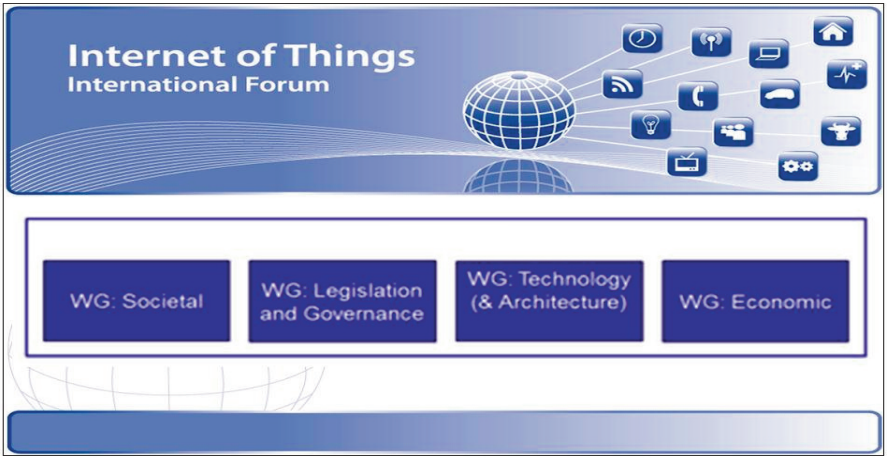


Fig. 6: Workgroups (WG) of the recently established Global IoT Forum (Source: IOT Forum website 2012)

Among the established working groups addressing Economics, Technology, Legislation and Governance issues, major attention will be paid to the Societal work group which provides a forum for the exchange of trends, challenges and barriers relating to societal matters around the Internet of Things.

The future

The Internet of Things is a real vision which has passed its conceptual stage. Although it is being built today it still remains vague as to what will happen when things, homes and cities become smart. In terms of penetration, the Internet of Things could permeate the whole economy and society if the public concerns that generally impede technological change (in particular privacy and security) are addressed and warranted in such a way that trust and enthusiasm are reflected in a strong market demand. Otherwise, should these demand signals not materialise, the Internet of Things would remain limited to a few niche areas (e.g., health care, logistics, manufacturing, security, transportation).

In this book you will find many answers to the questions which are being asked today -

- What is happening on a world-wide scale in the domain of the Internet of Things?
- What are the results and achievements so far in Europe on several dedicated aspects like architecture but also on identification and standardisation issues?
- What should be understood by IoT Governance and what ideas exist for a potential model?
- What are the future research challenges and road-mapping building blocks?
- How are current Internet of Things business perspectives perceived by regional and international players?

After considering the content of this book the reader might well ask what will come next.

The concept of the Internet of Things has been barely understood or served as an appropriate frame for discussion before it has started to get diluted and lose its trendiness. But this could be considered a good sign for the way forward. New players are coming on board. The ideas of the IoT filter into many different application areas and business concepts.

What is important is that in the end the underlying ideas and concepts should serve the present and future society.

Fig. 7: Mood board future society

(Image source: http://wallpaper-s.org 2012)

This article expresses the personal views of the author and in no way constitutes a formal or official position of the European Commission.

Peter Friess is Scientific and Policy Officer, EC-Coordinator IERC (Internet of Things European Research Cluster), European Commission Directorate General Information Society and Media

EUROPE'S IoT STRATEGIC RESEARCH AGENDA 2012

By Dr. Ovidiu Vermesan and...

... Dr. Peter Friess, Dr. Gunter Woysch, Patrick Guillemin, Sergio Gusmeroli, Harald Sundmaeker, Dr. Alessandro Bassi, Dr. Markus Eisenhauer, Dr. Klaus Moessner

1 Internet of Things - The Vision

Internet of Things (IoT) enables the objects in our environment to become active participants, i.e., they share information with other members of the network or with any other stakeholder and they are capable of recognizing events and changes in their surroundings and of acting and reacting autonomously in an appropriate manner. 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 concept goal of the Internet of Things is to enable things to be connected anytime, anyplace, with anything and anyone ideally using any path/ network and any service. Internet of Things is a new revolution of the Internet. Objects make themselves recognizable and they obtain intelligence thanks to the fact that they can communicate information about themselves and they can access information that has been aggregated by other things. For example - alarm clocks will go off early if there's traffic; plants will communicate to the sprinkler system when it's time for them to be watered; running shoes communicate time, speed and distance so that the wearer can compete in real time with people on the other side of the world; medicine containers tell your family members if you forget to take the medicine. All objects can play an active role thanks to their connection to the Internet.

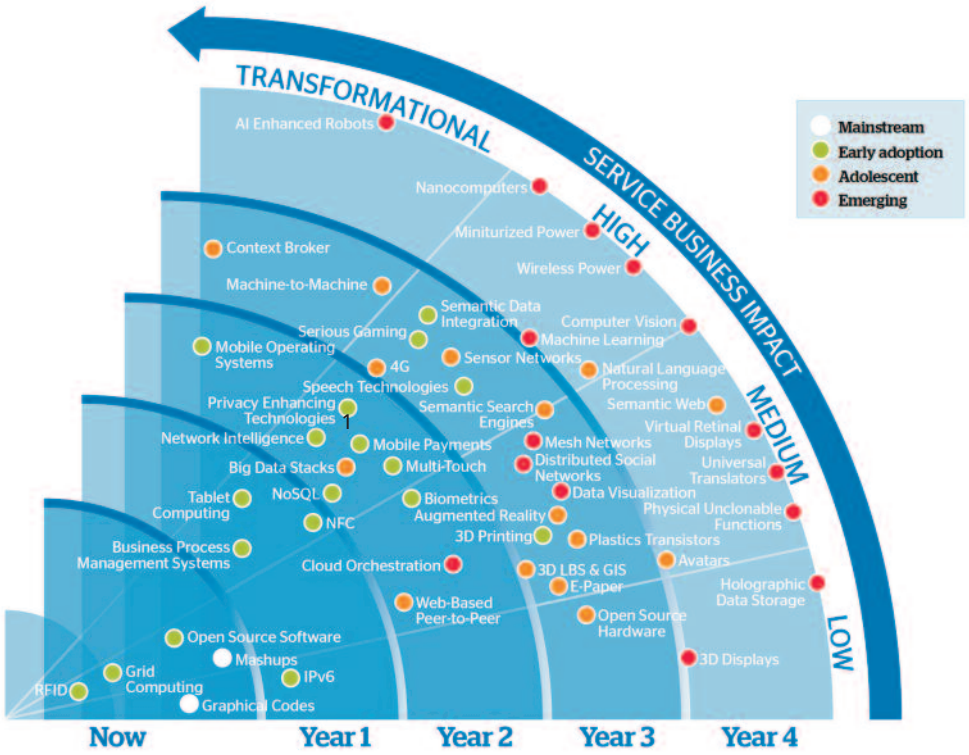


Figure 1 2012+ Enabling Information Technologies Radar [1]

The enabling technologies for Internet of Things such as sensor networks, RFID, M2M, mobile Internet, semantic data integration, semantic search, IPv6, etc. are considered in [1]. The overview raises awareness of the emerging trends, business needs and technologies that will drive innovation. Each trend has been analysed from three perspectives: potential size of impact on your business; likely time to impact your business and maturity. The radar diagram provides a pictorial view of the report's [1] findings, allowing us to quickly understand how disruptive each trend is likely to be and the actions that should be considered.

Communication between computers started with the Electronic Data Interchange that made direct dialogue possible between two PCs. All the computers connected to the Internet can talk to each other and with the connection of mobile phones it has now become mobile [104]. With Internet of Things the communication is extended via Internet to all the things that

surround us. The Internet of Things is much more than M2M communication, wireless sensor networks, M2M, 2G/3G/4G, RFID, etc. These are considered the enabling technologies that make "Internet of Things" applications possible. A vision of the evolution of Internet of Things is illustrated in [104].

1.1 Internet of Things Common Definition

The idea of an Internet of Things started many years ago. Nikola Tesla in an interview with Colliers magazine in 1926 stated[55]: "When wireless is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole.....and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket."

Mark Weiser's Scientific American article on ubiquitous computing 'The Computer for the 21st Century', discuss about the fact that "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it" [102].

Kevin Ashton in an article in RFID Journal declared that: "*I could be wrong, but I'm fairly sure the phrase "Internet of Things" started life as the title of a presentation I made at Procter & Gamble (P&G) in 1999*" [4] .

Neil Gershenfeld published his book "When Things Start to Think" and stated *"in retrospect it looks like the rapid growth of the World Wide Web may have been just the trigger charge that is now setting off the real explosion, as*

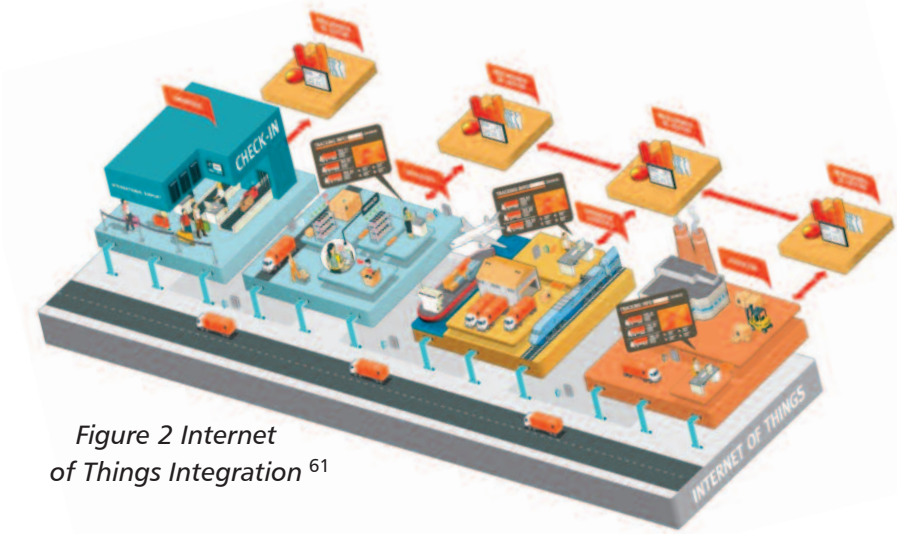


Figure 2 Internet of Things Integration [61]

things start to use the Net." [29]. In another article on "The Internet of Things" the authors stated "*The principles that gave rise to the Internet are now leading to a new kind of network of everyday devices, an "Internet-0"* [30]

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

The Internet of Things offer provides solutions based on integration of information systems and Enterprise Resource Planning (ERP) with enabling technologies such as RFID tags, sensor networks, positioning systems, route planning, Enterprise Application Integration (EAI) middleware as illustrated in [30] .

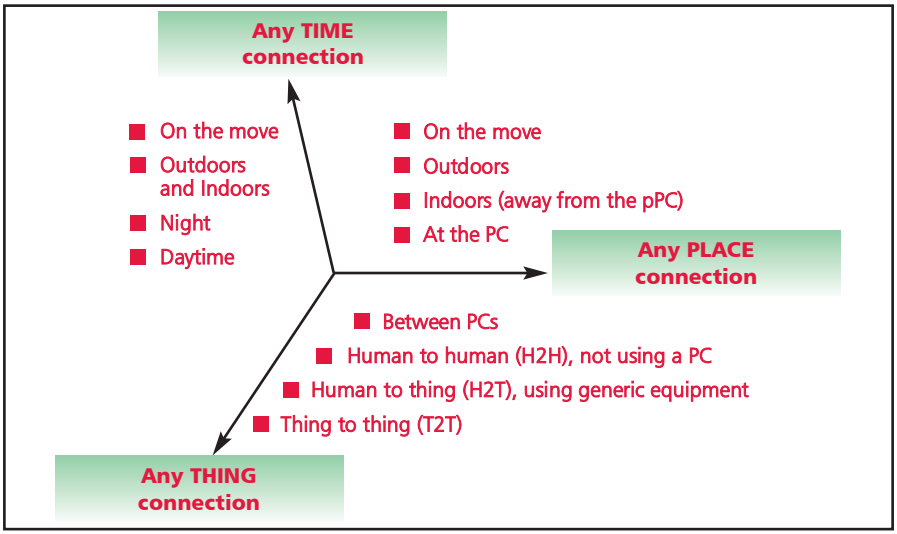


Figure 3 ITU-T Internet of Things (Source: ITU, adopted from Nomura Research Institute)

In this context it is not easy to coin a definition of the "Internet of Things". This has been the experience during the last few years of the IERC-European Research Cluster on the Internet of Things in working to provide a definition that would cover the many facets of this concept/idea/paradigm.

Internet of Things is a "global concept" and requires a global effort to find a common definition. ITU-T, Internet of Things Global Standards Initiative [54] is working to find a definition that is a "compromise" among many different views. This highlights the difficulty of defining a concept that is evolving. This process, however, has contributed greatly to an understanding of the

different perspectives proposed by different schools of thoughts and has helped to harmonize them.

IERC is actively involved in ITU-T and has been part of the team which has formulated the following proposed definition: **"In a broad perspective, the IoT can be perceived as a vision with technological and societal implications. From the perspective of technical standardization, IoT can be viewed as 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. 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 maintaining the required privacy."**

The IERC definition [97] states that IoT is **"A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network."**

The word **dynamic** is used to describe the fact that the network is evolving, changing, adapting, scaling, and reconfiguring. The ITU-T formulation **"for the information society, enabling advanced services"** is maybe incomplete. A better formulation would be **"for the knowledge society, enabling advanced applications and services".**

The words **with self-configuring capabilities** introduce the notions of self-organizing, self-healing, auto and self-management, autonomic, autonomous, scaling, content/context aware, network aware - attributes that are important in IoT applications.

The IERC definition describes the fact that the "things" are identifiable and have physical attributes that allow them to sense, actuate, identify, interact, interface and communicate.

The ITU-T definition includes the elements **identification, data capture, processing and communication,** which suggest a static system and does not capture the fact that the things can actuate and interact, making the IoT concept dynamic and interactive with the environment.

The term **"virtual personalities"** considers that the **"persona"** of the thing may change as the thing travels through space and time.

The ITU-T definition states that **IoT makes full use of things to offer services to all kinds of applications.** The value in the future applications is in the interconnections among things. As mentioned earlier , the IoT will generate applications and based on these applications, services. Maybe this formulation of words does not capture the point.

Adding **whilst maintaining the required privacy** in the proposed ITU-T definition is beneficial and the formulation can be improved by including **"to all kinds of secure, safe and trustworthy applications".**

The IERC definition refers to **"use intelligent interfaces, and are seamlessly integrated into the information network".** The use of the terms seamlessly integrated are needed in the definition of IoT since this is part of the whole IoT concept of what Mark Weiser wrote in 1991 [102] **"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it".**

2 IoT Strategic Research Directions

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

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.

IERC Strategic Research 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.

The Strategic Research 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.

Figure 4 Internet of Things –- Enabling Technologies

Since the release of the first version of the Strategic Research 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 Agenda, whilst on the other it created new challenges and research questions. Furthermore, recent advances in pertinent areas such as cloud computing, 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 Agenda builds incrementally on previous versions [90] and highlights the main research topics that are associated with the development of IoT enabling technologies, infrastructures and applications with an outlook towards 2020 [42] .

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 [25].

In addition to boosting the development of emerging architectures and services, the directions of the Strategic Research Agenda will collectively enable the formation of ecosystems for open innovation based on Internet of Things technologies.

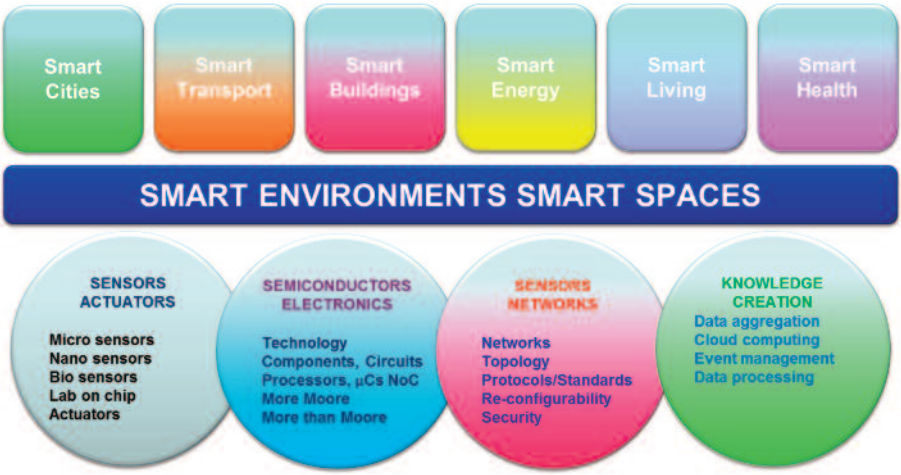


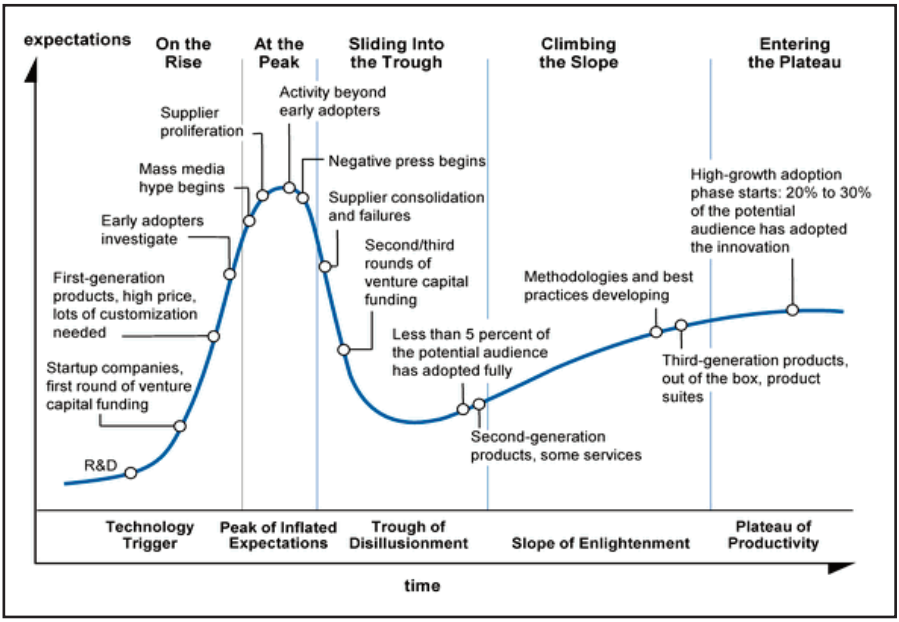
Figure 5 Internet of Things - Smart Environments and Smart Spaces Creation

The timeline of the Internet of Things Strategic Research 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.

Alan Curtis Kay the renowned computer scientist (object-oriented programming and windowing graphical user interface design) once said: "The best way to predict the future is to invent it". Following this strategy 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 Agenda covers in a logical manner the vision, the technological trends, the applications, the technology enablers, the research agenda, timelines, priorities, and finally summarises in two tables the future technological developments and research needs.

Advances in embedded sensors, processing and wireless connectivity are bringing the power of the digital world to objects and places in the physical world. IoT Strategic Research Agenda is aligned with the findings of the 2011 Hype Cycle developed by Gartner [23] , which includes the broad trend of the Internet of Things (called the "real-world Web" in earlier Gartner research.



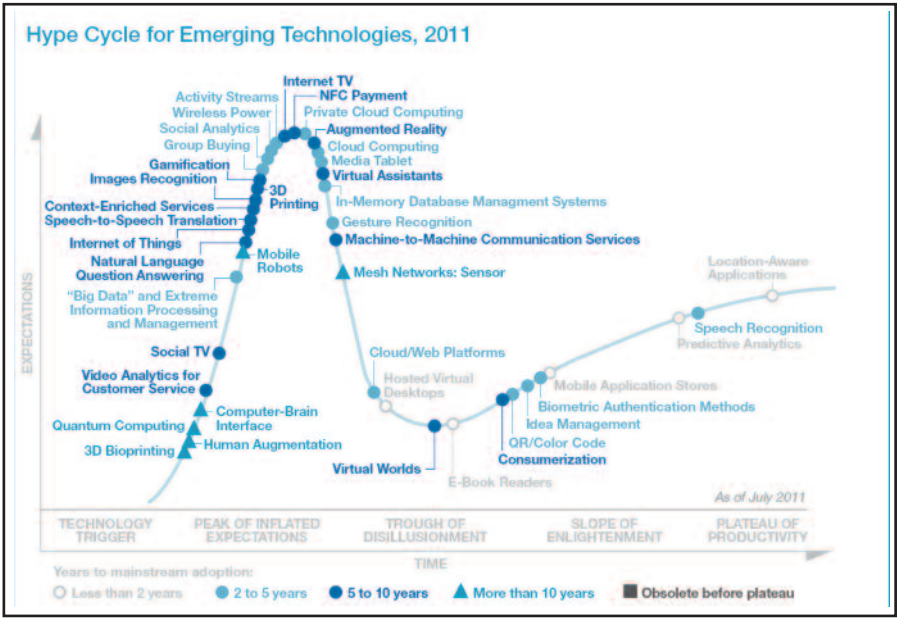


Figure 6 Hype Cycle developed by Gartner

This chapter builds on [90] and introduces the latest developments and challenges. It considers that the field of the Internet of Things is based on the paradigm of supporting the IP protocol to all edges of the Internet and on the fact that at the edge of the network many (very) small devices are still unable to support IP protocol stacks. This means that solutions centred on minimum Internet of Things devices are considered as an additional Internet of Things paradigm without IP to all access edges, due to their importance for the development of the field.

2.1 Applications and Scenarios of Relevance

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" [90], see Figure 7.

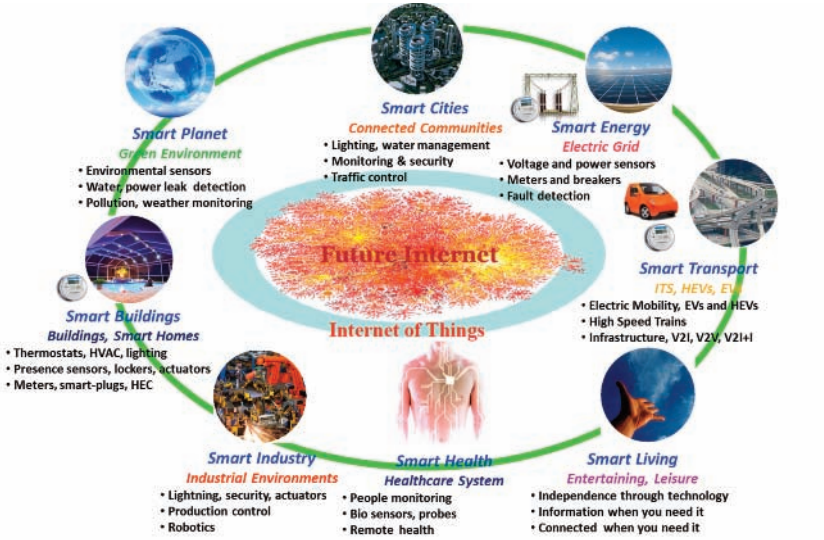


Figure 7 Internet of Things in the context of Smart Environments and Applications [47]

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.

In this context the new concept of Internet of Energy requires web based architectures to readily guarantee information delivery on demand and to change the traditional power system into a networked Smart Grid that is largely automated, by applying greater intelligence to operate, enforce policies, monitor and self-heal when necessary. This requires the integration and interfacing of the power grid to the network of data represented by the Internet, embracing energy generation, transmission, delivery, substations, distribution control, metering and billing, diagnostics, and information systems to work seamlessly and consistently.

This concept would enable the ability to produce, store and efficiently use energy, while balancing the supply/demand by using a cognitive Internet of Energy that harmonizes the energy grid by processing the data, information and knowledge via the Internet. In fact, as seen in Figure 8 [47] , the Internet of Energy will leverage on the information highway provided by the Internet to link computers, devices and services with the distributed smart energy grid that is the freight highway for renewable energy resources allowing stakeholders to invest in green technologies and sell excess energy back to the utility.

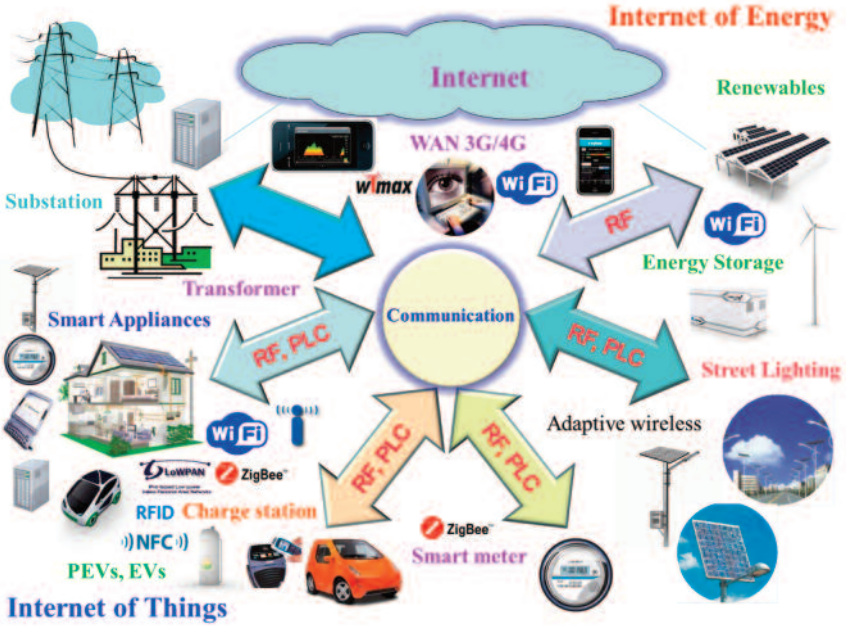


Figure 8 Internet of Things embedded in Internet of Energy applications [47]

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 [47] .

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.

2.2 IoT Functional View

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

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

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

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

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

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

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

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

Research challenges:

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

2.3 Application Areas

Potential applications of the IoT are numerous and diverse, permeating into practically all areas of every-day life of individuals, enterprises, and society as a whole. The 2010 Internet of Things Strategic Research Agenda (SRA)[97] has identified and described the main Internet of Things applications, which span numerous application domains: smart energy, smart health, smart buildings, smart transport, smart living and smart cities.

According to the survey that the IoT-I project ran during 2010 [52] 65 IoT application scenarios were identified, grouped in 14 domains: Transportation, Smart Home, Smart City, Lifestyle, Retail, Agriculture, Smart Factory, Supply chain, Emergency, Health care, User interaction, Culture and tourism, Environment and Energy. The survey was based on 270 responses from 31 countries and the scenarios attracting the most interest were: smart home, smart city, transportation and health care.

These domains are in line with the application domains identified in SRA 2010, which was more or less expected, as most of the FP7 projects providing scenarios for the survey were running at the time when SRA 2010 was being produced.

One of the weaknesses of the survey is its European-centric approach, both from the definition of the scenarios included in the survey and from the distribution of the survey participants. For Europe to excel in the IoT domain, a more global view of the potential IoT applications is required including understanding of how developing countries can benefit from the IoT technology as these regions represent large potential markets. Their needs, due to different economic, political and environmental conditions, might (and most probably will) be completely different from the needs of an average European citizen.

Libelium has released the document "50 Sensor Applications for a Smarter World. Get Inspired!" [60], covering the most disruptive sensor and Internet of Things applications.

The list presented below, includes the trendiest scenarios, and is grouped in 12 different verticals, showing how the Internet of Things is becoming the next technological revolution.

Smart Cities

Smart Parking: Monitoring of parking spaces availability in the city.

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

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

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

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

Waste Management: Detection of rubbish levels in containers to optimize the trash collection routes.

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

Smart Environment

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

Air Pollution: Control of CO2 emissions of factories, pollution emitted by cars and toxic gases generated in farms.

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

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

Smart Water

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

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

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

Smart Metering

Smart Grid: Energy consumption monitoring and management.

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

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

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

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

Security & Emergencies

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

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

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

Explosive and Hazardous Gases: Detection of gas levels and leakages in industrial environments, surroundings of chemical factories and inside mines.

Retail

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

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

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

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

Logistics

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

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

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

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

Industrial Control

M2M Applications: Machine auto-diagnosis and assets control.

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

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

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

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

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

Smart Agriculture

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

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

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

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

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

Smart Animal Farming

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

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

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

Domotic & Home Automation

Energy and Water Use: Energy and water supply consumption monitoring to obtain advice on how to save cost and resources.

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

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

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

eHealth

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

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

Sportsmen Care: Vital signs monitoring in high performance centers and fields.

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

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

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

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

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

- To increase their safety or the safety of their family members - forexample remotely controlled alarm systems, or activity detection for elderly people;
- To make it possible to execute certain activities in a more convenient manner - for example: a personal inventory reminder;
- To generally improve life-style - for example monitoring health parameters during a workout and obtaining expert's advice based on the findings, or getting support during shopping;
- To decrease the cost of living - for example building automation that will reduce energy consumption and thus the overall cost.

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

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

To ensure public safety - in the light of various recent disasters such as the nuclear catastrophe in Japan, the tsunami in the Indian Ocean, earthquakes, terrorist attacks, etc. One of the crucial concerns of the society is to be able to predict such events as far ahead as possible and to make rescue missions and recovery as efficient as possible. One good example of an application of IoT technology was during the Japan nuclear catastrophe, when numerous Geiger counters owned by individuals were connected to the Internet to provide a detailed view of radiation levels across Japan.

To protect the environment

- Requirements for reduction of carbon emissions have been included in various legislations and agreements aimed at reducing the impact on the planet and making sustainable development possible.
- Monitoring of various pollutants in the environment, in particular in the air and in the water.
- Waste management, not just general waste, but also electrical devices and various dangerous goods are important and challenging topics in every society.
- Efficient utilization of various energy and natural resources are important for the development of a country and the protection of its resources.

To create new jobs and ensure existing ones are sustainable - these are important issues required to maintain a high level quality of living.

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

Examples of the needs are as follows:

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

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

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

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

3 IoT Applications

It is impossible to envisage all potential IoT applications having in mind the development of technology and the diverse needs of potential users. In the following sections, we identified several applications, which in our opinion are of the highest importance, and that were not addressed in the SRA 2010. These applications are described, and the research challenges are identified.

The list should not be considered as exhaustive - it can and should be expanded. However, it provides a good indication of the research challenges. While the applications themselves might be different, the research challenges are often the same or similar.

3.1 Smart cities

More than 50% of the world population lives in cities today. Cities represent a complex, dynamic environment, catering for a large number of citizens and businesses ("users of city services"). The number of services that each city has to provide or enable is huge, ranging from utility services and public transport to security of citizens and infrastructure, thus integrating the main application domains that proved to be of interest to the IOT-i survey participants. Each of these services deals with events taking place in the real world and they have to adapt, often in real time, to the dynamics of the

city. The challenges and opportunities have increased with the introduction of the so called megacities. In China, there are already city clusters with close to 100 million citizens.

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

A number of living labs across Europe are active today, providing platforms for introduction and evaluation of a plethora of smart services (not necessarily IoT focused). Today, the largest smart city initiatives completely focused on IoT is undertaken by the FP7 SmartSantander project [90] . This project aims at deploying an IoT infrastructure comprising thousands of IoT devices spread across several cities (Santander, Guildford, Luebeck and Belgrade). This will enable simultaneous development and evaluation of services and execution of various research experiments, thus facilitating the creation of a smart city environment.

Similarly, the OUTSMART [78] project, one of the FI PPP projects, is focusing on utilities and environment in the cities and addressing the role of IoT in waste and water management, public lighting and transport systems as well as environment monitoring.

There are numerous important research challenges:

- Overcoming traditional silo based organization of the cities, with each utility responsible for their own closed world. Although not technological this is one of the main barriers
- Creating algorithms and schemes to describe information created by sensors in different applications to enable useful exchange of information between different city services
- Mechanisms for cost efficient deployment and even more important maintenance of such installations, including energy scavenging
- Ensuring reliable readings from a plethora of sensors and efficient calibration of a large number of sensors deployed everywhere from lampposts to waste bins
- Low energy protocols and algorithms
- Algorithms for analysis and processing of data acquired in the city and making “sense” out of it.

3.2 Participatory sensing

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

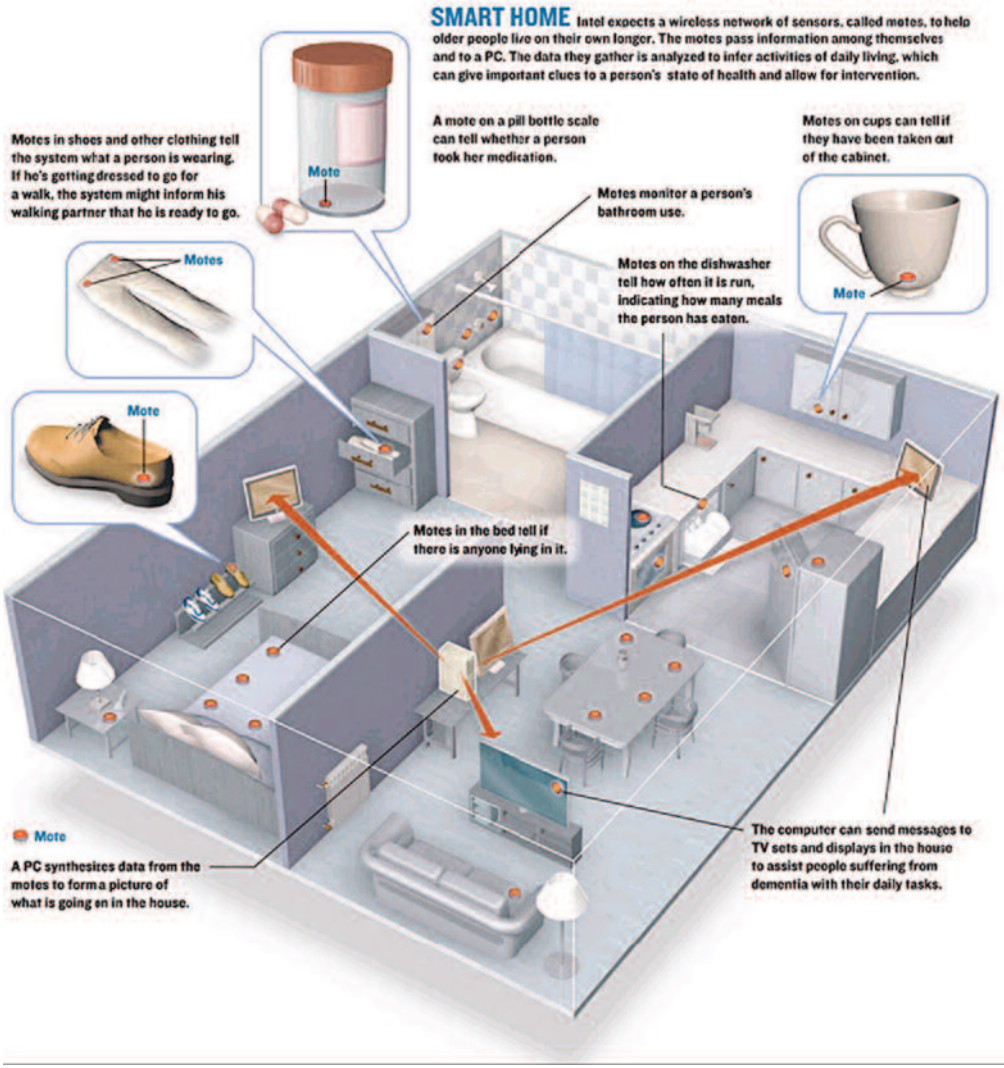


Figure 9 Internet of Things and Smart Home Concept (Source: Intel)

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

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

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

Low cost smart chips added to every device to give them an IP address and everything in one's life can become part of a private secure network to be monitored, controlled and smart via a smartphone, tablet or PC. NXP Semiconductors announced its GreenChip, which enables every light bulb to have its own wireless IP address. NXP has announced it is to make its JenNet-IP, ultra-low-power, IEEE 802.15.4-based, wireless network layer software available under an Open Source license.

Figure 10 Internet of Things and open source, ultra-low-power JenNet-IP [73]

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

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

- Design of algorithms for normalization of observations taking into account the conditions under which the observations were taken. For example temperature measurements will be different if taken by a mobile phone in a pocket or a mobile phone lying on a table;
- Design of robust mechanisms for analysis and processing of collected observations in real time (complex event processing) and generation of "community wisdom" that can be reliably used as an input to decision taking;
- Reliability and trustworthiness of observed data, i.e. design of mechanisms that will ensure that observations were not tampered with and/or detection of such unreliable measurements and consequent exclusion from further processing;
- Ensuring privacy of individuals providing observations
- Efficient mechanisms for sharing and distribution of "community wisdom".

3.3 Social networks and IoT

From a user perspective, abstract connectedness and real-world interdependencies are not easily captured mentally. What users however easily relate to is the social connectedness of family and friends. The user engagement in IoT awareness could build on the Social Network paradigm, e.g. as described in [27] and [13], where the users interact with the real world entities of interest via the social network paradigm. This combination leads to interesting and popular applications (such as [56]), which will become more sophisticated and innovative.

Future research directions in IoT applications should consider the social dimension, based on integration with social networks which can be seen as another bundle of information streams. Note also that social networks are

characterized by the massive participation of human users. Hence, the wave of social IoT applications is likely to be built over successful paradigms of participatory sensing applications (e.g.,[15], [69], [40]), which will be extending on the basis of an increased number of autonomous interacting Internet-connected devices. The use of the social networks metaphor for the interactions between Internet-connected objects has been recently proposed [58] and it could enable novel forms of M2M, interactions and related applications.

3.4 Smart Energy and the Smart Grid

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

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

The developing Smart Grid is expected to implement a new concept of transmission network which is able to efficiently route the energy which is produced from both concentrated and distributed plants to the final user with high security and quality of supply standards. Therefore the Smart Grid is expected to be the implementation of a kind of “Internet” in which the

energy packet is managed similarly to the data packet - across routers and gateways which autonomously can decide the best pathway for the packet to reach its destination with the best integrity levels. In this respect the "Internet of Energy" concept is defined as a network infrastructure based on standard and interoperable communication transceivers, gateways and protocols that will allow a real time balance between the local and the global generation and storage capability with the energy demand. This will also allow a high level of consumer awareness and involvement.

The Internet of Energy (IoE) provides an innovative concept for power distribution, energy storage, grid monitoring and communication as presented in Figure 11. It will allow units of energy to be transferred when and where it is needed. Power consumption monitoring will be performed on all levels, from local individual devices up to national and international level [92] .

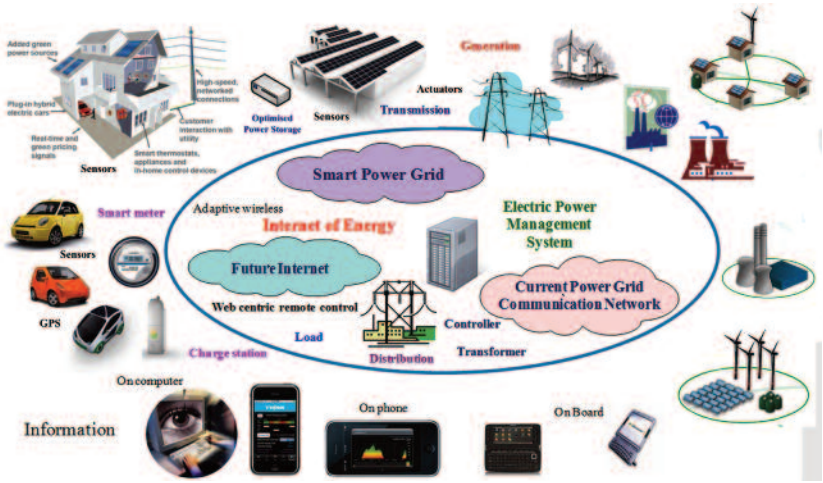


Figure 11 Internet of Energy Concept [92]

Saving energy based on an improved user awareness of momentary energy consumption is another pillar of future energy management concepts. Smart meters can give information about the instantaneous energy consumption to the user, thus allowing for identification and elimination of energy wasting devices and for providing hints for optimizing individual energy consumption. In a smart grid scenario energy consumption will be manipulated by a volatile energy price which again is based on the momentary demand (acquired by smart meters) and the available amount of energy and renewable energy production. In a virtual energy marketplace

software agents may negotiate energy prices and place energy orders to energy companies. It is already recognised that these decisions need to consider environmental information such as weather forecasts, local and seasonal conditions. These must be to a much finer time scale and spatial resolution.

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

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

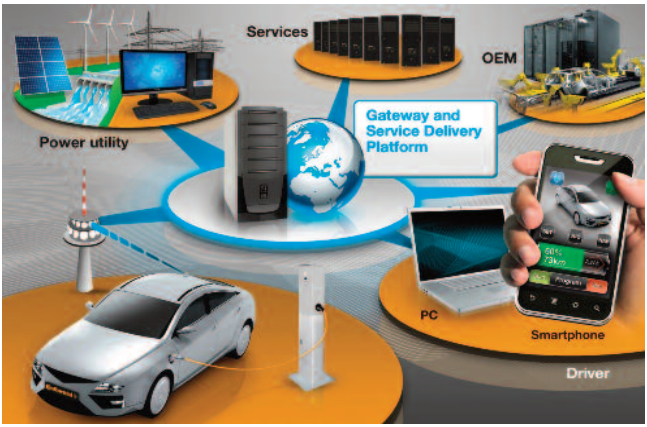


Figure 12 Electric Mobility Ecosystem (Source: Continental)

New organizational and learning strategies for sensor networks will be needed in order to cope with the shortcomings of classical hierarchical control concepts. The intelligence of smart systems does not necessarily need to be built into the devices at the systems' edges. Depending on connectivity, cloud-based IoT concepts might be advantageous when considering energy dissipation and hardware effort.

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

Some Research Challenges:

- Absolutely safe and secure communication with elements at the network edge
- Energy saving robust and reliable smart sensors/actuators
- Technologies for data anonymity addressing privacy concerns
- Dealing with critical latencies, e.g. in control loops
- System partitioning (local/cloud based intelligence)
- Mass data processing, filtering and mining; avoid flooding of communication network
- Real-time Models and design methods describing reliable interworking of heterogeneous systems (e.g. technical / economical / social / environmental systems).
- Identifying and monitoring critical system elements
- Detecting critical overall system states in due time
- System concepts which support self-healing and containment of damage; strategies for failure contingency management
- Technologies supporting self-organisation and dynamic formation of structures / re-structuring

3.5 Smart Mobility

The connection of vehicles to the Internet gives rise to a wealth of new possibilities and applications which bring new functionalities to the individuals and/or the making of transport easier and safer. At the same time creating new mobile ecosystems based on trust, security and convenience to mobile/contactless services and transportation applications will ensure security, mobility and convenience to consumer-centric transactions and services.

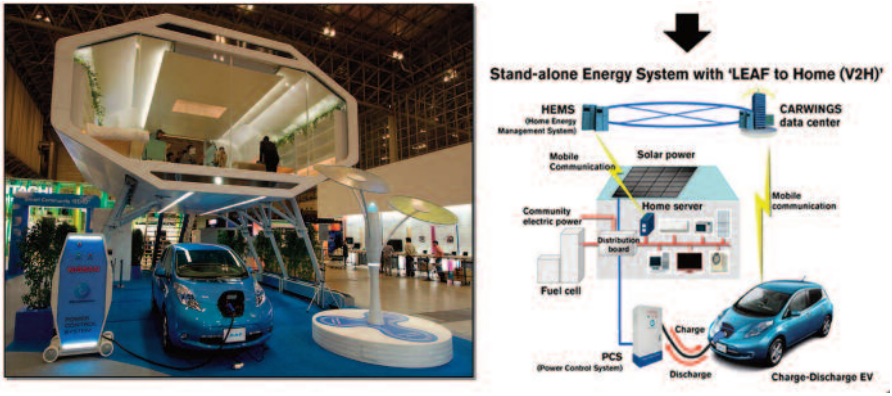


Figure 13 Standalone Energy Ecosystem (Source: Renault Nissan)

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

IoT as an inherent part of the vehicle control and management system: Already today certain technical functions of the vehicles' on-board systems can be monitored on line by the service centre or garage to allow for preventative maintenance, remote diagnostics, instantaneous support and timely availability of spare parts. For this purpose data from on-board sensors are collected by a smart on-board unit and communicated via the Internet to the service centre.

IoT enabling traffic management and control: Cars should be able to organise themselves in order to avoid traffic jams and to optimise drive energy usage. This may be done in coordination and cooperation with the infrastructure of a smart city's traffic control and management system. Additionally dynamic road pricing and parking tax can be important elements of such a system. Further mutual communications between the vehicles and with the infrastructure enable new methods for considerably increasing traffic safety, thus contributing to the reduction in the number of traffic accidents.

IoT enabling new transport scenarios (multi-modal transport): In such scenarios, e.g. automotive OEMs see themselves as mobility providers rather than manufacturers of vehicles. The user will be offered an optimal solution for transportation from A to B, based on all available and suitable transport means. Thus, based on the momentary traffic situation an ideal solution may be a mix of individual vehicles, vehicle sharing, railway, and commuter systems. In order to allow for seamless usage and on-time

availability of these elements (including parking space), availability needs to be verified and guaranteed by online reservation and online booking, ideally in interplay with the above mentioned smart city traffic management systems.

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

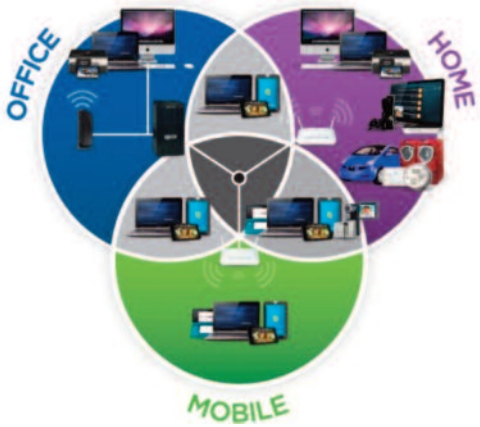


Figure 14 Communication Ecosystem (Source: Qualcomm)

Technical elements of such systems are smart phones and smart vehicle on-board units which acquire information from the user (e.g. position, destination and schedule) and from on board systems (e.g. vehicle status, position, energy usage profile, driving profile). They interact with external systems (e.g. traffic control systems, parking management, vehicle sharing managements, electric vehicle charging infrastructure). Moreover they need to initiate and perform the related payment procedures.

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

The (international) standardisation of protocol stacks and interfaces is of utmost importance to enable economic competition and guarantee smooth interaction of different vendor products.

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

Some Research Challenges:

- Absolutely safe and secure communication with elements at the network edge, inter-vehicle communication, and vehicle to infrastructure communication
- Energy saving robust and reliable smart sensors and actuators in vehicles and infrastructure
- Technologies for data anonymity addressing privacy concerns
- Dealing with critical latencies, e.g. in control loops
- System partitioning (local/cloud based intelligence)
- Mass data processing, Filtering and mining; avoid flooding of communication network
- Real-time Models and design methods describing reliable interworking of heterogeneous systems (e.g. technical/economical /social/environmental systems).
- Identifying and monitoring critical system elements.
- Detecting critical overall system states in due time
- Technologies supporting self-organisation and dynamic formation of structures / re-structuring

3.6 Food and water tracking and security

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

the origin or the production process. Using IoT in such scenarios to secure tracking of food or water from the production place to the consumer is one of the important topics.

This has already been introduced to some extent in regard to beef meat. After the "mad cow disease" outbreak in the late 20th century, some beef manufacturers together with large supermarket chains in Ireland are offering "from pasture to plate" traceability of each package of beef meat in an attempt to assure consumers that the meat is safe for consumption. However, this is limited to certain types of food and enables tracing back to the origin of the food only, without information on the production process.

The research challenges are:

- Design of secure, tamper-proof and cost-efficient mechanisms for tracking food and water from production to consumers
- Secure way of monitoring production processes, providing sufficient information and confidence to consumers. At the same time details of the production processes which might be considered as intellectual property, should not be revealed.

4 Internet of Things and related Future Internet technologies

4.1 Cloud Computing

Since the publication of the 2010 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[37].

As part of this convergence, IoT applications (such as sensor-based services) will be delivered on-demand through a cloud environment[103].

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.

Relevant topics for the research agenda will therefore include:

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

4.2 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) [8] , while relevant tools and techniques have just emerged [38]. 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.

4.3 Autonomy

Spectacular advances in technology have introduced increasingly complex and large scale computer and communication systems. Autonomic computing [44], 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.

4.3.1 Properties of autonomic IoT systems

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

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.

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

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.

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.

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.

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.

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 find a trade-off between the expressiveness, the conformity and the size of the descriptions. Self-description is a fundamental property for implementing plug 'n play resources and devices.

Self-discovery

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

Self-matchmaking

To fully unlock the IoT potential, virtual objects will have to:

- Be reusable outside the context for which they were originally deployed and
- Be reliable in the service they provide.

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

Self-energy-supplying

And finally, self-energy-supplying is a tremendously important (and very IoT specific) feature to realize and deploy sustainable IoT solutions. Energy harvesting techniques (solar, thermal, vibration, etc.) should be preferred as a main power supply, rather than batteries that need to be replaced regularly, and that have a negative effect on the environment.

4.3.2 Research directions for self-manageable IoT systems

Given the above mentioned challenges, we propose the following research directions to progress towards self-manageable IoT systems:

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

Novel methodologies, architectures, algorithms, technologies, and protocols should be developed taking into account IoT-specific 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.

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.

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.

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.

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.

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.

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.

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 from the distributed systems domain, fundamentals of economics can also be applied to resolve these issues.

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

Security and privacy issues should be considered very seriously since IoT deals 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 control abilities. Cyber-physical environments must thus be protected from any kind of malicious attacks.

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.

5 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.

5.1 Plug & 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. 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.

5.2 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.

5.3 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.

5.4 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. 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.

5.5 Security and privacy

In addition, an infrastructure needs to provide support functionality. This includes security and privacy support, including authentication and

authorization. Here the heterogeneity and the resource limitations of IoT technologies have to be taken into account. Interoperability between different basic approaches will be an important aspect.

5.6 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:

- How can the plug & play functionality be achieved taking into account the heterogeneity of the underlying technology?
- How should the resolution and discovery infrastructure look to enable finding things efficiently?
- How can monitoring and automatic adaptation be supported by the infrastructure?
- How can semantic information be easily added and utilized within the infrastructure?
- 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?
- How can the notion of physical location be best reflected in the infrastructure to support the required functionalities mentioned above?
- How should the infrastructure support for security and privacy look?
- How can the infrastructure support accounting and charging as the basis for different IoT business models?

6 Networks and Communication

Present communication technologies span the globe in wireless and wired networks and support global communication by globally-accepted communication standards. The Internet of Things Strategic Research Agenda intends to lay the foundations for the Internet of Things to be developed by research through to the end of this decade and for subsequent innovations to be realised even after this research period.

Within this timeframe the number of connected devices, their features, their distribution and implied communication requirements will develop; as will the communication infrastructure and the networks being used. Everything will change significantly. Internet of Things devices will be contributing to and strongly driving this development.

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

6.1 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.

6.1.1 Complexity of the networks of the future

A key research topic will be to understand the complexity of these future networks and the expected growth of complexity due to the growth of Internet of Things. The research results of this topic will give guidelines and timelines for defining the requirements for network functions, for network management, for network growth and network composition and variability.[24]

Wireless networks cannot grow without such side effects as interference.

6.1.2 Growth of wireless networks

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

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

Mankind is the maximum user group for the mobile phone system, which is the most prominent distributed system worldwide besides the fixed telephone system and the Internet. Obviously the number of body area

networks [68], [1], [101], 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.

6.1.3 Mobile networks

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

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

6.1.4 Expanding current networks to future networks

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

6.1.5 Overlay networks

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

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

6.1.6 Network self-organization

Wireless networks being built for the Internet of Things will show a large degree of ad-hoc growth, structure, organization, and significant change in time, including mobility. These constituent features will have to be reflected in setting them up and during their operation [20].

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.

6.1.7 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[96].

Disruptive developments are to be expected by analysing the energy requirements of current solutions and by going back to principles of communication in wired, optical and wireless information transfer. Research done by Bell Labs [32], [33] in recent years shows that networks can achieve an energy efficiency increase of a factor of 1,000 compared to current technologies [81].

The results of the research done by the GreenTouch consortium [32] should be integrated into the development of the network technologies of the future. These network technologies have to be appropriate to realise the Internet of Things and the Future Internet in their most expanded state to be anticipated by the imagination of the experts..

6.2 Communication technology

6.2.1 Unfolding the potential of communication technologies

The research aimed at communication technology to be undertaken in the coming decade will have to develop and unfold all potential communication profiles of Internet of Things devices, from bit-level communication to

continuous data streams, from sporadic connections to connections being always on, from standard services to emergency modes, from open communication to fully secured communication, spanning applications from local to global, based on single devices to globally-distributed sets of devices. [31]

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

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

6.2.2 Correctness of construction

Correctness of construction [34] of the whole system is a systematic process that starts from the small systems running on the devices up to network and distributed applications. Methods to prove the correctness of structures and of transformations of structures will be required, including protocols of communication between all levels of communication stacks used in the Internet of Things and the Future Internet.

These methods will be essential for the Internet of Things devices and systems, as the smallest devices will be implemented in hardware and many types will not be programmable. Interoperability within the Internet of Things will be a challenge even if such proof methods are used systematically.

6.2.3 An unified theoretical framework for communication

Communication between processes [41]running within an operating system on a single or multicore processor, communication between processes running in a distributed computer system [72], 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.

6.2.4 Energy-limited Internet of Things devices and their communication

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

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

6.2.5 Challenge the trend to complexity

The inherent trend to higher complexity of solutions on all levels will be seriously questioned – at least with regard to minimum energy Internet of Things devices and services, but not limited to them.

.. for energy limited Internet of Things devices and their communication

As mobile, energy limited Internet of Things devices will be highly common, their transmit and receive path architectures and all further processing tasks related to their specific application have necessarily to be included into the search for minimum realizations.

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.

6.2.6 Disruptive approaches

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

7 Processes

The deployment of IoT technologies will significantly impact and change the way enterprises do business as well as interactions between different parts of the society, affecting many processes. To be able to reap the many potential benefits that have been postulated for the IoT, several challenges regarding the modelling and execution of such processes need to be solved in order to see wider and in particular commercial deployments of IoT [36].

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 [99], will need to be extended.

7.1 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.

7.2 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.

7.3 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. 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).

7.4 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 [70] the decomposition and decentralization of existing business processes increases scalability and performance, allows better decision making and could even lead to new business models and revenue streams through entitlement management of software products deployed on smart items. For example, in environmental monitoring or supply chain tracking applications, no messages need to be sent to the central system as long as everything is within the defined limits. Only if there is a deviation, an alert (event) needs to be generated, which in turn can lead to an adaptation of

the overall process. From a business process modelling perspective though, it should be possible to define the process centrally, including the fact that some activities (i.e., the monitoring) will be done remotely. Once the complete process is modelled, it should then be possible to deploy the related services to where they have to be executed, and then run and monitor the complete process.

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

8 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. More than 60 million M2M devices are currently connected to networks around the globe. Multiple industry analysts are predicting 30-50% year-on-year growth, forecasting connectivity of more than 2 billion M2M devices by the year 2020. The forecasted number of connected devices by 2020 is shown in Figure 15.

There are many technologies and factors involved in the "data management" within the IoT context.

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

- Data Collection and Analysis
- Big data
- Semantic Sensor Networking
- Virtual Sensors
- Complex Event Processing.

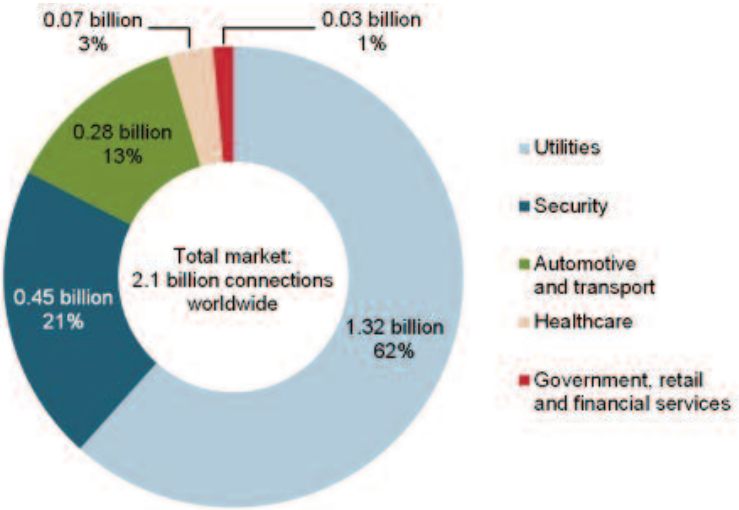


Figure 15: Commercial and consumer M2M device connections by industry sector, worldwide, 2020[1]

8.1 Data collection and analysis (DCA)

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

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

User/customer data storing:

Provides storage of the customer's information collected by sensors

User data & operation modelling:

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

On demand data access:

Provides APIs to access the collected data

Device event publish/subscribe/forwarding/notification:

Provides APIs to access the collected data in real time conditions

Customer rules/filtering:

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

Customer task automation:

Provides the customer with the ability to manage his automatic processes. Example: scheduled platform originated data collection, …

Customer workflows:

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

Multitenant structure:

Provides the structure to support multiple organizations and reseller schemes.

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

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

8.2 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," [39], where the majority of data will be stamped out by machines. These machines generate data a lot faster than people can, and their production rates will grow exponentially with Moore's Law. Storing this data is cheap, and it can be mined for valuable information. Examples of this tendency include:

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

Big data requires exceptional technologies to efficiently process large quantities of data within a tolerable amount of time. Technologies being applied to big data include massively parallel processing (MPP) databases, data-mining grids, distributed file systems, distributed databases, cloud computing platforms, the Internet, and scalable storage systems.

The biggest challenge of the Petabyte Age will not be storing all that data, it will be figuring out how to make sense of it. Big data deals with unconventional, unstructured databases, which can reach petabytes,

exabytes or zettabytes, and require specific treatments for their needs, either in terms of storage or processing/display.

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

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

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

8.3 Semantic sensor networks and semantic annotation of data

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

There are currently on-going efforts to define ontologies and to create frameworks to apply semantic Web technologies to sensor networks. The Semantic Sensor Web (SSW) proposes annotating sensor data with spatial, temporal, and thematic semantic metadata [88] . This approach uses the current OGC and SWE [12] 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 [93] is also working on developing an 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 [21] . On a large scale this machine interpretable information (i.e. semantics) is a key enabler and necessity for the semantic sensor networks. Emergence of sensor data as linked-data enables sensor network providers and data consumers to connect sensor descriptions to potentially endless data existing on the Web. By relating sensor data attributes such as location, type, observation and measurement features to other resources on the Web of data, users will be able to integrate physical world data and the logical world data to draw conclusions, create business intelligence, enable smart environments, and support automated decision making systems among many other applications.

The linked-sensor-data can also be queried, accessed and reasoned based on the same principles that apply to linked-data. The principles of using linked data to describe sensor network resources and data in an implementation of an open platform to publish and consume interoperable sensor data is described in [5] .

In general, associating sensor and sensor network data with other concepts (on the Web) and reasoning makes the data information widely available for different applications, front-end services and data consumers. The semantic description allow machines to interpret links and relations between the different attributes of a sensor description and also other data existing on the Web or provided by other applications and resources.

8.4 Virtual sensors

A virtual sensor can be considered as a product of spatial, temporal and/or thematic transformation of raw or other virtual sensor producing data with necessary provenance information attached to this transformation. Virtual sensors and actuators are a programming abstraction simplifying the development of decentralized WSN applications [63]. The data acquired by a set of sensors can be collected, processed according to an application-provided aggregation function, and then perceived as the reading of a single virtual sensor. Dually, a virtual actuator provides a single entry point for distributing commands to a set of real actuator nodes. We follow that statement with this definition:

> A virtual sensor behaves just like a real sensor, emitting time-series data from a specified geographic region with newly defined thematic concepts or observations which the real sensors may not have.

> A virtual sensor may not have any real sensor's physical properties such as manufacturer or battery power information, but does have other properties, such as: who created it; what methods are used, and what original sensors it is based on.

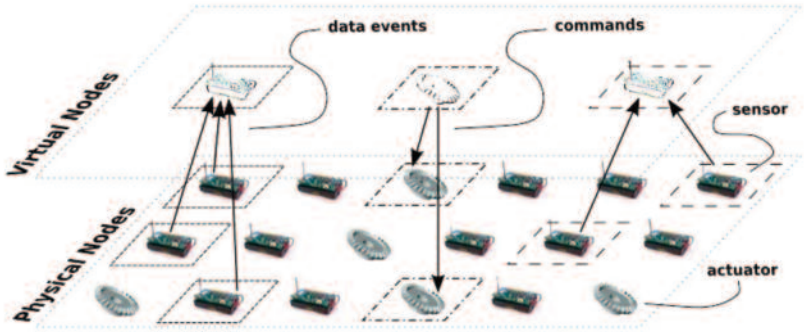


Figure 16 Flow of information between real devices and virtual sensors or actuators [63]

The virtualization of sensors can be considered at different levels as presented in Figure 17. At the lowest level are those related with the more local processing of several simple measurements (for example in a sensing node), and at the highest level, the abstract combination of different sensors at the application level (including user-generated virtual sensors).

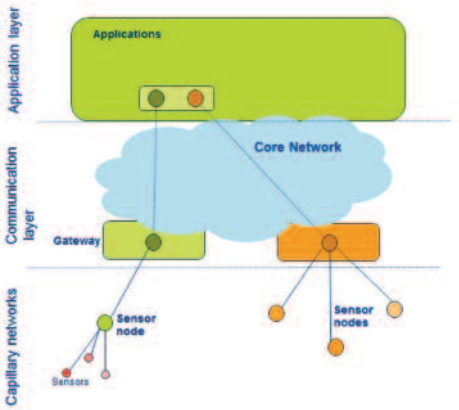


Figure 17 Different levels for sensor virtualization

In that sense the development of virtual sensors could be approached following two different degrees of complexity:

- The combination of a limited number of related sensors or measurements to derive new virtual data (usually done at the sensor node or gateway level).
- The complex process of deriving virtual information from a huge space of sensed data (generally at the application level).

Furthermore it is also important to consider that due to the temporal dimension of sensor data most of the processing required to develop virtual sensors is tightly related to the event concept as defined in ISO 19136 "an action that occurs at an instant or over an interval of time", as well as to Event Processing as "creating, deleting, reading and editing of as well as reacting to events and their representations" [17] .

An event, as a message indicating that something of interest happens, is usually specified through an event type as a structure of attribute-value tuples. An important attribute is the event occurrence time or its valid time interval. Timing is generally described using timestamps but its proper management presents important challenges in geographically dispersed distributed systems.

The complexity of deriving virtual information from a large number of sensor data as depicted in Figure 18, demands the use of proper methods, techniques and tools for processing events while they occur, i.e., in a continuous and timely fashion. Deriving valuable higher-level knowledge from lower-level events has been approached using different technologies

from many independent research fields (such as, discrete event simulation, active databases, network management, or temporal reasoning), and in different application fields (as business activity monitoring, market data analysis, sensor networks, etc.). Only in recent years has the term Complex Event Processing, CEP, emerged as a discipline of its own and as an important trend in industry applications where it is necessary to detect situations (specified as complex events) that result from a number of correlated (simple) events. CEP concept will be described in depth hereafter.

More specifically, as represented in Figure 18, considering that sensor data is generally delivered as a stream, a sub-form of CEP known as Event Stream Processing (ESP) [66] can be used for searching different patterns in continuous streams of sensor data events.

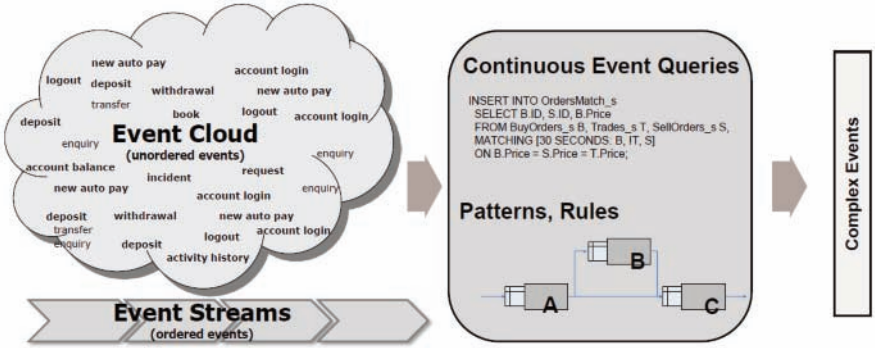


Figure 18 Complex Event Processing (CPE) and Event Stream Processing (ESP)

In the near future, some of the main challenges to be solved in the context of Virtual Sensors are:

- Seamless integration and interoperability of "real" and "virtual" sensors. This means that virtual sensors should be indistinguishable from real ones for the external or high level applications, but also for other sensors or system modules if necessary. This way, virtual sensors could be fed as input sensors for new virtual ones, making the flexibility and power of this approach almost unlimited.
- Support of (input) sensors and measurements heterogeneity. A virtual sensor should, ideally, be capable of handling input sensors of a very different nature. This results in a very powerful mechanism for implementing complex logics, also linking with CEP concepts. The integration of sensors capturing different phenomena may help

the implementation of heuristics or artificial intelligence-based decision modules, capable of handling aspects that are not homogeneous (not mere statistics functions over homogeneous figures). This also includes the automatic handling or conversion of different units or scales for input sensors measuring a same aspect.

Definition of virtual sensors based on semantic rules. A first approach for defining virtual sensors is by implementing the programmatic logic or processes associated with the "operation" to be performed by the sensor. But a much richer and more powerful scheme can be obtained if sensors can be defined by "high level" semantic rules (only describing the general behaviour or expected results) and implementation steps are automatically generated (from the rules) or hidden to external users.

8.5 Complex event processing

A concept linked with the notion and appearance of "Virtual Sensors" is the Complex Event Processing, in the sense that Virtual Sensors can be used to implement "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 (or 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 (TheCEPBlog).[16] 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.

8.5.1 Types

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

- 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
- 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:

- 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.
- 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.
- 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).

9 Security, Privacy & Trust

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

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

Solutions will need to address federation/administrative co-operation

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

9.1 Trust for IoT

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

- Lightweight Public Key Infrastructures (PKI) as a basis for trust management. Advances are expected in hierarchical and cross certification concepts to enable solutions to address the scalability requirements.
- Lightweight key management systems to enable trust relationships to be established and the distribution of encryption materials using minimum communications and processing resources, as is consistent with the resource constrained nature of many IoT devices.

Quality of Information is a requirement for many IoT-based systems where metadata can be used to provide an assessment of the reliability of IoT data.

Decentralised and self-configuring systems as alternatives to PKI for establishing trust e.g. identity federation, peer to peer.

Novel methods for assessing trust in people, devices and data, beyond reputation systems.

Assurance methods for trusted platforms including hardware, software, protocols, etc.

9.2 Security for IoT

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

DoS/DDOS attacks are already well understood for the current Internet, but the IoT is also susceptible to such attacks and will require specific techniques and mechanisms to ensure that transport, energy, city infrastructures cannot be disabled or subverted.

General attack detection and recovery/resilience to cope with IoT-specific threats, such as compromised nodes, malicious code hacking attacks.

Cyber situation awareness tools/techniques will need to be developed to enable IoT-based infrastructures to be monitored. Advances are required to enable operators to adapt the protection of the IoT during the lifecycle of the system and assist operators to take the most appropriate protective action during attacks.

The IoT requires a variety of access control and associated accounting schemes to support the various authorisation and usage models that are required by users. The heterogeneity and diversity of the devices/gateways that require access control will require new lightweight schemes to be developed.

The IoT needs to handle virtually all modes of operation by itself without relying on human control. New techniques and approaches e.g. from machine learning, are required to lead to a self-managed IoT.

9.3 Privacy for IoT

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

There are a number of areas where advances are required:

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

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

- Preserving location privacy, where location can be inferred from things associated with people.
- Prevention of personal information inference, that individuals would wish to keep private, through the observation of IoT-related exchanges.
- Keeping information as local as possible using decentralised computing and key management.

10 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.

10.1 Low power communication

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

- IEEE 802.15.4 has developed a low-cost, low-power consumption, low complexity, low to medium range communication standard at the link and the physical layers [46] for resource constrained devices.
- Bluetooth low energy (Bluetooth LE,[10]) is the ultra-low power version of the Bluetooth technology [9] that is up to 15 times more efficient than Bluetooth.
- Ultra-Wide Bandwidth (UWB) Technology [95] 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.
- RFID/NFC proposes a variety of standards to offer contactless solutions. Proximity cards can only be read from less than 10 cm and follows the ISO 14443 standard [53] 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-regeneratives 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 [79], [98]. In this field, standardization is required, as today only proprietary solutions exist, for an actual gain in the overall market to be significant.

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

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

Progressively, portable RF architectures are making it easy to add the RF feature to existing devices. This will lead to RF heavily exploiting digital blocks and limiting analogue ones, like passive / inductor silicon consuming elements, as these are rarely easy to port from one technology to another. Nevertheless, the same performance will be required so receiver architectures will have to efficiently digitalize the signal in the receiver or transmitter chain [83] . In this direction, Band-Pass Sampling solutions are promising as the signal is quantized at a much lower frequency than the Nyquist one, related to deep under-sampling ratio [64] . Consumption is therefore greatly reduced compared to more traditional early-stage sampling processes, where the sampling frequency is much lower.

Continuous-Time quantization has also been regarded as a solution for high-integration and easy portability. It is an early-stage quantization as well, but without sampling [59] . Therefore, there is no added consumption due to the clock, only a signal level which is considered. These two solutions are clear evolutions to pave the way to further digital and portable RF solutions.

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

10.2 Energy harvesting

Four main ambient energy sources are present in our environment: mechanical energy (vibrations, deformations), thermal energy (temperature gradients or variations), radiant energy (sun, infrared, RF) and chemical energy (chemistry, biochemistry). These sources are characterized by different power densities (Figure 19).

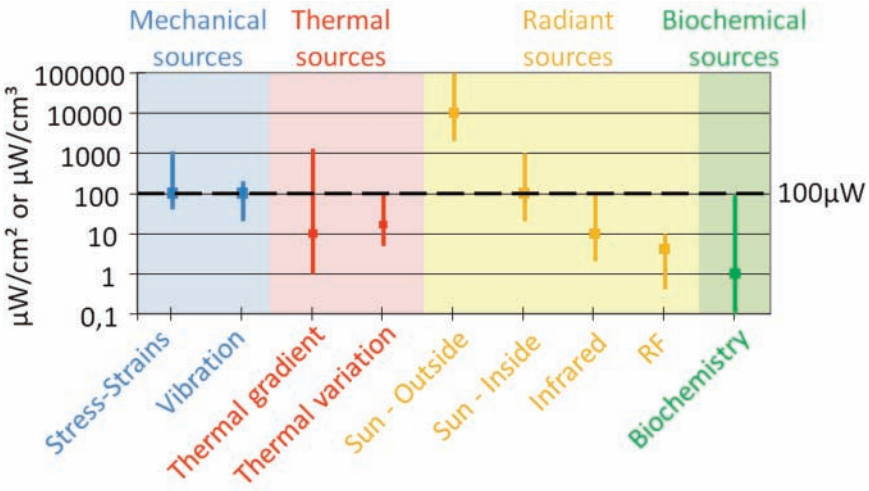


Figure 19 Ambient sources' power densities before conversion (Source: CEA-Leti)

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 (inside a machine, in a car …) there is no (or not enough) light and consequently thermal or mechanical energy may be a better alternative. Actually, it is mainly the primary energy source power density in the considered environment that defines the electrical output power that can be harvested and not the transducer itself, provided that this one is sufficiently well designed to extract this primary energy (15 to 30% efficiency for solar converters, 10 % of Carnot efficiency for thermo-electrical converters and around 50 % for mechanical converters). The figure also shows that, excluding "sun – outside", 10-100 μW is a fair order of magnitude for 1cm^2 or 1cm^3-EH output power [11].

Low power devices are expected to require 50mW in transmission mode and less in standby or sleep modes. EH devices cannot supply this amount of energy in a continuous active mode. Due to the ultra-low power consumption sleep mode, 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 Figure 20.

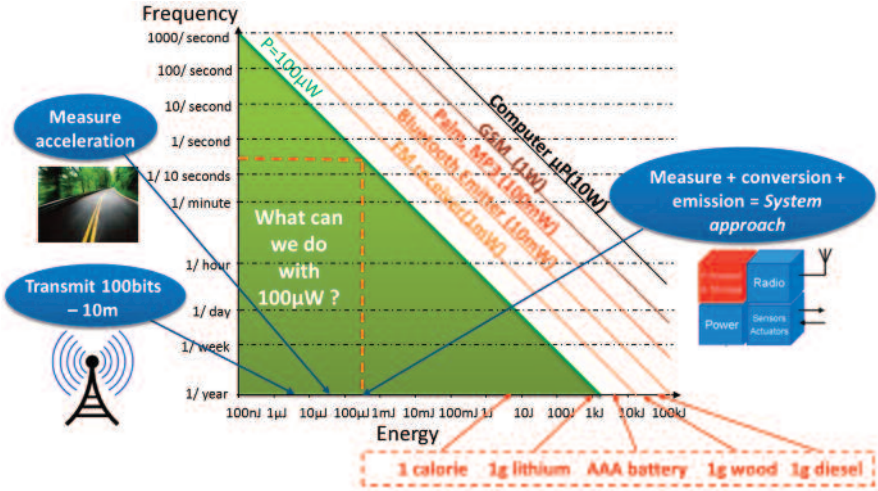


Figure 20 Power, Energy and Frequency diagram (Source: CEA-Leti)

By using log-log scales, with energy in abscissa and measurement frequency in ordinate, average power consumption is represented by straight lines of slope -1. Power sources are also represented in this diagram, and discrete sources (batteries, lithium, wood…) are compared with ambient energy sources (e.g. 100 μW is represented by the green line). For example, harvesting 100 μW during 1 year corresponds to a total amount of energy equivalent to 1 g of lithium.

Considering this approach of looking at energy consumption for one measurement instead of average power consumption, it results that, today:

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

Therefore, with 100 μW harvested continuously, it is possible to perform a complete measurement every 1-10 seconds (0.1-1Hz). This duty cycle can be sufficient for many applications (predictive maintenance); for the other applications, basic functions' power consumptions are expected to be reduced by 10 to 100 within 10 years; this will enable continuous running mode of EH-powered IoT devices.

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

10.3 Future Trends and recommendations

In the future, the number and types of IoT devices will increase, therefore inter-operability 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 [57] 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 of 100 in power consumption at same level of computation. Allowing for a 10 fold increase in IoT computation, power consumption should still be reduced by an order of 10.

On the other hand, energy harvesting techniques have been explored to respond to the energy consumption requirements of the IoT domain. For vibration energy harvesters, the most important focal area of research is probably the increase of the working frequency bandwidth that is still a technological bottleneck preventing this technology from being a viable and versatile supply source. A roadmap of vibration energy harvesters is provided in Figure 21.

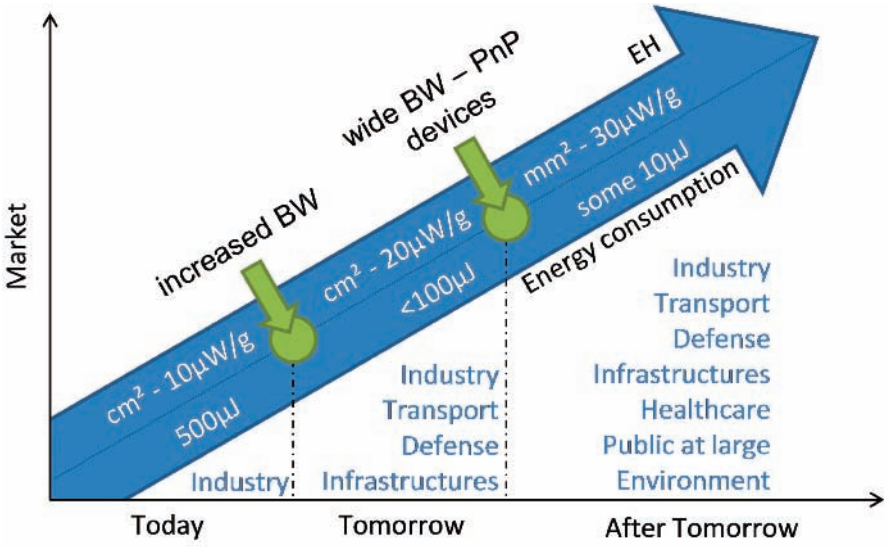


Figure 21 Roadmap for vibration energy harvesters (Source: CEA-Leti)

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

For thermoelectricity, the main challenge is not to increase the power density capability of thermoelectric materials as current materials are already able to convert large amount of powers (higher than 10 W/cm^2 for few 10's °C of thermal gradients). Yet, to produce 10 W of electrical power with a thermal gradient of 10°C, a thermal power flow of 3000 W is needed; this is very far from ambient thermal flows (around few mW).

Therefore, 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 even in darker places.

11 IoT Related Standardization

The IoT SRA 2010 [90] briefly addresses the topic of standardization and is focused on the actual needs of producing specific standards. This chapter examines further standardization considerations.

11.1 The role of standardization activities

Standards are needed for interoperability both within and between domains. Within a domain, standards can provide cost efficient realizations of solutions, and a domain here can mean even a specific organization or enterprise realizing an IoT. Between domains, the interoperability ensures cooperation between the engaged domains, and is more oriented towards a proper "Internet of Things". There is a need to consider the life-cycle process in which standardization is one activity. Significant attention is given to the "pre-selection" of standards through collaborative research, but focus should also be given to regulation, legislation, interoperability and certification as other activities in the same life-cycle. For IoT, this is of particular importance.

A complexity with IoT comes from the fact that IoT intends to support a number of different applications covering a wide array of disciplines that are not part of the ICT domain. Requirements in these different disciplines can often come from legislation or regulatory activities. As a result, such policy making can have a direct requirement for supporting IoT standards to be developed. It would therefore be beneficial to develop a wider approach to standardization and include anticipation of emerging or on going policy making in target application areas, and thus be prepared for its potential impact on IoT-related standardization.

A typical example is the standardization of vehicle emergency call services called eCall driven from the EC [22]. Based on the objective of increased road safety, directives were established that led to the standardization of

solutions for services and communication by e.g. ETSI, and subsequently 3GPP. Another example is the Smart Grid standardization mandate M/490 [67] from the EC towards the European Standards Organisations (ESOs), and primarily ETSI, CEN and CENELEC.

The conclusion is that any IoT related standardization must pay attention to how regulatory measures in a particular applied sector will eventually drive the need for standardized efforts in the IoT domain.

Agreed standards do not necessarily mean that the objective of interoperability is achieved. The mobile communications industry has been successful not only because of its global standards, but also because interoperability can be assured via the certification of mobile devices and organizations such as the Global Certification Forum [28] which is a joint partnership between mobile network operators, mobile handset manufacturers and test equipment manufacturers. Current corresponding M2M efforts are very domain specific and fragmented. The emerging IoT and M2M dependant industries should also benefit from ensuring interoperability of devices via activities such as conformance testing and certification on a broader scale.

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

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

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

From the point of view of standardisation IoT is a global concept, and is based on the idea that anything can be connected at any time from any place to any network, by preserving the security, privacy and safety. The concept of connecting any object to the Internet could be one of the biggest standardization challenges and the success of the IoT is dependant on the development of interoperable global standards. In this context the IERC position is very clear. Global standards are needed to achieve economy of scale and interworking. Wireless sensor networks, RFID, M2M are evolving to intelligent devices which need networking capabilities for a large number of applications and these technologies are "edge" drivers towards the "Internet of Things", while the network identifiable devices will have an impact on telecommunications networks. IERC is focussed to identify the requirements and specifications from industry and the needs of IoT standards in different domains and to harmonize the efforts, avoid the duplication of efforts and identify the standardization areas that need focus in the future.

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

11.2 Current situation

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

Another view is standards targeting protocols vs. systems. Much emphasis has been put on communications and protocol standards, but very little effort has previously been invested in standardizing system functions or system architectures that support IoT. Localized system standards are

plentiful for specific deployments in various domains. One such example is in building automation and control with (competing) standards like BACnet and KNX. However, system standards on the larger deployment and global scale are not in place. The on going work in ETSI M2M TC is one such approach, but is currently limited to providing basic application enablement on top of different networks. It should also be noted that ETSI represent one industry – the telecommunications industry. The IoT stakeholders are represented by a number of different industries and sectors reaching far beyond telecommunications.

11.3 Areas for additional consideration

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

The service layer infrastructure will require standardization of necessary capabilities like interfaces to information and sensor data repositories, discovery and directory services and other mechanisms that have already been identified in projects like SENSEI [87] and IoT-A [50] . Current efforts in ETSI M2M TC do not address these aspects.

The IoT will require federated environments where producers and consumers of services and information can collaborate across both administrative and application domains. This will require standardized interfaces on discovery capabilities as well as the appropriate semantic annotation to ensure that information becomes interoperable across sectors. Furthermore, mechanisms for authentication and authorization as well as provenance of information, ownership and "market mechanisms" for information become particularly important in a federated environment. Appropriate SLAs will be required for standardization. F-ONS [26] is one example activity in the direction of federation by GS1. Similar approaches will be needed in general for IoT including standardized cross-domain interfaces of sensor based services.

A number of IoT applications will be coming from the public sector. The Directive on Public Sector Information [82] requires open access to data. Integration of data coming from various application domains is not an easy task as data and information does not adhere to any standardized formats including their semantics. Even within a single domain, data and information is not easily integrated or shared. Consideration of IoT data and information integration and sharing within domains as well as between them, also needs to be considered at the international level.

Instrumental in a number of IoT applications is the spatial dimension. Standardization efforts that provide necessary harmonization and interoperability with spatial information services like INSPIRE [48] will be the key.

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

12 Recommendations on Research Topics

12.1 Applications

Applications of IoT are numerous, permeating into almost all domains of everyday life and activities of individuals and organizations. The challenges are numerous, varied and often related to a particular domain or the context in which an application is used. Abstracting those context specific challenges, the following are considered to be crucial for the successful development and adoption of IoT applications:

Efficient and simple mechanisms for interaction with "things"

Design of simple methods (and their standardization) that will enable application developers to include appropriate sensors, actuators and other "things" regardless of who designed and deployed them into applications without having to know the details of the implementation of each device.

These should include not only communication methods, but also normalization of observations taking into account the conditions under which the observations were taken.

Reliable and trustworthy participatory sensing

Inclusion of humans in the loop and leveraging their mobility and the mobility of their personal communication devices to capture "snapshots" of the physical world on a global scale and create a "community wisdom" view of the physical world.

Creating knowledge and making it available

Creation and provision of services capable of processing and analysing massive data generated by communicating things ("making sense out of sensed data") with open interfaces that allow their simple integration into various applications.

Set up interdisciplinary projects for smart energy, grid and mobility

Smart grid and smart mobility topics each merge know how from very different disciplines (e.g. traffic management, urban management, automotive, communication). Specialists in the fields are "speaking different languages" and need to come to a mutual understanding. Ideally projects should go along with show cases which could act as seeds for the new infrastructure. We need to address the challenges via a number of projects which are run by interdisciplinary consortia.

Foster Standardisation for smart energy, grid and mobility

Foster and promote international standardization activities in order to allow for coherent infrastructures and to open the market for competition.

Support Public Awareness

Some aspects of the technologies discussed are critical with respect to privacy and they will have social implications because, e.g., they deal with private information or they might affect urban planning. Accompanying studies could help us to understand social consequences and to identify eventual show stoppers by time. Critical issues should be put for public discussion in an early phase in order to avoid later acceptance problems.

Seamless integration of social and sensor networks

Tools and techniques for the seamless integration of social networks and

sensor networks, moving towards social IoT services that take into account the end-user's social preferences and interactions.

Infrastructures for social interactions between Internet-connected objects,

Infrastructure, which could enable new forms of M2M interactions along with associated opportunities for innovative applications and services. Research could build upon existing semantic interactions and M2M APIs.

Utility metrics and utility driven techniques for "Clouds of Things"

Specification of utility metrics and utility driven techniques in the scope of "Clouds of Things".

12.2 Recommendations for autonomic and self-aware IoT

Self-awareness from the design to deployment

The IoT will exponentially increase the scale and the complexity of existing computing and communication systems. Autonomy is thus an imperative property for the IoT systems to have. It should be considered from the very early phases of IoT systems implementations, from conception to deployment of devices, infrastructures and services. Self-awareness property should be injected to any software module, however separated from the functional code. 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.

Real-life use cases

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

Exploiting existing research

Existing fundamental research results from domains including artificial intelligence, biological systems, control theory, embedded systems and software engineering are necessary to build scientifically proven solid, robust and reliable solutions. Existing research may need to be tailored to the IoT context. In addition, multidisciplinary conferences and workshops should be organised to foster the interaction level between experts in those domains.

Security and privacy

Security and privacy issues should be considered very seriously since IoT deals not only with huge amount of sensitive data (personal data, business data, etc.) but also has the power of influencing the physical environment with its control abilities. Cyber-physical environments must thus be protected from any kind of malicious attacks. The IoT should autonomously tune itself to different levels of security and privacy, while not affecting the quality of service and quality of experience.

12.3 Infrastructure

IoT infrastructure as general infrastructure

More and more applications and services will rely on being directly connected to the physical world, i.e. for getting real-time information about the state of the real world or even for executing actuation tasks that directly influence the real world. Therefore, the IoT infrastructure needs to become a horizontal application-inde¬pendent infrastructure like electricity, water or communications infrastructures today. This requires a strong research focus on the infrastructure itself, which takes requirements from the large variety of IoT-related application areas, but is not specific to any one of them.

Easy connection and extension of infrastructure

It has to be made easy to add IoT devices to the IoT infrastructure based on plug-and-play type functionality, making additional configuration like semantic annota¬tion easy for the user. This will require more standardization activities on the protocol as at the information modelling level.

Core infrastructure services for supporting resolution, discovery, monitoring and adaptation

The infrastructure has to support the findings of relevant things and related services, enabling the connection to these services and facilitate the monitoring and adapta¬tion of applications and services as a result of changes in the IoT infrastructure, i.e., with respect to the availability of IoT and related services.

12.4 Networks, Communications

12.4.1 Networks

Research on mobile networks and mobile networks of networks

A widespread introduction of Internet of Things devices will cause mobile devices at the access fringe of the mobile communication network to evolve into their own mobile networks and even networks of networks. This predictable transition of the network structure has to become the topic of adequate research.

Research on load modelling of future IoT aware networks

In the emerging area of big data, related applications and widespread devices, sensors and actuators, predictive load modelling for the networks of the future will be essential for network optimization and pricing of network traffic, and it will influence the construction especially of such big data applications. The concurrent and synchronized development of all these fields is a field of challenging research.

Research on symbiosis of networking and IoT related distributed data processing

Large or global area applications will lead to a symbiosis of networking and distributed data processing. Generic architectures for this symbiosis, independent of specific applications, shall be researched, supporting data processing at the data sources, near to them or distributed randomly over the network.

12.4.2 Communications

Adapting the IP Protocol Paradigm

It is a paradigm that the IP protocol defines the Internet. Recent advances show that IP can be implemented on resource constrained IoT devices.

However, the constraints of very small IoT devices may be so limiting that optimised non-IP protocols may have to be used to communicate with them. Thus, it remains a research challenge to develop communications architectures that enable resource constrained devices to participate in the IoT while preserving the benefits of IP-based communications and application development.

Open communication architectures

Currently wireless communication standards are constructed to support the mobility of user devices. They use frame sizes of some milliseconds, implying a significant processing capacity at the user entities. Many classes of IoT devices neither use nor need this support, and they don't possess the required processing power. Methods to construct wireless mobile communications standards, open not only to constrained devices, but to all possible general communication modes in parallel at one time, shall be researched.

Communication architectures for (highly) constrained devices

Constrained and highly constrained devices in the context of the IoT promise to open new applications with significant market relevance. Due to their importance the air interfaces of these devices and their communication architecture should be researched starting from the constraints of these devices and they should be especially optimized for such (highly) constrained devices over all relevant communication layers.

Formal construction and proof methods in communications

Formal construction and proof methods in communications promise to lay a foundation for formally verifiable and formally verified communication architectures including interoperability up to the networks of networks structure of the Future Internet including the IoT. Such formal methods combined with semantic processing shall be topics in research aiming at their adoption for the construction and design of the Future Internet and the IoT.

Real-time lightweight protocols and platforms

Lightweight protocols and platforms for the real-time interaction with Internet-connected objects, including their interactive visualization.

12.5 Processes

The ability to model IoT-aware business processes, with all the peculiarities of such processes, and the availability of related process execution engines will be a key for further adoption of IoT technologies in the enterprise and business world. Research targeting the convergence of IoT with BPM and the necessary tooling needs to be strengthened. In particular it is recommended to address the following topics:

Modelling of IoT-aware processes

Existing (business) process modelling languages need to be extended and standardized in a way to support the highly event-driven nature of IoT processes, to explicitly integrate the notion of physical entities and devices, to add parameters for quality of information, trust, and reliability, and to enable the (sometimes ad hoc) distribution of sub-processes.

Inherent unreliability of IoT-aware processes

As the data coming from IoT devices such as sensors cannot always be guaranteed to be accurate and the devices and related services can suddenly fail, it is important that data quality and quality of service parameters can be modelled in order to build "reliable-enough" systems.

Execution of IoT-aware processes

Modelled processes as described above need to be executed both on centralized process execution engines, but often also on small, constrained devices. This holds true particularly for sub-processes responsible for the behaviour of a set of IoT devices. To support such operations, very lightweight and efficient process execution engines are needed.

Large-scale distribution of process logic

IoT processes are widely distributed in nature; certain parts of the business logic are often executed on local devices. This ranges from simple filtering and aggregation to the execution of business rules or even completely autonomous behaviour of individual devices. The methods and frameworks need to be developed to manage such distributions of software, to decide what (sub-) process is executed where, to monitor the systems, and to ensure that all parts always work in a safe operations envelope.

12.6 Data Information Management

In the context of Data Management, and the related and base technologies, there are some challenges and recommendations that should be considered as key elements to include in the Strategic Research Agenda for the near future. Some of the topics with room for improvement or unresolved issues are:

Standardisation and Interoperability

Different technologies and components involved in data processing still use proprietary or ad-hoc protocols or data formats, making the exchange of data among different systems or the interconnection of components for a combined processing of the information (for instance, connecting a Data Collection and Analysis platform with a Data Mining solution) impossible or very complex. It is essential that data representation, interfaces and protocols are standardised or open, allowing a true "protocol independence" and interoperability.

Distribution, Federation and De-centralisation

Currently, most of the systems and platforms devised for acquisition, storage or processing of data are centralised and operated by a single administrator managing physical resources allocated in a very precise geographical location. No interconnection or distribution of data is permitted, thus limiting the possibilities for parallel or concurrent processing of data and also limiting the scope and domain of data that can be collected by the system. In the future, systems should have the capacity to be deployed and distributed geographically. A distributed system avoids or reduces the risk of failures and minimises the existence of bottlenecks in certain parts or features of the system. Federation policies, with reliable trust mechanisms, must be established to ensure that data can be accessed or exchanged remotely without compromising the integrity or security of involved data.

Data protection, Privacy and Security

When addressing data management, coming from very various sources and containing information on many different aspects, data security and privacy aspects are critical. Different access levels, control policies, and mechanisms to guarantee that no identification of personal data is possible by unauthorised clients/operators must be carefully defined and applied.

In addition, and depending on the use case or scenario, "opt-in" paradigms (in which users must voluntarily express and confirm their awareness and willingness to share personal data) should be incorporated as much as possible.

Improved semantics and Data Mining

Currently, the volume of data susceptible of being collected and automatically stored in information systems is huge. Often, the main problem is how to "understand" the information captured by the sensors or stored in the databases. The lack of "data interpretation" impedes the efficient processing of the information when searching for results or trying to extract useful information from the source data. A lot of effort must be devoted to the definition and implementation of semantics and rules making it easier to process the information. Data representation (within databases) and search/processing algorithms should be capable of handling higher levels of abstraction, closer to human interpretation and manipulation of information, and allowing the (automatic) generation or extraction of relationships among data components (making possible the definition of complex inference rules). In this sense, definition and processing of Complex Events (the whole CEP concept) is a field yet to be explored.

Data sharing and optimization techniques

Novel data sharing and optimization techniques for cloud-based IoT environments.

Publishing techniques for sensor data and from interconnected objects

Techniques for the publishing of data stemming from sensors and Internet-connected objects as Linked Data, including techniques for the integration of IoT with the Linked Open Data Cloud (LOD).

12.7 Security

Improved frameworks and mechanisms for trust relationships

Further research is required to develop improved frameworks and mechanisms to enable trust relationships to be established, maintained and assessed. In IoT-centric scenarios, trust relationships are required between people, devices and data. Decentralised, self-configuring approaches are better suited to the IoT.

Security against infrastructure disruption

As IoT becomes incorporated into national and critical infrastructure, there is a requirement to provide security against infrastructure disruption. Research is required into attack detection and recovery/resilience for IoT-specific threats, as well as management support such as situational awareness tools/techniques and decision making.

Privacy protection mechanisms

As much of the IoT involves personal information, privacy mechanisms must be developed that enable individuals to control the handling of personal information. Research is required to develop privacy protection mechanisms that enable data to be stored/processed without the content being accessible to others and to prevent information being inferred about individuals from IoT exchanges.

12.8 Device Level Energy Issues

Low power communication

Power consumption reduction of RF full-receiver should have a target much below 5 mW to enable very small form factor and long life-time battery. Targeting below 1 mW would then enable support from energy harvesting systems enabling energy autonomous RF communications.

Ultra-wideband

Ultra-wideband is not to be forgotten in the Internet of Things domain, as it provides a feature of great interest in addition to the communication itself, which is the ranging or indoor localization one [71] . Here, standardization is also expected to arise and market development to come. Mature solutions are now available, and waiting for market deployment and public acceptance.

Solar and thermal energy harvesting

Thermoelectric materials' intrinsic efficiency should be improved 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). Similarly, photovoltaic cells should be efficiency improved to decrease photovoltaic cells' sizes and to harvest energy even in darker places for IoT devices.

Vibration energy harvesting

Vibration energy harvesters will have higher power densities in the future (from 10 μW/g to 30 μW/g) and work on a wider frequency bandwidth. We expect that vibration energy harvesting devices to be Plug and Play (PnP) and to be able to work in any vibrating environment, within 10 years.

12.9 Standardization

Life-cycle approach towards standardization

Standardization should be viewed as only one activity in a life-cycle process that also includes preparatory regulatory and legislative activities, as well as post-standardization activities towards certification and validation. Special care should be taken for understanding pre-standardization impacts coming from the various applied sectors.

Increased influence from applied Internet of Things sector

As the Internet of Things represents a set of technologies and tools to support a number of different applied sectors with varying needs, standardization efforts increasingly need to connect to those applied sectors and cannot be done in isolation as a self-contained topic. In particular, attention should not only be paid to proper SDOs, but also to Special Interest Groups, various Industry Alliances, but also open communities which also drive technology development and set "de facto" standards in their particular applied domain.

Reduce technology fragmentation

Technology fragmentation is a feature of the Internet of Things, particularly on the device side. There is a need to drive further standardization of device technologies in the direction of using standard Internet protocols and Embedded Web technologies including Internet of Things data semantics, with the purpose to achieve true interoperability and horizontalization. More attention need also be taken towards standardized and open tools for development of Internet of Things devices.

Open system for integration of Internet of Things data

It is necessary to ensure the efficient integration of Internet of Things data from devices in an open environment. This will require standardization of Internet of Things data formats and semantics. Furthermore, tools and technologies are required to achieve sharing of Internet of Things data across applied domains, and standardization should be considered as a means to ensure the open and secure availability of Internet of Things data and information.

Transparent interaction with third-party IoT infrastructures

Tools and techniques for transparently interacting with third-party IoT infrastructures (including standards-based architectures (OGC/SWE) and Internet of Things platforms (such as Pachube.com)).

12.10 Societal, Economic and Legal Issues

Accessibility

The complexity of user requirements resulting from personal characteristics and preferences, together with the variety of devices they might use, poses a problem of systems being non-inclusive for individual users that have non-mainstream needs. Accessibility of future IoT technologies will be a challenge that needs to be addressed.

Trust and Privacy

Users' privacy concerns about the accessibility and use of information captured by IoT devices and sensors is an important challenge, and users need to be assured that the future Orwellian Big Brother nightmare isn't becoming a reality. They must be enabled to understand and manage and control the exposure of their private and sensitive data. This also includes legislation ensuring individual privacy rights with respect to what kind of surveillance and information the authorities can employ and access.

Development	2012-2015	2016-2020	Beyond 2020
Identification Technology	• Unified frameworkfor unique identifiers • Open framework for the IoT • URIs	• Identity management • Semantics • Privacy awareness	• "Thing DNA" identifier
Internet of Things Architecture Technology	• IoT architecture developments • IoT architecture in the FI • Network of networks architectures • F-O-T platforms interoperability	• Adaptive, context based architectures • Self-* properties	• Cognitive architectures • Experimental architectures
Internet of Things Infrastructure	• Special purpose IoT infrastructures • Application specific deployment • Operator specific deployment	• Integrated IoT infrastructures • Multi application infrastructures • Multi provider infrastructures	• Global, general purpose IoT infrastructures
Internet of Things Applications	• Participatory sensing • Cheap, configurable IoT devices	• IoT in food/water production and tracing	• IoT information open market
Communication Technology	• Ultra low power chip sets • On chip antennas • Millimeter wave single chips • Ultra low power single chip radios • Ultra low power system on chip	• Wide spectrum and spectrum aware protocols	• Unified protocol over wide spectrum
Network Technology	• Self aware and self organizing networks • Sensor network location transparency • Delay tolerant networks • Storage networks and power networks • Hybrid networking technologies	• Network context awareness	• Network cognition • Self-learning, self repairing networks
Software and algorithms	• Large scale, open semantic software modules • Composable algorithms • Next generation IoT-based social software • Next generation IoT-based enterprise applications • IoT-aware process modelling languages and corresponding tools	• Goal oriented software • Distributed intelligence, problem solving • Things-to-Things collaboration environments	• User oriented software • The invisible IoT • Easy-to-deploy IoT sw • Things-to Humans collaboration • IoT 4 All
Hardware	• Multi protocol, multi standards readers • More sensors and actuators • Secure, low-cost tags (e.g. Silent Tags) • NFC in mobile phones • Sensor integration with NFC • Home printable RFID tags	• Smart sensors (bio-chemical) • More sensors and actuators (tiny sensors)	• Nano technology and new materials

Development	2012-2015	2016-2020	Beyond 2020
Data and Signal Processing Technology	• Energy, frequency spectrum aware data processing • Data processing context adaptable	• Context aware data processing and data responses	• Cognitive processing and optimisation
Discovery and Search Engine Technologies	• Distributed registries, search and discovery mechanisms • Semantic discovery of sensors and sensor data	• Automatic route tagging and identification management centres	• Cognitive search engines • Autonomous search engines
Power and Energy Storage Technologies	• Energy harvesting (energy conversion, photovoltaic) • Printed batteries • Long range wireless power	• Energy harvesting (biological, chemical, induction) • Power generation in harsh environments • Energy recycling • Wireless power	• Biodegradable batteries • Nano-power processing unit
Security, Privacy & Trust Technologies	• User centric context-aware privacy and privacy policies • Privacy aware data processing • Virtualization and anonymisation • Scalable PKI based on hierarchical and Cross certification approaches • Lightweight key management for establishing trust relationships • Privacy by Design techniques, including data minimisation, identification, authentication and anonymisation	• Security and privacy profiles selection based on security and privacy needs • Privacy needs automatic evaluation • Context centric security • Homomorphic Encryption • Searchable Encryption • Protection mechanisms for IoT DoS/DdoS attacks	• Self adaptive security mechanisms and protocols • Self-managed secure IoT
Material Technology	• SiC, GaN • Silicon • Improved/new semiconductor manufacturing processes/technologies for higher temperature ranges	• Diamond	• Graphen
Standardisation	• IoT standardization • M2M standardization • Interoperability profiles • Application independent sensor and actuator semantics and profiles	• Standards for cross interoperability with heterogeneous networks • IoT data and information sharing	• Standards for autonomic communication protocols

Research Needs	2012-2015	2016-2020	Beyond 2020
Identification Technology	• Convergence of IP and IDs and addressing schem • Unique ID • Multiple IDs for specific cases • Extend the ID concept (more than ID number) • Electro Magnetic Identification - EMID	• Beyond EMID	• Multi methods – one ID
IoT Architecture	• Extranet (Extranet of Things) (partner to partner applications, basic interoperability, billions-of- things)	• Internet (Internet of Things) (global scale applications, global interoperability, many trillions of things)	
Internet of Things Infrastructure	• Application domain-independent abstractions & functionality • Cross-domain integration	• Cross-domain integration and management • Large-scale deployment of infrastructure • Context-aware adaptation of operation	• Self management and configuration
Internet of Things Applications	• Incentives and trust issues in participatory sensing applications • Linked open data for IoT • Standardization of APIs	• IoT information open market	• Building and deployment of public IoT infrastructure with open APIs and underlying business models
SOA Software Services for IoT	• Composed IoT services (IoT Services composed of other Services, single domain, single administrative entity) • Modelling and execution of IoT aware (business) processes • Quality of Information and IoT service reliability	• Highly distributed IoT processes • Semi-automatic process analysis and distribution	• Fully autonomous IoT devices
Internet of Things Architecture Technology	• Adaptation of symmetric encryption and public key algorithms from active tags into passive tags • Universal authentication ofobjects • Graceful recovery of tags following power loss • More memory • Less energy consumption • 3-D real time location/position embedded systems • IoT Governance scheme	• Code in tags to be executed in the tag or in trusted readers • Global applications • Adaptive coverage • Object intelligence • Context awareness	• Intelligent and collaborative functions
Communi - cation Technology	• Longer range (higher frequencies – tenths of GHz) • Protocols for interoperability • Protocols that make tags resilient to power interruption and fault induction • Collision-resistant algorithms	• On chip networks and multi standard RF architectures • Plug and play tags • Self repairing tags	• Self configuring, protocol seamless networks
Network Technology	• Grid/Cloud network • Hybrid networks • Ad hoc network formation • Self organising wireless mesh networks • Multi authentication • Sensor RFID-based systems • Networked RFID-based systems interface with other networks – hybrid systems / networks	• Service basednetwork • Integrated/universal authentication • Brokering of data through market mechanisms	• Need based network • Internet of **Everything** • Robust security based on a combination of ID metrics • Autonomous systems for non stop information technology service

Research Needs	2012-2015	2016-2020	Beyond 2020
Software and algorithms	• Self management and control • Micro operating systems • Context aware business event generation • Interoperable ontologies of business events • Scalable autonomous software • Software for coordinated emergence • (Enhanced) Probabilistic and non-probabilistic track and trace algorithms, run directly by individual "things" • Software and data distribution systems	• Evolving software • Self reusable software • Autonomous things: o Self configurable o Self healing o Self management • Platform for object intelligence	• Self generating "molecular" software • Context aware software
Hardware Devices	• Paper thin electronic display with RFID • Ultra low power EPROM/FRAM • NEMS • Polymer electronic tags • Antennas on chip • Coil on chip • Ultra low power circuits • Electronic paper • Devices capable of tolerating harsh environments (extreme temperature variation, vibration and shock conditions and contact with different chemical substances) • Nano power processing units • Silent Tags • Biodegradable antennae	• Polymer based memory • Molecular sensors • Autonomous circuits • Transparent displays • Interacting tags • Collaborative tags • Heterogeneous integration • Self powering sensors • Low cost modular devices	• Biodegradable antennas • Autonomous "bee" type devices
Hardware Systems, Circuits and Architectures	• Multi protocol front ends • Multi standard mobile readers • Extended range of tags and readers • Transmission speed • Distributed control and databases • Multi-band, multi-mode wireless sensor architectures • Smart systems on tags with sensing and actuating capabilities (temperature, pressure, humidity, display, keypads, actuators, etc.) • Ultra low power chip sets to increase operational range (passive tags) and increased energy life (semi passive, active tags) • Ultra low cost chips with security • Collision free air to air protocol • Minimum energy protocols	• Adaptive architectures • Reconfigurable wireless systems • Changing and adapting functionalities to the environments • Micro readers with multi standard protocols for reading sensor and actuator data • Distributed memory and processing • Low cost modular devices • Protocols correct by construction	• Heterogeneous architectures • "Fluid" systems, continuously changing and adapting
Data and Signal Processing Technology	• Common sensor ontologies (cross domain) • Distributed energy efficient data processing	• Autonomous computing • Tera scale computing	• Cognitive computing
Discovery and Search Engine Technologies	• Scalable Discovery services for connecting things with services while respecting security, privacy and confidentiality • "Search Engine" for Things • IoT Browser • Multiple identities per object	• On demand service discovery/integration • Universal authentication	• Cognitive registries
Power and Energy Storage Technologies	• Printed batteries • Photovoltaic cells • Super capacitors • Energy conversion devices • Grid power generation • Multiple power sources	• Paper based batteries • Wireless power everywhere, anytime • Power generation for harsh environments	• Biodegradable batteries

Research Needs	2012-2015	2016-2020	Beyond 2020
Security, Privacy & Trust Technologies	• Adaptation of symmetric encryption and public key algorithms from active tags into passive tags • Low cost, secure and high performance identification/ authentication devices • Quality of Information to enable reliable data processing • Assurance methods for trusted platforms • Access control and accounting schemes for IoT • General attack detection and recovery/resilience for IoT • Cyber Security Situation Awareness for IoT • Fine-grained self configuring access control to IoT • Ensuring end users that they are in control of their sensitive and private data	• Context based security activation algorithms • Service triggered security • Context-aware devices • Object intelligence • Decentralised self configuring methods for trust establishment • Novel methods to assess trust in people, devices and data • Location privacy preservation • Personal information protection from inference and observation	• Cognitive security systems • Self-managed secure IoT • Decentralised approaches to privacy by information localisation
Societal responsibility	• Impact of IoT on environment, labour market, education, society at large • IoT also for underprivileged people	• Smart assistance by IoT in daily live	
Governance (legal aspects)	• Allocation and management of IPv6 addresses + RFID tags • Identifier uniqueness	• Legal framework for transparency of IoT bodies and organizations	
Economic	• Business cases and value chains for IoT		
Material Technology	• Carbon • Conducting Polymers and semiconducting polymers and molecules • Conductive ink • Flexible substrates • Modular manufacturing techniques	• Carbon nanotube	• Graphen

References

1. Analysys Mason, Imagine an M2M world with 2.1 billion connected things, online at http://www.analysysmason.com/about-us/news/insight/M2M_forecast_Jan2011/

2. ATOS - Ascent Look Out – Telecom, Media & Technology, online at http://ascentlookout.atos.net/en-us/download/default.htm

3. "Body Area Networks and Technology", BANET project, France, 1.1.2008-30.6.2010,

www.banet.fr

4. K. Ashton, "That 'Internet of Things' Thing", online at http://www.rfidjournal.com/article/view/4986, June 2009

5. P. Barnaghi, M. Presser, and K. Moessner, "Publishing Linked Sensor Data", in Proceedings of the 3rd International Workshop on Semantic Sensor Networks (SSN),

Organised in conjunction with the International Semantic Web Conference (ISWC) 2010, November 2010

6. Worldwide Cellular M2M Modules Forecast, Beecham Research Ltd, August 2010

7. The Global Wireless M2M Market, Berg Insight, 2010, http://www.berginsight.com/ReportPDF/ProductSheet/bi-gwm2m-ps.pdf

8. C. Bizer, T. Heath, K. Idehen, and T. Berners-Lee, "Linked Data on the Web",

Proceedings of the 17th International Conference on World Wide Web (WWW'08),

New York, NY, USA, ACM, pp.1265-1266, 2008

9. The Official Bluetooth Technology Info Site, online at http://www.bluetooth.com/

10. Bluetooth Low Energy (LE) Technology Info Site, online at

http://www.bluetooth.com/English/Products/Pages/low_energy.aspx

11. S. Boisseau and G. Despesse,"Energy Harvesting, Wireless Sensor Networks & Opportunities for Industrial Applications", in EETimes, 27th Feb 2012, online at http://www.eetimes.com

12. M. Botts, G. Percivall, C. Reed, and J. Davidson, "oGC Sensor Web Enablement: Overview and High Level Architecture",The Open Geospatial Consortium, 2008, online at

http://portal.opengeospatial.org/files/?artifact id=25562

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

14. BUTLER, EU FP7 project, Smartlife – Secure and Context Awareness in the IoT,

http://www.iot-butler.eu/

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

16. The CEP Blog, http://www.thecepblog.com/

17. K. M. Chandy and W. R. Schulte, "What is Event Driven Architecture (EDA) and Why Does it Matter?", 2007, online at http://complexevents.com/?p=212, (accessed on: 25.02.2008).

18. Creative Partnerships Are Key To M2M Market Development for Wireless Carriers

White paper, Harbor Research, Inc, 2011

19. E. Dans (2011), Big Data: a small introduction, Retrieved from online at,

http://www.enriquedans.com/2011/10/big-data-una-pequena-introduccion.html

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

21. S. Decker and M. Hauswirth, "Enabling networked knowledge", in CIA '08:

Proceedings of the 12th international workshop on Cooperative Information Agents XII,

Berlin, Heidelberg: Springer-Verlag, pp. 1-15, 2008.

22. eCall - eSafety Support, online at

http://www.esafetysupport.org/en/ecall_toolbox/european_commission/index.html.

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

24. A. El Gamal, and Y-H Kim,"Network Information Theory", Cambridge University Press, 2011.

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

26. Federated Object Naming Service, GS1, online at http://www.gs1.org/gsmp/community/working_groups/gsmp#FONS

27. J. Formo, M. Gårdman, and J. Laaksolahti, "Internet of things marries social media", in

Proceedings of the 13th International Conference on MobileHCI, ACM, New York, NY, USA, pp. 753-755, 2011.

28. Global Certification Forum, online at http://www.globalcertificationforum.org

29. N. Gershenfeld, When Things Start to Think, Holt Paperbacks, New York, 2000

30. N. Gershenfeld, R. Krikorian and D. Cohen, Scientific Am., Sept., 2004.

31. A. Gluhak, M. Hauswirth, S. Krco, N. Stojanovic, M. Bauer,

R. Nielsen, S. Haller, N. Prasad, V. Reynolds, and O. Corcho, "An Architectural Blueprint for a Real-World

Internet", in The Future Internet - Future Internet Assembly 2011: Achievements and Technological Promises, Lecture Notes in Computer Science, Vol. 6656, 1 st Edition, Chapter 3.3 Interaction Styles, 2011.

32. GreenTouch Consortium, online at www.greentouch.org.

33. GreenTouch, "Annual Report 2010-2011", online at http://www.greentouch.org/uploads/documents/GreenTouch_2010-2011_Annual_Report.pdf

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

35. S. Haller, S. Karnouskos, and C. Schroth, The Internet of Things in an Enterprise Context, in

J. Domingue, D. Fensel und P. Traverso (Eds.)

First Future Internet Symposium - FIS 2008

LNCS 5468, Springer Verlag 2009, pp. 14-28.

36. S. Haller and C. Magerkurth, "The Real-time Enterprise: IoT-enabled Business Processes",

IETF IAB Workshop on Interconnecting Smart Objects with the Internet, March 2011

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

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

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

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

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

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

43. M. C. Huebscher, J. A. McCann, A survey of autonomic computing — degrees, models, and applications. ACM Computing Surveys (CSUR), Volume 40 Issue 3, August 2008.

44. IBM, "An architectural blueprint for autonomic computing", IBM White paper. June 2005

45. iCore, EU FP7 project, Empowering IoT through Cognitive Technologies, http://www.iot-icore.eu/

46. IEEE Std 802.15.4™-2006, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), online at http://www.ieee802.org/15/pub/TG4.html

47. IERC – European Research Cluster on the Internet of Things, "Internet of Things - Pan European Research and Innovation Vision", October, 2011, online at, http://www.theinternetofthings.eu/sites/default/files/Rob%20van%20Kranenburg/IERC_IoT-Pan%20European%20Research%20and%20Innovation%20Vision_2011.pdf

48. INSPIRE, EU FP7 project, – Infrastructure for Spatial Information in Europe, online at http://inspire.jrc.ec.europa.eu/

49. IoT6 – Universal Integration of the Internet of Things through an IPv6-based Service Oriented Architecture enabling heterogeneous components interoperability http://www.iot6.eu/

50. IoT-A, EU FP7 project, online at http://www.iot-a.eu

51. IoT.est, EU FP7 project, Internet of Things Environment for Service Creation and Testing,

http://ict-iotest.eu/iotest/

52. IoT-I, Internet of Things Initiative, FP7 EU project, FP7-ICT-2009-5-257565

http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_LANG=EN&PJ_RCN=11411957, http://www.iot-i.eu

53. ISO, International Organization for Standardization (ISO), Identification cards -- Contactless integrated circuit(s) cards -- Vicinity cards, ISO/IEC 14443, 2003.

54. ITU-T , Internet of Things Global Standards Initiative, http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

55. J. B., Kennedy, "When woman is boss, An interview with Nikola Tesla", in Colliers, January 30, 1926.

56. M. Kirkpatrick, "The Era of Location-as-Platform Has Arrived", ReadWriteWeb, January 25, 2010.

57. J.G. Koomey, S. Berard, M. Sanchez, and H. Wong, "Implications of Historical Trends in the Electrical Efficiency of Computing", in IEEE Annals of the History of Computing, vol. 33, no. 3, pp. 46-54, March 2011.

58. M. Kranz, L. Roalter, and F. Michahelles, "Things That Twitter: Social Networks and the Internet of Things", in What can the Internet of Things do for the Citizen (CIoT) Workshop at

The Eighth International Conference on Pervasive Computing (Pervasive 2010), Helsinki, Finland, May 2010.

59. D. Lachartre, "A 550 μW inductorless bandpass quantizer in 65 nm CMOS for 1.4-to-3 GHz digital RF receivers", VLSI Circuits 2011, pp. 166-167, 2011.

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

61. Link, Internet of Things, online at http://www.link.pt/default.aspx?idl=2

62. Y. Liu, D. Hill, A. Rodriguez, L. Marini, R. Kooper, J. Myers, et al., "A new framework for on-demand virtualization, repurposing and fusion of heterogeneous sensors", International Symposium on Collaborative Technologies and Systems, pp. 54-63, 2009.

63. Logical Neighborhoods, Virtual Sensors and Actuators, online at http://logicalneighbor.sourceforge.net/vs.html

64. L. Lolis, C. Bernier, M. Pelissier, D. Dallet, and J.-B. Bégueret, "Bandpass Sampling RX System Design Issues and Architecture Comparison for Low Power RF Standards", IEEE ISCAS 2010.

65. D. Luckham, The Power of Events, Addison-Wesley, Boston, USA, 2002.

66. D. Luckham, "What's the Difference Between ESP and CEP?", 2006, online at http://complexevents.com/?p=103, accessed on 15.12.2008

67. European Commission, "Smart Grid Mandate, Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployments", M/490 EN,,Brussels 1st March, 2011.

68. Z. Ma, "An Electronic Second Skin", in Science, vol. 333, 830-831 12 August, 2011.

69. N. Maisonneuve, M. Stevens, M. E. Niessen, L. Steels, "NoiseTube: Measuring and mapping noise pollution with mobile phones", in Information Technologies in Environmental Engineering (ITEE 2009), Proceedings of the 4th International ICSC SymposiumThessaloniki, Greece, May 28-29, 2009.

70. makeSense, EU FP7 Project, online at http://www.project-makesense.eu/,

last accessed: November 15, 2011

71. G. Masson, D. Morche, H. Jacquinot, and P. Vincent, "A 1 nJ/b 3.2-4.7 GHz UWB 50 Mpulses/s Double Quadrature Receiver for Communication and Localization", in ESSCIRC 2010.

72. R. Milner, "Communicating and Mobile Systems: The π-calculus", Cambridge University Press, 1999, ISBN 0-521-65869-1.

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

74. OASIS, Web Services Business Process Execution Language, online at

http://docs.oasis-open.org/wsbpel/2.0/wsbpel-v2.0.html, last accessed: November 15, 2011

75. occam 2.1 Reference Manual, SGS-Thomson Microelectronics Ltd, INMOS document 72 occ 45 03. Open Geospatial Consortium (OGC), "Geospatial and location standards", online at

http://www.opengeospatial.org

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

77. Open IoT, Open Source blueprint for large scale self-organizing cloud environments for IoT applications, http://cordis.europa.eu/fetch?CALLER=PROJ_ICT&ACTION=D&CAT=PROJ&RCN=101534

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

79. N. Pletcher, S. Gambini, and J. Rabaey, "A 52 μW Wake-Up Receiver With 72 dBm Sensitivity Using an Uncertain-IF Architecture", in IEEE Journal of Solid-State Circuits, vol. 44, no1, January, pp. 269-280. 2009

80. PROBE-IT, EU FP7 project,, Pursing Roadmaps and Benchmarks for the Internet of Things

http://www.probe-it.eu/

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

82. Directive 2003/98/EC of the European Parliament and of the Council on the reuse of public sector information, 17 November 2003, online at http://ec.europa.eu/information_society/policy/psi/docs/pdfs/directive/psi_directive_en.pdf.

83. J. Ryckaert, A. Geis, L. Bos, G. van der Plas, J. Craninckx, "A 6.1 GS/s 52.8 mW 43 dB DR 80 MHz Bandwidth 2.4 GHz RF Bandpass Σ-Δ ADC in 40 nm CMOS", in IEEE Radio-Frequency Integrated Circuits Symposium, 2010.

84. IEEE International Conferences on Self-Adaptive and Self-Organizing Systems

http://www.saso-conference.org/

85. Dieter Scholz-Reiter, Marc-André Isenberg, Michael Teucke, Harry Halfar, (2010)

An integrative approach on Autonomous Control and the Internet of Things

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

87. SENSEI, EU FP7 project, online at http://www.sensei-project.eu.

88. A. Sheth, C. Henson, and S. Sahoo, "Semantic sensor web", Internet Computing, IEEE, vol. 12, no. 4, pp. 78-83, July-Aug. 2008

89. Smart Food and Agribusiness, EU FP7 project, Future Internet for Safe and Healthy Food from Farm to Fork http://smartagrifood.eu/

90. SmartSantander, EU FP7 project,, Future Internet Research and Experimentation, online at

http://www.smartsantander.eu/

91. O. Vermesan, P. Friess, Internet of Things - Global Technological and Societal Trends, River Publishers, 2011, ISBN 978-87-92329-67-7.

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

93. W3C Semantic Sensor Network Incubator Group, Incubator Activity, online at

http://www.w3.org/2005/Incubator/ssn/

94. Semantic Sensor Network Incubator Group, State of the Art Survey

http://www.w3.org/2005/Incubator/ssn/wiki/State_of_the_art_survey

95. M-G. Di Benedetto and G. Giancola, Understanding Ultra Wide Band Radio Fundamentals,

Prentice Hall, June 27, 2004

96. S. Venkatesan, "Limits on transmitted energy per bit in a cellular wireless access network",

Private communication, Radio Access Domain, Bell Labs, New Jersey, USA

97. O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, et al., "Internet of Things Strategic Research Agenda", Chapter 2 in Internet of Things - Global Technological and Societal Trends, River Publishers, 2011, ISBN 978-87-92329-67-7.

98. A. Vouilloz, M. Declercq, and C. Dehollain, "A Low-Power CMOS Super-Regenerative Receiver at 1 GHz", in IEEE Journal of Solid-State Circuits, vol. 36, no3, March, pp. 440-451, 2001.

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

100. R.H. Weber/R. Weber, Internet of Things - Legal Perspectives Springer, Berlin 2010

101. Body Area Networks, IEEE 802.15 WPAN Task Group 6 (TG6), online at

http://www.ieee802.org/15/pub/TG6.html

102. M. Weiser, "The Computer for the 21st Century," Scientific Am., Sept., 1991, pp. 94-104; reprinted in IEEE Pervasive Computing, Jan.-Mar. 2002, pp. 19-25."

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

104. Casaleggio Associati, "The Evolution of Internet of Things", February 2011, online at http://www.casaleggio.it/pubblicazioni/Focus_internet_of_things_v1.81%20-%20eng.pdf

Acknowledgments

The IoT European Research Cluster - European Research Cluster on the Internet of Things (IERC) maintains its Strategic Research Agenda (SRA), taking into account its experiences and the results from the on going exchange among European and international experts. The present document builds on the 2009 and 2010 Strategic Research Agendas and presents the research fields and an updated roadmap on future R&D until 2015 and beyond 2020.

The IoT European Research Cluster SRA is part of a continuous IoT community dialogue initiated by the European Commission (EC) DG INFSO-D4 Unit for the European and international IoT stakeholders. The result is a lively document that is updated every year with expert feedback from on going and future projects within the FP7 Framework Program on Research and Development in Europe.

Many colleagues have assisted over the last few years with their views on the Internet of Things strategic research agenda document. Their contributions are gratefully acknowledged.

List of Contributors

Abdur Rahim Biswas, IT, create-net, iCore
Ali Rezafard, IE, Afilias, EPCglobal Data Discovery JRG
Amine Houyou, DE, SIEMENS, IoT@Work
Andras Vilmos, HU, Safepay, StoLPaN
Anthony Furness, UK, AIDC Global Ltd & AIM UK, CASAGRAS, RACE networkRFID
Antonio Manzalini, IT, Telecom Italia, CASCADAS
Carlo Maria Medaglia, IT, University of Rome 'Sapienza', IoT-A
César Viho, FR, Probe-IT
Claudio Pastrone, IT, ISMB, Pervasive Technologies Research Area, ebbits
Daniel Thiemert, UK, University of Reading, HYDRA
David Simplot-Ryl, FR, INRIA/ERCIM, ASPIRE
Dimitris Kiritsis, CH, EPFL, IMS2020
Eric Mercier, FR, CEA-Leti
Erik Berg, NO, Telenor, IoT-I
Florent Frederix, EU, EC, EC
Franck Le Gall, FR, Inno, WALTER
François Carrez, GB, IoT-I
Frederic Thiesse, CH, University of St. Gallen, Auto-ID Lab
Giuseppe Abreu, IT, Butler

Ghislain Despesse, FR, CEA-Leti
Harald Vogt, DE, SAP, SToP
Harald Sundmaeker, DE, SmartAgriFood, ATB GmbH, CuteLoop
Humberto Moran, UK, Friendly Technologies, PEARS Feasibility
Ian Smith, UK, CASAGRAS2
Jan Höller, EAB
Jens-Matthias Bohli, DE, NEC
John Soldatos, GR, Athens Information Technology, ASPIRE, OpenIoT
Jose-Antonio, Jimenez Holgado, ES, TID
Karel Wouters, BE, K.U. Leuven, PrimeLife
Klaus Moessner, UK, UNIS, IoT.est
Kostas Kalaboukas, GR, SingularLogic, EURIDICE
Levent Gürgen, FR, CEA-Leti
Mario Hoffmann, DE, Fraunhofer-Institute SIT, HYDRA
Mark Harrison, UK, University of Cambridge, Auto-ID Lab, BRIDGE
Markus Eisenhauer, DE, Fraunhofer-FIT, HYDRA, ebbits
Markus Gruber, DE, ALUD
Martin Bauer, DE, NEC, IoT-A
Maurizio Spirito, IT, Istituto Superiore Mario Boella, Pervasive Technologies
Research Area, ebbits
Maurizio Tomasella, UK, University of Cambridge, Auto-ID Lab, SMART, BRIDGE, Auto-ID Lab
Mirko Presser, DK, Alexandra Institute, IoT-I
Neeli Prasad, DK, CTIF, University of Aalborg, ASPIRE
Paolo Paganelli, IT, Insiel, EURIDICE
Payam Barnaghi, UK, UNIS, IoT.est
Philippe Cousin, FR, easy global market, PROBE-IT, Walter, Myfire, Mosquito, EU-China IoT
Raffaele Giaffreda, IT, create-net, iCore
Richard Egan, UK, TRT
Rolf Weber, CH, UZH
Sébastien Boissseau, FR, CEA-Leti
Stephan Haller, CH, SAP, CoBIS
Srdjan Krco, RS, Ericsson, IoT-I
Sönke Nommensen, DE, UZL, SmartSantander
Trevor Peirce, BE, CASAGRAS2
Vincent Berg, FR, CEA-Leti
Vlasios Tsiatsis, SE, EAB
Wang Wenfeng, CN, CESI/MIIT, CASAGRAS
W. König, DE, ALUD
W. Templ, DE, ALUD
Zsolt Kemeny, HU, Hungarian Academy of Sciences, TraSer

Contributing Projects and Initiatives

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

Introduction to the CASAGRAS Inclusive Model

By Professor Anthony Furness

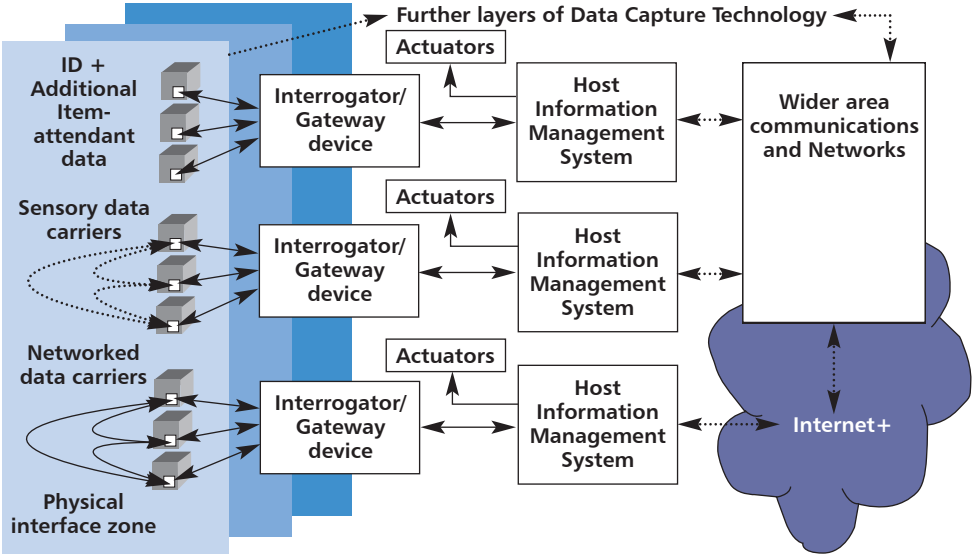
While models for the Internet of Things (IoT) have been suggested that are simply based upon radio frequency identification (RFID) and other radio-based edge technologies, a more inclusive model is necessary to accommodate and exploit the extreme potential for interfacing and interacting with the physical world. It is also important as a vehicle for accommodating the inevitable vagaries in networks and connectivity that are likely to arise in realising practical, scalable systems.

While the inclusive model is more demanding in its outlook and realisation it is a vision that can be approached in a migratory, progressive, standards-supported manner. The framework presented by the CASAGRAS inclusive model distinguishes the various layers of structure and connectivity that can be seen to exist between the real world objects and their virtual counterparts, information management structures and networks, including the existing and evolving Internet. The essential elements are presented opposite.

The structure comprises:

Physical layers – in which the physical objects or 'things' are identified and rendered functional components of the IoT through the use of object-connected data carrier technologies, including RFID. The objects so identified may also be grouped or networked to fulfil particular application needs. Devices with additional functionality, in the form of sensory, location, global positioning and local communications capabilities, may be used to achieve network structures as well as single-device operation. Processing capability is an important distinguishing feature in the devices constituting nodes within the IoT. With developments in processing power and reductions in cost and size an increasing percentage of object-based applications may be expected to exploit embedded or attached processing nodes. The range and flexibility of these devices and networks will clearly have an important bearing on the range of applications.

Schematic summary of the CASAGRAS Inclusive Model



Note: Sensor-RFID structures may be distinguished that (1) allow communication simply with host readers and (2) between sensor devices (dotted lines).

The European Commission (2006) report, 'From RFID to the Internet of Things – Pervasive Networked Systems,'[1] identified the following network-supporting communication devices that parallel the object-connected technology depiction for the physical layer:

- Purely passive devices (RFID) that yield fixed data output when queried
- Devices with moderate processing power to format carrier messages, with the capability to vary content with respect to time and place
- Sensing devices that are capable of generating and communicating information about environment or item status when queried
- Devices with enhanced processing capability that facilitate decisions to communicate between devices without human intervention – introducing a degree of intelligence into networked systems

These categories of technology clearly present implications with respect to the physical zone interfacing and networking requirements. They also have ramifications with respect to other parts of the data transfer and processing chain and data structuring needs. The ISO/IEC Standards-developing communities have, and are continuing to develop international standards to meet these needs. The following illustrates the ISO/IEC developments with respect to various interfaces and functions, including sensors for RFID.

Also important within the physical layers are the structures, such as electro and electro-mechanical devices (phones, displays, printers, and access barriers), for achieving activation (depicted as actuators in the schematic) and other feedback functions - an integral part of many real-world applications.

Interrogator-Gateway Layer – providing effectively the interfaces between the object-connected devices and between the interrogator and the information management systems. Fixed, broadband and mobility communication technologies that will yield the connectivity required for the IoT. Networking of interrogators and gateway devices may also be seen as an important infrastructural feature in this layer and an important contributory feature within the IoT. Interfacing with respect to actuation and control devices within real-world applications is a further important feature of this layer.

Information Management, Application and Enterprise Layer – Interfacing with the interrogator-gateway layer, the information management layer provides the functional platform for supporting applications and services. Networking and the facility to provide intelligent capability (in accordance with state-of-the-art developments) constitutes further important features in realising an IoT.

Wider communications and Internet Layer – Providing the interface with other structures and networks including the Internet.

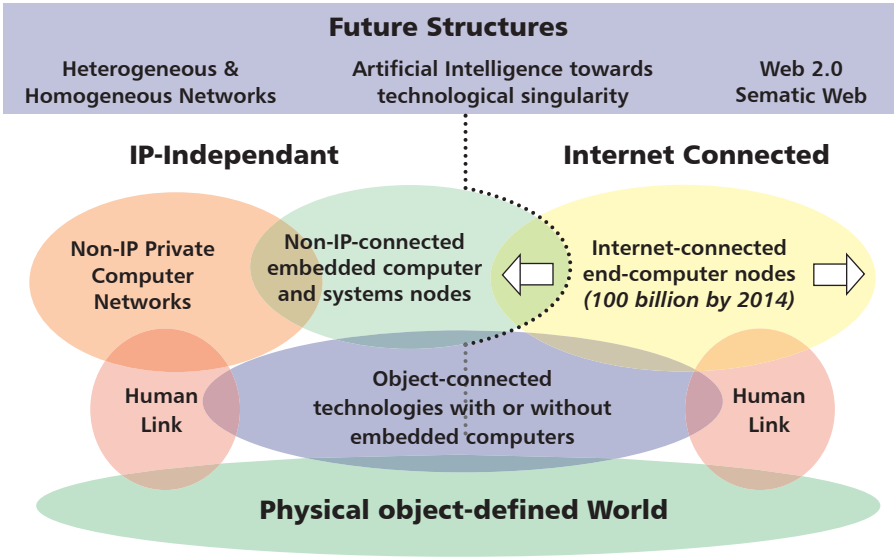
While interfaces are distinguished between each layer, interfacing may also bypass layers, adding still further flexibility and options for object-connected applications and services.

Net-borne, as well as those requiring gateway support, can thus be distinguished. Moreover, the developments in ubiquitous computing and networking, with integral communication capability, provides the key

technological foundation for an Internet of Things infrastructure and its integration within the existing and evolving Internet.

While the Internet is taken as an imperative for IoT development, what emerges from the consideration of the Internet together with the imperative for physical world interfacing and interaction, is a prospect for both Internet and Internet-independent (or IP-independent) IoT developments. It has also raised the prospect of what may be described as Latent IoT developments, developments that initially have no link with Internet or IP-independent network of network structures, but could well be linked in some way at a future date. Many automatic identification and data capture (AIDC) applications fit into this category of structure, including prospective Internet protocol (IP) and IP-independent supervisory control and data acquisition (SCADA) systems.

The schematic below represents the holistic tri-state structure proposed through CASAGRAS2 for the IoT.



In terms of the original CASAGRAS1 inclusive model the CASAGRAS2 extension can be effectively viewed as layered structures that access and exploit either the Internet (IP-based) or IP-independent structures, or both.

Both aspects of the model are generic in nature and present scope for the development of the IoT concept.

Further delineation of layers and structures can be effected to achieve more detail of consideration, including functionality and application specific factors.

Delineation of layers

In considering further the delineation of layers it is possible, in a systematic manner, to distinguish the various areas of enabling technologies and associated standards, including gaps in relation to standards and regulations. Still further delineation can take it to the levels of layering exemplified, but not constrained by the Open Systems Interconnection (OSI) standard, for all the enabling technologies, including the physical edge, object-connected technologies. Together with associated data and communication protocols this constitutes a framework for design and systems development. In this respect it is also important within such a framework to provide a guide to standards interpretation and use.

The design perspective extends to applications and services and the prospective structures for supporting such developments.

A further dimension to delineation relates to governance and the needs to address both directly and indirectly details relating to the overarching framework. Many of these aspects of delineation, including those relating to governance can be found in this book. The nature and complexity of the IoT development point to still more delineation and roadmaps for both research and development.

Reference

1. European Commission (2006) From RFID to the Internet of Things – Pervasive networked systems ISBN: 92-79-01941.

Professor Furness is the Technical Coordinator of CASAGRAS2
anthony.furness@btconnect.com

The Technological Fabric of the Internet of Things

By Alessandro Bassi

Architecture

The technological domain of the Internet of Things (IoT) embraces several developments, which are generally disjointed, as they belong to totally different environments. Being completely separated, they do not necessarily converge. Furthermore, as the definition of IoT itself is still under heavy discussion, it is quite difficult, if not impossible, to set precise boundaries in order to determine clearly which technologies are within the IoT range, and which are clearly excluded.

Considering, for the sake of brevity, that IoT is built by "interconnected smart objects", we can orientate our interest more towards communication technologies, developing the way this connection is established, or else consider the "smart object" perspective, in which for instance, developments related to energy harvesting and conservation, as well as the miniaturisation of printed circuits, and inclusion of transistors into commonly used materials such as plastic, wood or metals are of central importance.

Foundation

Starting at the service level and moving through to the devices, we find today a wide range of technologies which claim to use the "IoT" label.

Regarding architectures, several public funded projects, especially in the EU, have attempted to set common reference models and/or architectures. The EU project IoT-A has produced a publicly available deliverable highlighting in details the IoT state of the art (IoT-A, 2011).

In general, for IoT Architecture we mean an integration of heterogeneous wireless sensor and actuator networks (WS&AN) into a common framework of global scale and made available to services and applications via universal service interfaces. The EU project SENSEI aims to create an open, business driven architecture addressing the scalability problems for a large number of globally distributed WS&AN devices.

To enable RFID and EPCGlobal standard solutions in practice, technical, social and educational constraints - particularly in the area of security must be overcome. BRIDGE (Building Radio Frequency Identification solutions for the Global Environment) addresses these problems by extending the EPC network architecture (Bridge, 2011). This is done by researching, developing and implementing tools that will enable the deployment of EPCGlobal applications in Europe. The enablement is mostly in the development of security apparatus, both in hardware, software and business practices.

The Cross Ubiquitous Platform (CUBIQ) project aims to develop a common platform that facilitates the development of context-aware applications (CUBIQ 2010). The idea is to provide an integrated platform that offers unified data access, processing and service federation on top of existing, heterogeneous ubiquitous services.

The CUBIQ architecture consists of three layers:

- a data resource layer,
- an intra-context processing layer and
- an inter-context processing layer.

The data resource layer provides transparent data access and handles mobility, migration, replication, concurrency, faults and persistency. The intra-context layer provides data processing services. The inter-context processing layer is responsible for service composition. The CUBIQ architecture provides interfaces for each layer. (Dempo, 2010)

Beside the results coming from these research efforts, there are several architectures currently used in a number of commercial products. Zigbee developed by the Zigbee Alliance is probably the most popular one. It is a simpler, more scalable alternative to Bluetooth. (Ashton, 2009)

WirelessHART, an extension of the popular HART (Highway Addressable Remote Transducer) communication technology, provides several features such as security and robustness, but provides no interoperability with other communication technologies because of its single-purpose philosophy (Mindtech, 2009; Song, 2008).

Sun SPOTs are a platform from Sun Microsystems for the development of sensor networks and embedded systems. Sun SPOT is an acronym that stands for Sun Small Programmable Object Technology (Sunspot, 2010).

Representational state transfer (REST) is a coordinated set of architectural constraints that attempt to minimize latency and network

communications, while at the same time maximizing the independence and scalability of component implementations. This is achieved by placing constraints on connector semantics, where other styles have focused on component semantics (Fielding, 2000). REST enables the caching and re-use of interactions, dynamic substitutability of components, and processing of actions by intermediaries, in order to meet the needs of an Internet-scale distributed hypermedia system. REST elaborates only those portions of the architecture that are considered essential for Internet-scale distributed hypermedia interaction.

Communication protocols

Regarding communication protocols, several solutions have been developed to overcome the limitations of current network technologies. Stream Control Transmission Protocol (SCTP) is an IETF proposed standard protocol for the transport layer. It is designed to eventually replace TCP and perhaps also UDP (Stewart, 2000). Like TCP, SCTP is reliable but offers new features such as multi-streaming and multi-homing. In particular, the multi-homing feature of SCTP enables it to be used for mobility support, without any special router agents in the network. Other features included in SCTP are error-free and non-duplicated data transfer, network-level fault tolerance through supporting of multi-homing, and resistance to flooding or masquerade attacks.

The Host Identity Protocol (HIP) is a solution that locates the mobility between the network and transport layers (Moskowitz, 2006). HIP introduces a new Host Identity layer (layer 3.5) between the IP layer (layer 3) and the upper layers. The reason for this is to avoid the situation where binding sockets to IP addresses forces the address into a dual role of endpoint and forwarding identifier. In HIP, upper layer sockets are bound to Host Identities (HI, identifiers) instead of IP addresses. In addition, the binding of these host identities to IP addresses (the locators) is done dynamically. The purpose of HI is to support trust between systems, enhance mobility, and greatly reduce the Denial-of-Service (DoS) attacks.

The Mobile IP protocol is an IETF proposed standard that provides a network layer solution to node mobility across IPv4 (Mobile IPv4, Perkins, 2002) and IPv6 networks (Mobile IPv6, Johnson, 2004). Mobile IP allows a node to change its point of attachment to the Internet without needing to change its IP address.

This is not simply a configuration simplification, but can facilitate continuous application-level connectivity as the node moves from point to point.

Using Mobile IP, it is possible to move a single IP device from point to point on the Internet without losing higher level connections. However, with the proliferation of IP and the desire to always remain connected to the Internet, we are seeing entire networks of IP devices moving together from one place to another. It is possible to enable mobility for all of these devices using standard Mobile IP; however, this would require all devices to be capable of Mobile IP and generate excess overhead as every device would have to perform Mobile IP functions.

Another solution to the problem is Network Mobility (NEMO) that works by moving the mobility functionality from Mobile IP mobile nodes to a moving network's router (Devarapalli, 2005). The router is able to change its attachment point to the Internet in a manner that is transparent to attached nodes. NEMO is an extension of Mobile IP that enables an entire network to change its attachment point to the Internet.

IoT domain

In the IoT domain, smart objects and services exploiting them are distributed globally. Thus, there must be some kind of identification and resolution infrastructure to discover and lookup the services that allow accessing information about smart objects as well as controlling them. Resource Identification can essentially encompass both the naming and addressing of a resource, or either of them. In the Web, the identification of a resource that represents some form of information has been achieved by the development of the "Universal Resource Identifier" (URI) [W3, 2004], which is a global agreement on the identification of a particular resource based on specified schemes. In IoT, similar to the Internet and the Web, objects and resources need to have common naming and addressing schemes and also discovery services to enable global reference and access to them.

In SENSEI the resource ID is formed through a concatenation of several parameters; the domain of resource's provider, the type of device, a name representative of the resource's function, and a unique identifier that differentiates the resource from others of the same device type (Much-Ellingsen, 2011). In the Ubiquitous ID (uID) framework identification is

represented by the "ucode", which is a unique identifier for either physical or logical entities. The ucode itself is a 128-bit number that has no relationship to what it represents, but rather the relationship is retrieved from dedicated database servers. The structure of the uCode is formed in a manner to support its management (uID, 2011).

In the field of RFIDs, EPCglobal have promoted the adoption and standardization of Electronic Product Code (EPC), which has been used as a means of uniquely identifying RFID tags (EPCglobal, 2005). It is based on the URI model. ID@URI developed by the DIALOG research project and is another identification model that takes the same properties of the EPC/ONS standard but can also be manifested in barcodes as well (Dialog, 2011).

The Internet in the Internet of Things

Whatever the perspective, however, there is a need for substantial progress in research achievements in several fields. Firstly, today there is no single way of identifying an object in the internet of things: there are several standards, such as 2-D bar codes, GS1, uID, IPv6 addresses, but they are non-compatible. Moreover, reference architectures which can lead the way to any kind of real-life system implementation must be identified and standardised. In addition, security mechanisms should ensure reasonable safety and privacy properties. Communication protocols, from physical layer to interfaces with services and applications, need substantial advances in order to leverage any future IoT vision. These are just a few examples of areas of research that need substantial development in the coming five to 10 years.

Within the "interne" side of IoT, which is dealing with communication between objects, there is a need to develop a convergence between different communication means. Today, several communication mechanisms, as shown in the table opposite, are deployed in current applications, and any novel technologies will need to guarantee interoperability between different protocols.

We must also consider that the lifetime of network technologies might be much shorter than the one of the physical objects connected to it, and where that same technology is applied. In the "common" internet, the interoperability between low-layer technology and services is assured by the

Physical Communication Interface Type	Communication Type	Protocols	OSI Layers
802.15.X series (Zigbee,Bluetooth, RFID, etc)	Wireless Wireless	NWK/APS/API defined by each standardisation body (all non-IP)	Network Transport upper
WIFI	Wireless	IP-TCP/UDP	Network Transport upper
UWB	Wireless	Baseband/LinkManager/L2CAP (non-IP)	Network Transport upper
Sensor network busses (CAN, profibus, ...)	Fixed	up to data link	data link
Serial	fixed	up to data link	data link
USB	fixed, wireless	up to data link	data link
DeviceNet	fixed	DeviceNet network and transport	Network Transport upper
ControlNet	fixed	ControlNet network and transport	Network Transport upper
Ethernet/IP	fixed	IP-TCP/UDP	Network Transport upper
Power line (KNX, LonWorks)	fixed	Network/transport layers according Network layer/Transport to KNX and LonWorks specifications	Network/Transport

use of the Internet Protocol (IP). Usually, the network technologies are represented in an hourglass shape, with the IP layer in the middle, and this is commonly referred as 'the narrow waist' of internet. The questions of what shape the IoT 'narrow waist' will have - and even if such a thing will exist considering the heterogeneity of IoT technologies - are of primary importance, and future research should clearly focus on them.

Here is an example of the complexity we face. If we describe the communication layers in the classic way, we could imagine a 'thin layer', just below the service and application layers and above all the different technologies used to transfer information, as the glue of different solutions

developed for a specific target using very specific technologies. However, such a solution is clearly simplistic, as we would then need high-level gateways between different technology silos, and this would not make any sense not only from the technological point of view, but first and foremost from the economical point of view.

Security issues

Regarding security issues of communicating objects, a significant research effort has been undertaken on cryptography tailored for low-cost, low-throughput, and resource-cons\-traint devices. This domain has been referred to as "light-weight cryptography", and has produced a number of new protocols that have been proposed for small devices, such as RFID tags (Internet Security Group, 2011). In spite of the large number of available methods, there are very few which have been examined enough to be considered safe.

In the past years, a few light cryptography algorithms that have been widely deployed were proven vulnerable such as, for instance, the well known case of MiFare Crypto-1 [Garcia, 2008]. The development of light cryptography standards is paramount for the wide-spread adoption of IoT technologies.

In addition, the combination of lightweight cryptography protocols for use with light duty devices and a regular cryptography framework such as Public Key Infrastructure (PKI) for back-end infrastructures should be analyzed. A very important consideration in this is key management: such a holistic framework should identify the actors generating the encryption keys, in case of private/public keys schemes, how these will be distributed and who (which agencies/companies/authorities) will eventually be given access to such keys when necessary.

Breaking the Unbreakable: The End-to-End Principle

The internet as we know it today is based on a few, very simple and very meaningful principles. One of these is the "end-to-end" principle: keeping the technologies in the network very simple and dealing with complexity at the end points only, allowing the Internet architecture to be very scalable (Carpenter, 1996).

With regards to the IoT domain, there might be a different point of view. It has to be considered up to what extent IP technology will be used. While many technologists believe that IP will finally be on each and every smart device there are two particular cases which show the likeliness that different

solutions are necessary. Firstly, real-time devices, such as the braking systems in cars, which cannot be based on the best-effort, connectionless, unreliable protocol (as the IP is, by definition) (Ipso, 2011). Secondly, tiny, extremely cheap devices, (such as passive RFID tags) which may be stateless, and therefore cannot use complex protocols such as IP.

Moreover, it is questionable if the end-to-end principle can (and will) be used in the IoT domain. As the end points of IoT can be extremely simple (as a temperature sensor), even if they will be able to use the IP protocol it is unlikely that they will be able to deal with complexity. Moreover, smart devices do not necessarily need to speak the same language: a medical device such as a Nano robot used to fight cancer cells in the human body has totally different needs than those of a smart fabric needing to communicate its characteristics to a washing machine. Therefore, it is likely that, at some layer, there will be bridges between systems; and these bridges (or gateways) might be considered the end-to-end points between communicating entities. In other words, between two different objects communicating, the communication path may be broken into different sections (object-to-gateway, gateway-to-gateway, and gateway-to-object). As this is considered a "curse" in today's internet, and is likely to be a highly controversial topic, there is a strong need to further investigate this matter, and to come up with a commonly accepted set of founding principles.

The things in the Internet of Things

With regard to smart objects, there seem to be a few main research axes to be developed: energy harvesting and conservation, integration of smart components into materials, and the combination and integration of different subsystems into more complex and complete systems (also called more-than-moore).

So far as energy is concerned, in all its phases of harvesting, conservation and consumption, there is a need to develop solutions with the objective of developing a level of entropy as close as possible to zero. In other words, all ambient energy should be gathered, should be stored without any loss, and should be used as efficiently as possible.

Common objects, such as mobile phones, should be able to harvest the energy they need, whether by photo-voltaic cells, transforming the vibrations and motion into electric energy, or suing differences in temperature and humidity. Current technology development is inadequate in this respect and existing processing power and energy capacity is too low

to cope with future needs. The development of new and more efficient and compact energy storage sources such as batteries, fuel cells, and printed/polymer batteries, as well as new energy generation devices coupling energy transmission methods or energy harvesting using energy conversion, will be the key factors for the roll out of autonomous wireless smart systems, which will be the backbone of any conceivable IoT architecture.

Second direction developments

The second direction of technological development in the area of smart objects, however, is one step further. The integration of chips and antennas into non-standard substrates, such as textiles and paper, will become mainstream technologies in the coming years. Metal laminates and new substrates based on polymer with conducting paths and bonding materials, better adapted to harsh environments and environmentally friendly disposal will become as commonplace as silicon is today. RFID inlays will be used to connect the integrated circuit chip and antenna in order to produce a variety of shapes and sizes of labels, instead of direct mounting.

Inductive or capacitive coupling of specifically designed strap-like antennas will avoid galvanic interconnection and thus increase reliability and allow even faster production processes. The target must be to physically integrate the RFID structure with the material of the object to be identified, in such a way as to enable the object to physically act as the antenna.

Looking back a few years there was a huge hype in polymer RFID prototyping, with companies such as PolyIC [PolyIC, 2004]and Philips [Philips, 2006] demonstrating fully polymer RFID tags. In parallel, silicon ultra-thin structures, such as the Hitachi mu-chip [Hitachi, 2007] need to be developed, with regards not only to further miniaturisation, but especially to resistance to harsh environments and packaging, in order to be included in commonly used objects.

Furthermore, the integration of different capabilities in the same chipset will provide subsystems able to provide not only basic information, but also process that information and provide ambient knowledge to higher-level services. Subsystems able to sense the environment using the observation of physical properties are under study [Nikitin, 2009], and can provide very interesting results. As well, the miniaturisation of accelerometers, magnetometers and temperature sensors can provide any smart object the possibility of understanding its own movements and its position.


From Identification to Discovery

By Paul Chartier and George Roussos

Abstract

A lot of material has been published about the Internet of Things, ranging from high level and generally abstract architecture models to a view of future applications. As the CAGAGRAS2 project comes to an end after two years, it has been able to build on the previous two years in the initial CASAGRAS project. Also as co-ordination projects, there is a basic requirement to focus on what "is" and then consider developments and extrapolations from existing points. The two CASAGRAS projects have always considered that support for legacy identification systems is critical for the rapid adoption of the IoT.

This section of our book provides a status report, as of mid-2012, of the current position.

Section 1 provides some background into two main classes of Things for the IoT: things, effectively devices, that have processing capability and things that require some form of more automated identification.

In Section 2 we describe the objectives of CASAGRAS2 Work Package 3 UII and Data Capture Protocols.

Section 3 describes the current perspective of the IERC Activity Chain "AC02-Naming, addressing, search, discovery". While we use this perspective as a reference,

in Section 4 we propose that the communication layers need to be sub-divided, and propose nine layers.

Section 5 shows the outcome of our work on a framework model for edge data capture technologies linking to the Internet of Things.

Section 6 considers in some detail four identifier schemes using the 9-layer model as a common structure (but skipping some obvious layers).

We show our conclusions in Section 7.

1. Introduction

Our goal is to provide an overview of the work carried out in the CASAGRAS2 project under Work Package 3 UII and Data Capture Protocols. The work builds on previous work undertaken in the first CASAGRAS project, but as that was mainly focused on Radio Frequency Identification (RFID) technologies, the current work expands to other edge data carrier technologies.

There is a need to distinguish between two main classes of Things for the Internet of Things:

- Smart things that have some on-board processing, generally considered as associated with M2M, sensor networks, ubiquitous computing and so forth. Some experts view that this, and only this, is the Internet of Things.
- Things, potentially including humans, that have to achieve their connectivity by some means of data carrier such as an RFID tag, 2-dimensional symbol, or other data carriers.

The CASAGRAS2 perspective is that both classes are important and essential to a comprehensive appreciation of the potential of the Internet of Things. This chapter will focus on data carriers and the IoT, because that is the main scope of the Work Package. However, both are important. Here is an abstract from the opening paragraph of a European Commission Your Voice survey undertaken in 2012:

> The next evolution will make it possible to access information related to our physical environment, through a generalised connectivity of everyday objects. A car may be able to report the status of its various subsystems using communicating embedded sensors for remote diagnosis and maintenance; home information about the status of the doors, shutters, and content of the fridge may be delivered to distant smart phones; personal devices may deliver to a central location the latest status of healthcare information of remotely cared patients; environmental data may be collected and processed globally for real time decision making.[1]

Whereas many of these examples are in the class of smart devices, the fridge will have no knowledge of its content unless it has some means of data capture of its contents and they have some means of identification and

translation into a humanly understandable context. The same applies to product distribution, use, consumption, and recalls.

An on-board sensor might detect a problem in a vehicle but unless the problem is self-healing there will be a requirement for some form of physical maintenance ensuring that the right part is fitted using the correct procedures. In today's robot-dominated automobile assembly lines, piece parts require the use of identification technologies that are 40 years old. Even the latest developments of aircraft construction and maintenance [2] are being established based on RFID technology with some due consideration of the Internet of Things.

So a key objective is to enable all the things that are currently identified for purposes and applications that were established prior to the Internet of Things to be in a ready state for the IoT. CASAGRAS2 considers these `as IoT-latent [3] applications. The most obvious example (but far from only one) is the GS1 bar code system, evolving into the GS1 EPC RFID system, which already has structures suitable for the Internet of Things.

An often-quoted prediction is that there will be 50 billion things on the Internet by 2020.[4] But put this in perspective with more basic things. A few years ago GS1 claimed that there were 6 billion beeps (i.e. scans) a day.[5] This was mainly based on retail point-of-sale. Add to this all the automatic data capture of all types of items in industrial, commercial, service, and government operations.

Billions of events every day!

Based on various applications and general market share data, we estimate that this results in a total of around **20 to 25 billion automatic data capture events a day.** This might even be a conservative value. Not all will be part of the Internet of Things, but a significant minority will be. The legacy of automatic identification and data capture (AIDC) technologies, therefore, has a significant potential for the Internet of Things and cannot be ignored.

An example of the rapidly changing technological, commercial and social factors can be seen in the changes in the use of QR Code. It is a two-dimensional (2D) bar code symbology, originally developed by Denso Wave, for industrial applications including the automotive sector in Japan. QR stands for Quick Response, another name for just-in-time production techniques.

QR codes have been used as a data carrier for ucode (see Section 6.5). A real explosion has taken place for the use of this symbology for promotional purposes in newspapers, magazines and billboards and apps on mobile phones are able to read the symbol and link to the Internet.

In turn, this raises two other developments that we will cover later:

- The use of bar codes as edge data capture technologies for the Internet of Things.
- The use of internet-enabled mobile devices.

2. Initial Objectives

As with all projects, the CASAGRAS2 Work Package had to begin with a key objective, as shown here:

To establish a heterogeneous framework model at the data capture edge covering:

- unique item identifier (UII) structures,
- the UII encoding in various data carriers, from within the set of standardised RFID tags, linear and 2D bar code symbologies, real-time location systems (RTLS), sensor networks, and other standardised data carriers.
- the data capture protocol that might be used between the data carrier and the data capture device,
- the application communications protocol from the data capture device to other systems.

Initially this was seen as a layered model, effectively based on these four bullet points, but as the project developed, greater layers of complexity emerged, challenging details of every aspect except the need for the fundamental need for a heterogeneous framework. This was a conclusion from the first CASAGRAS project, and what has been identified in the current project is even greater diversity, not less.

Implicated in this framework under "the application communications protocol from the data capture device to other systems" is the requirement to communicate with the Internet.

The final report of the initial CASAGRAS project contained a SWOT analysis [6] of the way that the various identifier schemes were capable of being used for the Internet of Things.

A second objective was:

> To catalogue and analyse the current and emerging proposals for object naming schemes, using the results of the first CASAGRAS project as a base, to produce each object naming scheme's specific model within the data capture edge framework

A key point to understand with a ***heterogeneous framework*** is the fundamental fact that there will be differences. Our view is that these are best expressed upon the foundation of an established, or developing, object naming scheme. This is because the object naming scheme will have at least one of the following characteristics essential for the rapid introduction of the Internet of Things:

- one or more established IoT-latent applications that will extend existing functionality to adopt services that will evolve with the introduction of the Internet of Things
- an object naming scheme that has a structure suitable for being resolved in the classic manner of a URL
- a potential service associated with the Internet of Things

Another objective was:

- To analyse:
- The capabilities of emerging proposals against the comprehensive four-layer framework model described
- Identify various strengths and weaknesses

In subsequent sections we explore a set of major object naming schemes, updating as necessary the analysis carried out and reported in the first CASAGRAS project. We show various models, first at a high level, and then in more detail for each of the object naming schemes. We also extend and update the SWOT analysis to provide a current status of developments.

3. IERC Activity Chain "AC02 - Naming, addressing,search, discovery" Perspective

The lead project responsible for delivering the Activity Chain is OPENIOT. The projects Involved in the Activity Chain are:

OpenIoT	Open Source Solution for the Internet of Things into the Cloud
IOT-A	Internet of Things Architecture
EBBITS	Enabling the Business-Based Internet of Things and Services
IoT@Work	Internet of Things at Work
SPRINT	Software Platform For Integration Of Engineering And Things
CASAGRAS2	Coordination and Support Action for Global RFID-related Activities and Standardisation – 2

With the exception of CASAGRAS2, which ends in June 2012, the other projects extend to 2013 and even 2014. This means that the cluster can take a longer-term perspective than CASAGRAS2 in reaching its conclusions. In addition, some of the other projects have a different brief from CASAGRAS2, with more of a focus on M2M and less on physical things with attached data carriers that make them IoT-latent technologies and applications.

This is an abridged abstract of the scope and objective of the activity chain:

> The main objective of the activity chain (AC2) of the IERC is to explore naming and addressing schemes, which will be used in the scope of open loop multi-domain highly distributed and massively scaleable applications involving internet-connected objects. Along with these schemes, AC2 will provide accompanying search and discovery mechanisms for resolving internet-connected objects, including services for discovering their capabilities.
>
> The main challenge for the AC2 stems from the number, dynamism and heterogeneity of the devices, services and application domains that comprise an internet-of-things environment.

These devices and services come with a number of readily available (and in most cases mature) addressing schemes and search/ discovery mechanisms, which are not however always compatible and interoperable. As a result, AC2 will have to deal with:

- multiple addressing technologies
- naming technologies
- naming/addressing resolution technologies
- directory services
- service discovery

Furthermore, a number of semantic schemes (e.g., based on the W3C SSN ontologies) should be also studied.

Because the W3C semantic sensor network, and directory services, and service discovery are typically associated with M2M systems, they are not covered in this chapter. Instead, we focus on the naming technologies, some of the addressing technologies, and the resolution technologies associated with particular naming technologies. In Section 4, we use names for functions that are more familiar with the types of application that are associated with object naming or identification schemes and their potential resolution over the internet and Internet of Things.

4.The CASAGRAS2 Communication Layers

Using the IERC AC2 functions, but extending these downwards to data carriers and encoded UIIs, it is possible to identify nine layers associated with the communication from the identifier to its associated discovery services. This is illustrated in Figure 1.

Not all the layers are necessary for each of the identifier and object naming schemes we have studied. Also, some that are considered necessary for providing IoT services based on a particular item identifier scheme are not yet in place.

In other words, these are areas that need to be addressed to make the identifier schemes part of the Internet of Things.

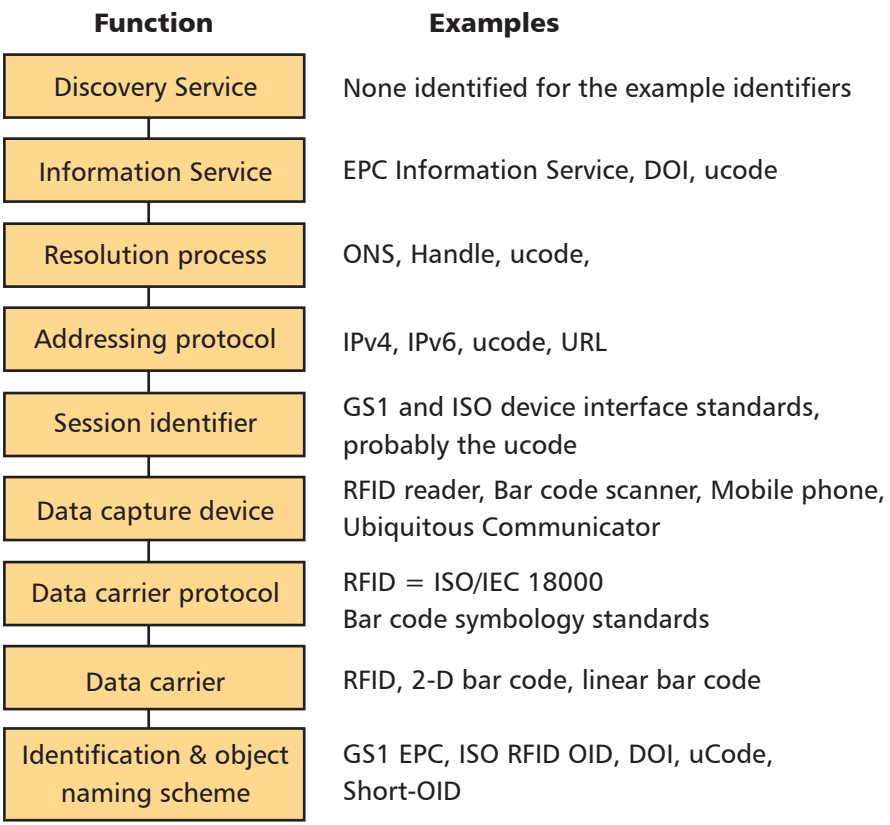


Figure 1: The Identifier to IoT Communication Layers

Figure 1 shows examples for each of the layers in the schemes that we explore in Section 6. The descriptions for functions at each of the layers, starting from the lowest level, are as follows:

Identification and object naming scheme - this refers to any of the established identifier schemes that either have very large-scale implementations and/or a structure that is already suitable for resolving.

Data carrier – this applies to any technology that has the capability of encoding an identifier, which is used in a recognised manner to identify the object (or thing) to which it is attached.

Data carrier protocol – the means of communication between the data capture device and the data carrier

Data capture device – a device with processing capabilities that is used to control and communicate with the data carrier and also communicate with higher layers.

Session identifier – an identifier of a packet or message, containing the basic identifier plus additional attribute data or sensor data, for communicating to upper layers within the enterprise or internet.

Addressing protocol – the addressing mechanism used by the data capture device over its network (e.g. an IP address).

Resolution process – the process of converting the identifier to establish a URI where more information can be located about the specific identifier that is submitted.

Information service – a repository of additional data associated with a specific item identifier. The information service does not need to contain all the information relating to a specific ID and, insome cases, different information services are context related.

Discovery service – a process, or protocol, to link different information services to create a more comprehensive knowledgebase about an object. This could be different attributes based on the context, or based on a time line for track and trace.

(Note: not to be confused with service discovery, generally applied to wireless devices when identifying basic functionality when a communication is established.)

5. The Framework models

5.1 Basic and generic model

Bearing in mind that the research in Work Package 3 of CASAGRAS2 is focussed on things that are made identifiable by attaching a data carrier to them, then Figure 2 represents a generally acceptable framework for processing such an object.

In this framework there can be various combinations of encoded unique item identifier (UII) and data carrier. However not all UIIs are capable of being encoded in a particular data carrier. This can be constrained by the rules and procedures associated with a particular application domain.

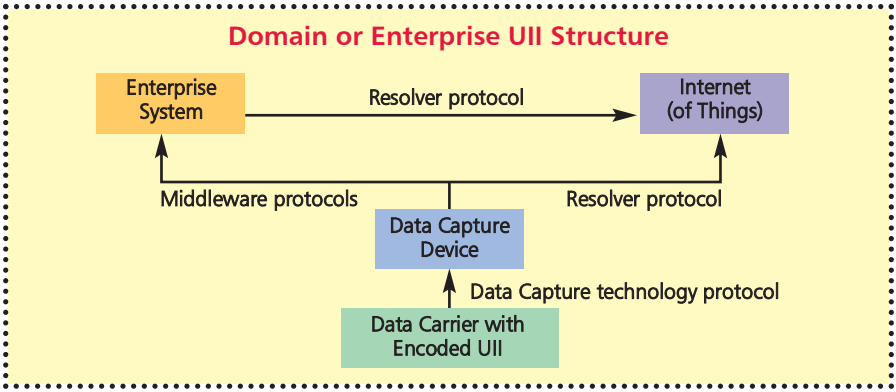


Figure 2: The Basic and Generic Framework

For example, UIIs based on the GS1 EPC standards may only be encoded in two types of RFID data carrier, and this was only extended from one data carrier within the past year. Another constraint can be imposed by a combination of application and data carrier technology. An example that illustrates this case is that of Near Field Communication (NFC), where particular encoding rules and a specified data capture technology protocol have to be used, which in turn restricts the choice of data carrier.

5.2 Data Carrier Issues

The relationship between the data carrier, data capture device, and technology protocol varies based on the technology being used. As examples, we consider two major technologies with respect to the lower two blocks in the framework: RFID and bar code.

For RFID, what is known as the air interface protocol is standardised and the data carrier and data capture device are built to comply with the standardised protocol. A mandatory feature of an air interface protocol is the frequency at which it operates. However each air interface protocol has a number of optional features, and even permits custom features. Thus, the variety of "compliant" data carrier products and data capture devices can be quite extensive. The rapid growth of the technology – still way behind bar code in market penetration – has also resulted in a number of editions of the air interface protocols over a very few years. The impact of product manufacturers choosing to include or exclude some optional features, plus the fact that products may comply to earlier and recent

editions of a protocol standard can result in available features not being used in some sector applications and certainly in individual implementations of the technology. An example of this is the memory capacity for the UII for the GS1 EPC applications [7] The standard has always supported a fairly large UII, but because the original EPC code was predicated on a 96-bit value, the vast majority of tags can only support that length of UII string. Other applications, even within the GS1 EPC domain require UII values up to 202 bits in length [8] The evolutionary changes to the ISO/IEC 18000-6 Type C air interface protocol standard also mean that the memory assigned for the encoded UII can signal different functionality supported by the RFID tag. An example of this is that there are now tags on the market that support sensor functions, which can be identified when the UII is read.

As RFID has now developed to a point where the vast majority of the technology on the market is read-write, the data capture device also acts as an encoder. Interestingly, the air interface protocols are only concerned with encoded bits and the semantics of the UII have to be specified in other standards like the GS1 EPC Tag Data Standard or ISO/IEC 15962.

RFID is perceived by some as the precursor to the Internet of Things, where things are physical entities. This is an abstract from the introduction to an early MIT-AUTOID Center paper :[9]

> Our vision is to create a "Smart World," that is, an intelligent infrastructure linking objects, information and people through the computer network. This new infrastructure will allow universal coordination of physical resources through remote monitoring and control by humans and machines. Our objective is to create open standards, protocols and languages to facilitate worldwide adoption of this network – forming the basis for a new "Internet of Things."

Bar code technology was once considered as legacy or 'old technology' and not even suitable for consideration as a data carrier for the Internet of Things. CASAGRAS2 takes a different view, given that the implementation of the technology is far more ubiquitous and is a much less expensive data carrier. Another early MIT-AUTOID Center paper was entitled "Towards the 5 cent Tag" ,[10] for which the world still awaits. Adding a 5-cent tag to a $1 dollar (ex-factory) price adds 5% to the cost of that item. The cost-benefit equation needs some significant benefits to justify RFID as a source-encoded data carrier.

Bar codes can be source marked, as part of the packaging, for a tiny fraction of a cent per product. Dismissing bar code from the Internet of Things will constrain the take-up of services, or restrict the IoT to those physical things where it is cost effective to apply RFID tags. We will come back to discuss bar code applications and the Internet of Things in later sections.

The vast majority of bar code technology is read only, so that the encoder (typically a printer) and data capture device are separate entities. Bar code technologies are specified by symbology standards, such as ISO/IEC 15438 for the PDF417 symbology. A symbology standard specifies the encoding rules and a reference decode algorithm. The encoding rules do impose constraints on what data can be encoded in a particular symbology, particularly those that can only support numeric data. The reference decode algorithm is generally only used for implementation in products that are used for conformance testing. Products that are used for day-to-day scanning can include features that enhance performance or produce a probabilistic decode based on some quite clever software implementations.

Scan stitching

An example is scan stitching,[11] where a set of partial but overlapping scans of a symbol are used to reconstruct, with a high probability of success, a valid decode. Apart from many product innovations that impact on performance, the rules defined in a symbology specification are generally mandatory. Where there is an option (e.g. a choice of error correction level), the scanner is expected to support all variants. This has resulted in any given symbology remaining unchanged over a long period of time. The standards are revised, but usually to improve clarification of complex points, and not to change the fundamentals of the symbology.

Many symbologies are independent of their application. In this case, there is a risk of symbols containing what is known as "other people's data" being accidentally read in a particular domain. This will be discussed in more detail in Section 6. Some symbologies, for example that used by GS1 for retail products [12] are intended to be used exclusively for a defined application. But even this symbology has been used for the sortation of fur pelts, for entry tickets to amusement parks, and even for cheating in the early public marathons that used bar codes for identifiers. Some symbologies have mechanisms that enable applications to be declared. But the risk of "other people's data" cannot be eliminated given the ubiquitous nature of the symbologies and availability of encoding devices.

The nature of applying data carrier technology to physical things is that the source encoder for RFID and the source marking for bar code is generally achieved in a physically different location from subsequent decoding. This is illustrated in Figure 3.

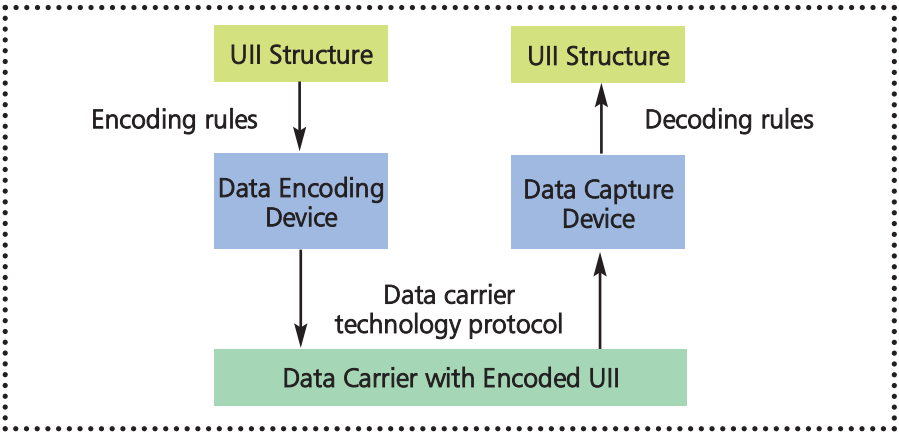


Figure 3: The Separation of the Encoding and Decoding Process

Effectively, such data carriers can be considered as relays. Not only is it the general case that the physical location for encoding and decoding are separate, but there is an ongoing space/time continuum. Data capture is either along a single continuum such as tracking a product through supply chain, or repeated cycles for returnable items such as library books or returnable plastic containers. For the Internet of Things, this means that in addition to the identifier two other attributes might need to be considered: space and time.

For bar code technology, the encoding and data capture devices are fundamentally different but the encoder still needs to correctly encode an identifier so that it can be recognised by any bar code scanner.

The permanent nature of the encoding brings with it advantages and disadvantages. The main advantage is the avoidance of accidental or deliberate changes to the encoding, and damage can be compensated in two-dimensional symbols by the use of error correcting techniques.

With RFID, the same type of device can be used for encoding and decoding, but there is still the compliance issue because there is no certainty that subsequent data capture will use the same device as used for encoding.

Because RFID tags are generally read/write, the data on the tag can change (again accidentally or deliberately), unless a process is invoked that makes part or all of the tag read-only (for example by locking memory). Many RFID technologies permit selected locking of data so that certain data elements can be permanently locked to protect the integrity of the associated thing to which it is attached, but leaving other data elements in a read/write state. This enables additional and up-to-date data to be encoded on the RFID tag at subsequent data capture points beyond the original encoding point. While this does not normally change the UII, having relevant and recent attribute data at the next data capture point is a means of distributing "downwards to the edge" aspects of the Internet of Things.

With RFID technology, it is also possible to add sensors to their basic functionality. A sensor attached to an RFID tag can continually monitor the environmental characteristics that it is designed for, and write appropriate data to memory. So at the next data capture point, environmental changes that have had an impact on the object can be captured. This adds a different analytical challenge in processing the data because the timing of sensory events and associated observations can be captured without necessarily having any information about the location at which the sensor event was captured. RFID sensor tags are obviously more expensive, and so rules are generally applied to allow the sensor to be re-configured for subsequent cycles (or missions or trips). Some tag manufacturers have already undertaken development on a disposable (one-trip) RFID sensor tag that can continue its monitoring process through the supply chain and even to the consumer.

5.3 The Middleware and the Enterprise Route to the internet (of Things)

Figure 2 shows two routes to the Internet of Things. Here we discuss the route via the enterprise. This route is a key component of the GS1 EPC system, and it is also highly relevant for many other applications and types of objects (things). Most enterprises capture information about things on input through a facility such as a factory, warehouse, store or office. This has a long business tradition of dealing with an event such as a change of state or change of ownership of the object. As examples: a pallet of goods being received into a warehouse, baggage arriving at an airport, a library

book being returned, or a tax return being received by a government department.

If the object is known or has some reference that makes it known, then subsequent procedures are based on the internal business operations of the enterprise. However, the object is not always known. Consider a new product, or an item of airline baggage arriving at the wrong airport. Then there is often no, or at least incomplete, data about such objects. There is a need to look up the missing relevant data so that the enterprise or industry sector processes can be applied. Although in the minority, such instances are commonplace and will account for a significant volume of IoT traffic, given our estimate of 20 to 25 billion daily transactions. Transferring EDI and XML messages (usually faster than the physical objects) between source and destination supports the vast majority of enterprise processing, giving advanced warning of the arrival of things. This everyday procedure by various types of enterprise provides a significant filtering process, reducing the need for the Internet of Things on every occasion. A more radical view is to consider such transactions as essential to the Internet of Things, pushing data to future points of use.

Not all businesses or operations can justify the expense of an enterprise-wide system, particularly if SMEs are to become able to implement and benefit from the Internet of Things. In future, the SME might employ the Internet of Things in some novel manners:

- As with looking up web pages currently, the SME could keep an information system that previously accessed the Internet of Things on a local cache.
- If the SME uses out-sourced data storage on the "cloud", then any resolving functions for the IoT might be transferred so that the cloud-based system actually invokes the resolving process for the IoT information.

5.4 Resolving from the Data Capture Device

There is no reason to assume that the scale of operation for using the Internet of Things cannot be extended to the micro business and even the individual. As we mentioned in the Introduction, the fridge reporting its contents to a distant smart phone held by an individual implies two different, and somewhat opposing, scale effects.

Delivering information to an individual smart phone requires the entire service to be scaled right down so that George receives the message instead of Paul. Simultaneously, it means that smart phone apps that enable such a service to be delivered will result in a large volume of data being processed from effectively random point to random point, and at random times. This is a fundamentally different concept for a manufacturer of an FMCG product providing prior notice of a delivery to a major retail warehouse using an XML message. The subject that we now discuss is the impact of data capture and accessing the Internet of Things from handheld and therefore mobile devices.

Data from the UK

Recent data for the United Kingdom[13] shows that smartphone ownership has grown from 38% of the adult population in January 2010 to 51% by January 2012. Of these owners, 54% are using their smartphones to access the Internet, with 38% having completed at least one online purchase from their phone. Statistics from another source[14] provide some global statistics:

- There are 5.9 billion mobile subscribers globally
- Feature phone sales in 2011 outnumbered smartphone sales 2:1
- There are 1.2 billion mobile web users worldwide
- By 2011, 85% of new handsets were web-enabled (i.e. this is not just smartphones)
- Over 300,000 mobile apps have been developed in 3 years, with nearly 11 billion downloads

This data is compiled from a number of sources and with slightly different time references so, rather than take the data in absolute terms, we just present it as a significant trend. At the start of the first CASAGRAS project four years ago, we were aware of the novel use of mobile phones – not necessarily smart phones – to scan two-dimensional symbols in Japan. Since then, there has been an explosion in the use of mobile phones use with 2D symbologies as a means of both data capture (because of the camera on a phone) and as a means of "printing" by using the display area to show the bar code (see Figure 4).

Figure 4: Mobile Phones used to Display and Capture Bar Codes

Organisations such as IATA have encouraged the use of 2D symbologies for electronic boarding passes, with different airlines choosing to use a particular bar code symbology. There has been a very significant growth in QR Code being used as a promotional mechanism in newspapers, magazines and billboards. In fact, there has been such a rapid implementation of bar code symbologies used with mobile phones that there is concern about the quality of some of the symbols being displayed. This has led to ISO currently developing a standard [15] to address the topic.

In another Work Package in CASAGRAS2, an interesting set of applications has been identified which presents two technological challenges:

- The first challenges whether RFID is essential for the Internet of Things because this example makes use of linear bar code technology.
- The second point challenges the need for unique serialisation as this uses a generic product code.

The applications are about providing consumers and citizens with information about ingredients of food products that should be avoided by people with food allergies. The basic principle of operation is built upon the fact that mobile phones have an in-built capability to scan bar codes so that consumers have the opportunity to use this facility to look up information about a specific product and its implications for those with specific food allergies. Various charitable organisations that focus on particular allergies have expressed an interest to make use of this technology. There are also commercial organisations that see multiple sales of low cost phone apps as a means of earning revenue. In addition, some major food companies and other organisations are also working towards providing this type of information.

There are two basic operational models:

- One model stores an entire product/allergy database on the mobile phone, leaving the user to update at a frequency of their choice. The cited advantage of this model is that the database is accessible, irrespective of the strength of the mobile phone signal and/or access that the mobile phone has to the Internet.
- The other model works in real time, providing a smaller footprint on the mobile phone, with real time access being necessary to obtain the information and with the addition of a call charge.

Examples of some of the schemes identified are: Foodwiz, IsItInIt (by an organisation called Food Angel – although there are some doubts as to whether this still exists), Nutrisleuth, and Scanavert. Each of these organisations has a commercial interest in selling the smart phone app, but has the cost implications of maintaining the database irrespective of the two operating models discussed above.

Another prototype application is being developed jointly by GS1 Australia, Deakin University, and Nestlé. The advantage of this approach is that multinational food suppliers can provide relevant information as part of the GS1 pooled data system.

In addition to food allergies, this type of application can also apply where particular foods might not be suitable for a particular health condition, for example hypertension. Similarly, the application can be applied to foods where their ingredients and processes are relevant to cultural and religious constraints.

The following components are part of the system:

- Unique Item Identifier: The GS1 EAN-13 or UPC-A code, which is only unique to the product level.
- Edge data carrier: The various GS1 retail bar code symbologies seen on products: EAN-13, EAN-8, UPC-A, UPC-E.
- Data capture: Conventional bar code scanning into a phone with a camera, or key entry of the product code.
- Internet access: Depending on the operation mode, using the browser associated with the mobile phone app to look up individual results in real time, or to periodically update the database.
- The repository: The repository is either a commercially held database or, in the case of the GS1 Australia example, the nationally held GS1 held product database.

The potential benefits of this type of application, particularly if it is customised to specific allergies or health conditions, is that it could contribute to the well-being of a population at a very low cost. Given that there are over 9 million products listed on the GS1 Global Data Synchronisation Network (GDSN) [16] and the mobile phones with cameras and web access will exceed 5 billion this year, this seems like a fairly straightforward way to accelerate the Internet of Things at a very low cost. The infrastructure of data carriers exists (even more than the current GDSN data), the data capture devices with access to the Internet exist in their billions, the GDSN forms the basis of the information system.

One of the challenges that might exist is matching the skill sets and knowledge base of particular allergy charities, self-help groups, and medical organisations with knowledge of the health condition or allergy, with access to a repository of the bar code product information.

6. Global Identifier Systems and Associated Resolver Schemes

6.1 Overview

Here we discuss various identifier systems and how they can connect to the Internet or the Internet of Things. Figure 5 illustrates a generic schematic that combines elements of the physical architecture in the flows.

Not all the identifier systems follow exactly the same schematic or have all the components yet in place. Differences will be highlighted for the systems.

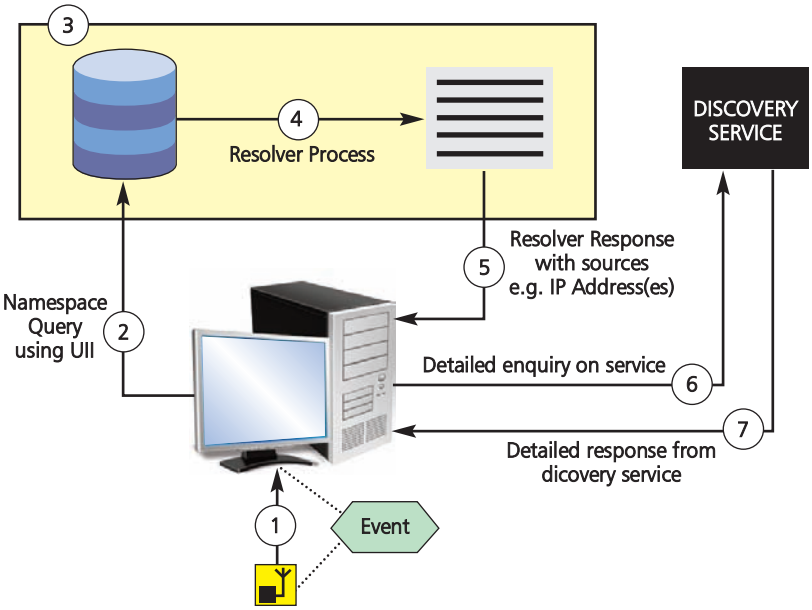


Figure 5: Schematic of a Resolution Process

If we assume that there is a unique item identifier (UII) encoded on an RFID tag, and this is associated either with a triggered event or an observed event, we can follow the process steps through the system. Although we refer to the UII being encoded on an RFID tag, this could be almost any edge-based data carrier or associated technology. Also, as we have seen in the example of using existing GS1 linear bar codes, the concept of uniqueness is context related. A triggered event could be one where an observer decides to read a particular RFID tag, say, from a poster or from a tag that might have encoded data such as a destination code or a particular batch number. An observed event in contrast could simply be the declaration of the presence of a tag as it passes along a conveyor system or, in a more sophisticated example, it declares that the sensor is in an alarm state.

Working through the steps:

1. The relevant UII is read from the RFID tag into the computer system. This is obviously an over-simplified description of the process that assumes all the processing from the interrogator through to an application that is involved with business decisions.

2. A namespace query based on the UII code is sent to a resolving system, using appropriate syntax.

3. For simplicity, in this illustration the "database" could be a network of servers that might be used in the system.

4. The resultant process could be recursive or iterative, depending on the rules of the system, but the objective is to identify a list of source addresses where the query data might be found.

5. Using appropriate syntax, the response is sent back to the enquiring device with the relevant source information. For reference, in the case of a DNS enquiry this is one or more IP addresses where the relevant data can be found.

6. Once the decision is made of which source to use, the specific detailed enquiry is placed on the information service, or discovery service (if this exists). Again, using a DNS analogy, this is requesting the specific page of the website; because it is only the website address that is identified by the resolving service.

7. Information on the response is sent back to the enquirer. In the case of a web browser, this is the image of the web page appearing on the screen.

In the remainder of this section, we will look at a number of the unique code structures that have been proposed in association with RFID, bar code and other data carrier technologies. A number of them are implemented on a reasonable scale. We shall consider features such as the process and the potential scope of such a namespace system and identify some potential constraints of the system. All of these points will be discussed at a high overview level, because a detailed analysis of each of these systems could justify a single report in its own right.

6.2 The GS1 EPC System

This was previously known as EPCglobal, but is now subsumed within the parent GS1 system. The EPC code is a recognised URN namespace on the Internet, as defined in RFC 5134. This IETF document not only describes the structure of the URN, but also outlines the resolving mechanism. The entire architecture is shown in Figure 6.

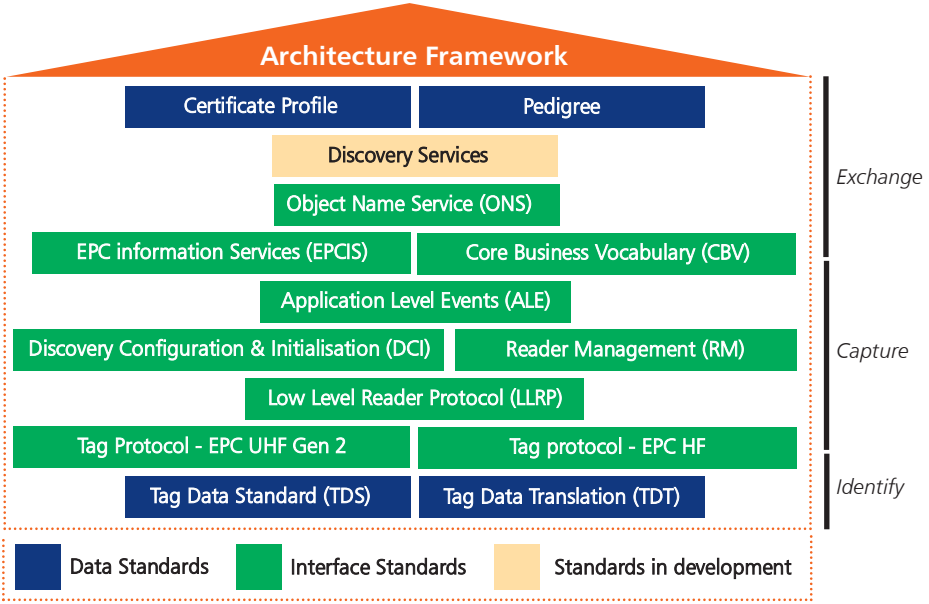


Figure 6: GS1 EPC Architecture

6.2.1 Item coding

The GS1 EPC system supports a number of code structures for unique item identifiers. A few have been specified to comply with pre-existing GS1 serialised codes, or to add serialisation to other such codes. In addition, some generic code structures are specified such as the General Identifier (GID-96) with a number of other code structures to be reserved.

The most common code structure is likely to be the Serialised Global Trade Identification Number (SGTIN), and the URN structure for this is shown below:

urn:epc:id:sgtin:900100.0003456.1234567

The three components of the numeric string represent: the company code under the GS1 system, the product code assigned by the manufacturer, and finally the serialised code. It is this code that would be presented for a resolving system.

The encoding on the RFID tag is somewhat different. The three numeric components are each encoded separately as binary values of fixed or variable length. The variable length components of the SGTIN are preceded by 14 bits. These comprise: an 8-bit header that identifies the type of EPC code (e.g. SGTIN-96), the code for logistic purposes that identifies the level of packaging, and the code which determines the relative size of the variable length components in the remainder of the code.

Conversion from the encoded 96 bits on the RFID tag, or other length (as specified by the EPC header) is dealt with by the interrogator or higher level decoding software.

The current GS1 EPC standard [17] defines the structure of 10 different codes:

- Serialized Global Trade Item Number (SGTIN)
- Serial Shipping Container Code (SSCC)
- Global Location Number With or Without Extension (SGLN)
- Global Returnable Asset Identifier (GRAI)
- Global Individual Asset Identifier (GIAI)
- Global Service Relation Number (GSRN)
- Global Document Type Identifier (GDTI)
- General Identifier (GID)
- US Department of Defense Identifier (DOD)
- Aerospace and Defense Identifier (ADI)

The inclusion of the GDTI suggests that documents are within the scope of the Internet of Things, a fact strongly endorsed by another scheme, the Digital Object Identifier (see Section 6.4).

The SSCC is also an interesting code structure, because it is identical whether encoded in an RFID tag or a bar code. However, we are not aware of IoT implementations that use the SSCC from bar code data capture.

6.2.2 Data Capture Protocol

Although the claim is that the GS1 EPC identifiers can be applied to any data capture technology, the reality is that all the focus is on RFID. Explicitly this is the RFID air interface protocol defined in ISO/IEC 18000-6 Type C, which is a UHF technology operating at 860 to 960 MHz. In September 2011, the choice of technology was extended to include ISO/IEC 18000-3 Mode 3, which operates at 13.56 MHz, a high frequency technology. No clear advice is provided about the specific use of each technology. Chip manufacturers that only produce UHF products have been arguing for years of the merits of their technology. The future is uncertain given that the physics of HF and UHF RFID are fundamentally different, in other words interoperability is not easy or inexpensive.

6.2.3 Session Identifier

The Low Level Reader Protocol (LLRP) and the equivalent and expanded ISO/IEC 24791-5 defines the interface from the RFID data capture device to the enterprise. Each message transfer has an identifier and time stamp. This function is subsumed in what are considered to be smart devices, where the device can directly access the Internet for the resolving process.

6.2.4 Addressing Protocol

There is no standardised addressing protocol for the system, but conventionally within the enterprise IP address is the use for identifying devices.

6.2.5 Resolving Process

Although RFC 5134 mentions the resolving process, this is more fully specified in the EPCglobal Object Name Service (ONS) standard. Resolving is undertaken over the company and product code information, but not the serialised component. The intention is to provide a service similar to that of the website DNS, in providing sources where further information may be obtained.

6.2.6 Information Service

To quote directly from the EPCIS standard:

> *The EPCIS specification specifies only a standard data sharing interface between applications that capture EPC-related data andthose that need access to it. It does not specify how the service operations or databases themselves should be implemented.*

As such, it provides a fundamental interface, but other components required for an Internet of Things have still to be developed. These include the GS1 EPC discovery service and some form of subscriber authentication. GS1 EPC is developing standards for both of these functions and their associated interface standards. The embryonic systems that are running at present have been built by various commercial organisations interested in providing a service to the marketplace. They will probably need to be adapted to ensure interoperability on a global basis once the GS1 EPC standards are in place.

6.2.7 SWOT Analysis

STRENGTHS	OPPORTUNITIES
The system has a potential base of all the GS1 bar code implementations An end-to-end code to discovery service system architecture	Potential rapid deployment if driven by major retailers, which has only recently begun with item-level coding of clothing
WEAKNESSES	**THREATS**
Probably restricted to the GS1 domain. Limited and uncertain RFID data carrier options at the item level, because of the introduction of RFID tags operating at 13.56 MHz	The cost of source marking an entire batch when there are few retailers using the system Privacy issues could delay take-up and render post sale IoT features redundant

6.3 ISO RFID Object Identifiers

We need to qualify what we mean by the title of this section. Object Identifiers are defined in ISO/IEC 9834-1, and within this definition can apply to a physical or logical entity that complies with the basic definition. Here, we are specifically focussing on a sub-set where the Object Identifiers comply but are registered under the ISO/IEC 15961-2 Registration Authority

rules for encoding on an RFID tag. This means that the Object Identifiers can be encoded and processed through the communication chain of a series of ISO RFID standards and can support many applications that, for various reasons, do not comply with the GS1 EPC rules. Typical applications include:

- ANSI data formats (a long established code structure used by industry similar in scope the the GS1 system)
- Industrial traceability codes such as ISO/IEC 15459 and the ISO 1736x series
- IATA baggage handling, library codes defined in ISO 28560
- ISBT codes (for blood, tissue, organ and cellular therapy products)
- Mobile phone data capture
- Even the GS1 codes themselves are standardised within this register

6.3.1 Item coding

The procedure developed for encoding unique item identifiers in RFID tags is to create a {object identifier + data} pair. The registration requires the data to be unique within the domain, and the object identifier defines that domain and the particular class of UII within the domain. As an example:

urn:oid:1.0.15961.12.1 = IATA Baggage Identification Number (BIN)
00176367789 = Unique BIN for a flight HKG – DBX - LGW

The encoding of the OID and the unique data needs to comply with one of the encoding rules of ISO/IEC 15962.

By concatenating the unique data value to the OID (effectively adding another arc to the OID structure) the {OID + data} pair becomes a code that is unique among all the ISO RFID registered domains. In addition to the IATA example cited above, a number of other domains have been pre-registered, including that for ISO traceability (ISO/IEC 15459), the library community and other pre-existing ISO OID schemes. Other domains are in the process of registering, and there is significant scope for using existing Registration Authority code structures as and when RFID is adopted.

The ISO/IEC 15459 series of standards that provide unique identifiers for traceability offers the prospect of encompassing a number of long-established encoding schemes used in the automotive, chemical, electronics and transport sectors among others.

6.3.2 Data Capture Protocol

The encoding of ISO RFID object identifiers is potentially far more extensive to that of the GS1 EPC system. Effectively, any of the ISO/IEC 18000 series air interface protocols may be used because of the way the encoding rules have been specified.

In a separate role, the co-authors of this paper have been involved with a UK-based research project that has explored the feasibility of extending the ISO RFID object identifier structures to bar code symbologies. This would be based on making the 2D symbologies a read-only emulation of an RFID tag using ISO/IEC 15962 encoding rules. This would enable the higher levels of the protocol stack to be used irrespective of whether the data was encoded in an RFID tag or a 2D symbol. A less sophisticated means of integration is one adopted by IATA, where the Baggage Identification Number can be captured irrespective of the data capture technology, and then this in itself can used as the UII of an OID structure.

The difference between the two options is that the bar code emulation of RFID encoding provides an IoT-ready OID structure, whereas the second option might be better for integrating RFID in an existing application where there is still a high proportion of bar code data capture.

6.3.3 Session Identifier

ISO/IEC 24791-5 defines the interface from the RFID data capture device to the enterprise. Currently the standard only supports the ISO/IEC 18000-6 Type C protocol, but is easily extendable to ISO/IEC 18000-3 Mode 3. The European standards committee CEN TC225 has a work item to create a device interface to support ISO/IEC 18000-3 Modes 1 and 3.

6.3.4 Addressing Protocol

There is no standardised addressing protocol for the system, but conventionally within the enterprise IP address is the use for identifying devices.

.

6.3.5 Resolving Process

The IETF RFC 3061 document clearly defines that a resolver system has yet to be defined. There is a particular challenge with respect to the URN for the ISO RFID object identifiers. If the basic Internet DNS principles are followed, eventually the route for the tree either becomes ISO, ITU or ISO/ITU

combined. This was the status as reported at the end of the initial CASAGRAS report two years ago. Since then, there have been two developments:

- The first is that ITU has unilaterally (despite using the ISO/ITU combined route) developed a resolver solution for the short OID scheme.
- Developments have taken place, initially led by the authors of this paper, for a completely different approach that links the domain as defined by the ISO/IEC 15961-2 register with the information services of that domain. We discuss this point below.

Extending beyond the UK research project (mentioned above) details of a scaleable ID/locator resolution for the IoT were published for the 2011 IEEE international conferences on the Internet of Things, and cyber, physical and social computing.[18] In that paper, we discussed the weaknesses of what we considered to be in the DNS-based approach and suggested a robust alternative based on the Handle System (see Section 6.4) and demonstrated the feasibility of this in that paper. Effectively, we proposed a three-step process:

Step 1: An OID for the UII under the ISO/IEC 15961-2 register which has appended to it a unique item identifier. Using the example in Section 6.3.1, this would result in an OID that is resolvable down to the UII as follows:

1.0.15961.12.1.00176367789

Step 2: Next the Handle system is used, with the generic structure as follows:

<Handle> ::= <Handle Prefix> "/"<Handle Suffix>

During our experimentation, we used the Handle prefix 10673, with the suffix 1, thus resulting in the concatenated Handle and OID of:

10673/1.1.0.15961.12.1.1234567890

Step 3: This is now in a structure suitable for resolving via a Handle browser or equivalent process.

The Handle **10673/1** is the one we used for experimentation. If this approach was to be implemented, the Handle prefix could either be generic and associated with the ISO/IEC 15961-2 register, or could be specific to individual registrations, for example, with different prefixes assigned to IATA and the library community. The advantage of this approach is that the ID/locator for the information service and discovery services could be specific to a particular domain. We see further flexibility in using the Handle prefix and suffix. For example, sub-domains could be created within an IATA structure that separates information services by airlines; in the automotive sector using ISO/IEC 15459 the sub-division could be to a major manufacturer. Already, the ISO/IEC 15961-2 register is in a machine-readable format so that it can be continually updated on RFID readers. All that would be necessary would be to have an expanded machine-readable table with relevant Handle prefixes and suffixes to enable a common platform for a wide variety of domains using RFID to access the Internet of Things.

One challenge that remains are claims from ITU-T that this OID structure, combined with the Handle system, cannot be used.

There are syntactical challenges in some of the legacy item identifier structures. For example the ISO/IEC 15459 traceability codes have a hierarchical structure while the IATA Baggage Identification Number has one digit position which defines attribute data. To enable these unique item identifiers to be fully resolvable, CEN TC225 has received a proposed work item to address the conversion of each of the registered legacy structures into a resolvable OID format. If this work is approved by European standards bodies the relevant specification should be available some time in 2013. Because of the "political" issues associated with the ITU-T, no resolution process will be included within the European Technical Specification.

6.3.6 Information Service

Although the Information Service does not exist, we are of the view that the proposals in our IEEE paper Scaleable ID/Locator Resolution for the IoT can form the basis for a common core resolving process to link to domain-specific information services. We claim that another advantage of this approach is that besides requiring a very small platform on the edge data capture device linking the UII directly to a common resolving process, the

information services can be very specific to a particular domain or even sub-domain. The advantage of this approach is that the very nature of the different things, as identified in the existing and expanding ISO/IEC 15961-2 register, naturally calls for different attributes to be relevant. For example, the bibliographic information associated with a library book is fundamentally different from the track-and-trace attributes of airline baggage that is, in turn, fundamentally different from attributes of blood donation products. Linking the edge data carrier identifier to a specific type of information service using a common backbone could be essential to make the Internet of Things a means of supporting heterogeneous types of thing.

6.3.7 SWOT Analysis

STRENGTHS	OPPORTUNITIES
An established code structure that can accommodate legacy systems that differ from GS1, potentially addressing significantly more objects	Has the potential to address any type of application by accepting the domains code structure of the ISO/IEC 15961-2 registration, becoming more accepted for RFID applications
WEAKNESSES	**THREATS**
There is no resolver system to address the different OID structures, although we have proposed a solution Very low level PR – there is no marketing budget for an ISO standard	Without concerted policy decisions, all these applications will function in a perfectly interoperable manner at the data capture level, by fail to expand to the Internet of Things

6.4 Digital Object Identifiers

The Digital Object Identifier (DOI) system provides a digital identifier for any object. It is not "Identifier of a Digital Object", because the object can be any entity (thing: physical, digital, or abstract). Its main and traditional use has been applied to electronic versions of technical papers and reports. The DOI is, in fact, a naming authority within the Handle system, which provides a resolving method for accessing the location(s) of the objects. This is why we considered it a suitable basis for a resolver for ISO RFID Object Identifiers, as discussed in Section 6.3.5.

Some facts of the system [19] are:

- Foundation launched to develop system in 1998. First applications launched 2000
- Currently used by well over 5,000 naming authorities (assigners) e.g., publishers, science data centres, movie studios, etc.
- Over 55 million DOI names assigned to date
- Over 210,000 DOI name prefixes (naming authorities within the DOI System)
- Around 100 million DOI resolutions per month
- DOI names have been assigned by 12 RAs (past and current)
- Initial applications are simple redirection — a persistent identifier
- More sophisticated functionality available, e.g., multiple resolution, data typing
- International Standard

In fact ISO 26324:2012 Information and documentation -- Digital object identifier system was published in April 2012, and its associated ISO Registration Authority also established.[20]

The number of DOI records far exceeds the number on the GS1 EPC ONS system, now and in the near future. It also probably has a significantly larger installed base of resolver software than will be used for the GS1 EPC system during the next few years. On this basis, it at least provides another model for comparison purposes.

6.4.1 Item coding

The DOI system has grown to be the predominant method for identifying digital media, particularly electronically available reports and papers. A typical DOI is:

10.1000/123456

The structure is as follows. The "/" separates the prefix from the suffix code. The Handle resolving process uses the prefix, whereas the suffix is used to access the content details (i.e. the information service). The prefix for the DOI [21] is sub-divided into at least two parts: the numeric code before the

first "." identifies the particular Handle application (10 identifies DOI), and the part(s) after the "." identify the registration.

Some of the other Handle applications cover sensitive defence material, and the assumption that we are making is that the Handle prefix separates applications to which different security features can be applied. In addition, the Handle system operates with proxy servers (see below) which can support resolutions for authorised users of the application.

6.4.2 Data Capture Protocol

The DOI does not specify any particular data capture protocol.

6.4.3 Session Identifier

Because there is no explicitly defined data capture protocol, there is no associated session identifier.

6.4.4 Addressing Protocol

Addressing the resolver is based on the Handle.

6.4.5 Resolving Process

The Handle system operates a completely independent server system to the DNS system, although the DNS is used for subsequent processing. At the top level of the Handle system is a Global Handle Registry, which is currently supported by multiple server sites.

As we understand the system, these sites only hold the resolution of the prefix or "naming authority Handle". So, in the example above, the global registry will identify the server holding the "10.1000" information associated with that particular registry on the DOI system.

The next level down is the local Handle server, for example for the DOI system, or specifically for any of the other Handle applications. This domain separation enables the resolver system to be scaled based on the requirements of the Handle application and for specific features such as security and specific enquiries to be domain specific.

Figure 7 shows the process for accessing a Handle identifier from a computer.

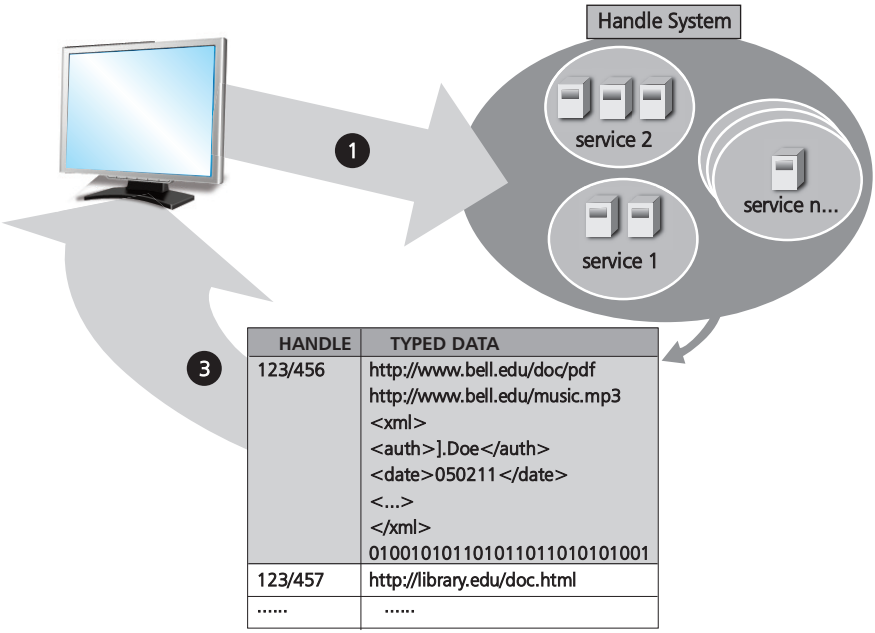


Figure 7: Handle Resolution

Here is the process, slightly simplified :[22]

1. A client such as a web browser encounters a handle, e.g. 123/456, typically as a hyperlink or other kind of reference.
2. The client sends the handle to the Handle System for resolution. The Handle System consists of a collection of local handle services. Each service consists of at least one primary site and any number of secondary sites, with each site containing any number of handle servers. Each identifier can be associated with one or more pieces of typed data.
3. In this example, the handle 123/456 is associated with, and so resolves to two URLs (it would also be possible to associate multiple instances of the same data type), and also XML and binary data.

6.4.6 Information Service

One of the key advantages cited for the Handle system, and carried through into digital object identifiers, is that the information services can be structured according to the needs of the domain defined by the Handle prefix. In the case of the DOI, this would be controlled by the sub-divided parts of the prefix (see Section 6.4.1).

An interesting application is the use of the DOI for what is known as the "actionable ISBN" (or ISBN-A).

The International Standard Book Number was established in 1968 as a 10-digit code, derived from the previous British Standard Book Number of 9 digits. In 1981, the first ISBN/EAN bar code appeared, but the two code structures remained separate, but interoperable. In January 2007, the ISBN formally converted to a 13-digit code (effectively a sub-set of the GS1 system). As such, there are now mechanisms to make it possible for the ISBN to be encoded in an RFID tag compliant with the GS1 EPC system.

The ISBN-A[23] is a DOI name derived from an existing ISBN, by including the ISBN in the syntax string of the DOI. The ISBN-A and the ISBN are used in different systems for different purposes:

- In particular, current supply chain ordering procedures use only the ISBN or ISBN-derived bar code.
- An ISBN on its own cannot be resolved in the DOI System. It must be expressed and registered as an ISBN-A.

The purpose of creating the ISBN-A is to make an existing ISBN useful in a DOI application, for example as an information service. The ISBN-A can resolve to a managed web page service providing descriptive detail about the book e.g. publisher, title, author, subject and product description, cover image, cataloguing data. Publishers can further customise their pages with hyperlinks they control.

The ISBN-A is constructed by incorporating an ISBN into the allowed DOI syntax:

Example: 10.978.12345/99990

The syntax specification, reading from left to right, is:

- Handle System DOI name prefix = "10."
- ISBN (GS1) prefix for books = "978." or "979."
- ISBN registration group element and publisher prefix = variable length numeric string of 2 to 8 digits (in the example '12345')
- Prefix/suffix divider = "/"
- ISBN Title enumerator and check digit = maximum 6 digit title enumerator and 1 digit check digit(in the example '99990')

The relevance of this example is that it clearly illustrates how physical things can be made part of the Internet of Things with a simple extension to an established resolver system. The scale of the potential for the ISBN-A linking physical things to the Internet of Things should not be underestimated. Based on UNESCO data,[24] 8 countries in the world have more than 1 million book titles in print. WorldCat, a bibliographic database used by libraries, currently has over 264 million individual bibliographic records making up 1.8 billion individual holdings.[25] Although not directly linked to ISBN-A, the WorldCat statistics show the extensive size of existing repositories for an information system.

6.4.7 SWOT Analysis

STRENGTHS	OPPORTUNITIES
Well established system supporting an increasing number of domains. Supported by both ISO and IETF standards	A cross-over to physical products, as with ISBN-A, has the potential for an instant IoT set of services
WEAKNESSES	**THREATS**
Has no direct links to data carriers, but can be applied as an additional layer	Considered (probably wrongly) as having a narrow focus

6.5 Ubiquitous Code (ucode)

The Ubiquitous Code, or ucode, offers an end-to-end system that is capable of linking objects with the Internet of Things. Most of the development work has taken place in Japan and the Far East under the umbrella of the T-Engine Forum and, more specifically, the Ubiquitous ID Center. The T-Engine is the name for an architecture, which is arguably one of the most advanced platforms for ubiquitous computing to be found anywhere in the world. It has evolved from an open computing and communications architecture (TRON project) developed in the 1980's by Professor Ken Sakamura.

The system has some fundamental differences from some of the other means of linking objects to the Internet of Things. Firstly, in addition to the basic ucode uniquely identifying objects, other ucodes identify space (locations) and even concepts and relationships (e.g. name, materials, producer). Thus, to access particular information, it is necessary to use a relational database of the different ucodes. There are other differences that are described in detail below.

6.5.1 Item coding

The basic ucode consists of 128-bit code structure with the possibility of being extended to a longer code in the future. The basic structure comprises of five components:

4 bits = version control

16 bits = Top Level Domain Identification Number Code (TLDc)

4 bits = Class Code, which is syntax to define the boundary point between the next two components

m bits (8 to 88) = Low Level Identification Number Code (SLDc)

n bits 96 to 16) = Individual Identification Number Code

A ucode may be applied to physical objects or locations. Unlike the GS1 system, there is no spefic key code such as the GTIN (for products) and GLN (for locations) to distinguish between these functions. An argument put forward by the Ubiquitous ID Center is that a product (e.g. a lamppost) becomes a location when installed in a street. This philosophical view is not shared in all domains.

6.5.2 Data Capture Protocol

The Ubiquitous ID Center claims, and has demonstrated the use of ucode with many different AIDC technologies, so can rightly claim to be agnostic with respect to the data capture technology being used, and there are examples of the ucode in 2D symbols and encoded in an RFID tag.

In the development of the GS1 EPC system and the ISO RFID system, great care was taken to ensure that that data encoding according to the rules of one system did not clash with the other. This was effectively achieved by the ISO RFID system using a mechanism known as data constructs (and registered in the rules of ISO/IEC 15962, and the GS1 EPC system not using these but applying a header code. Neither of these mechanisms was built into the ucode system when using data carriers adopted by other domains. The implication is that there is the potential of a system clash because of the overlapping nature of bits encoded in an RFID tag. A very recent development (February 2012) by the Ubiquitous ID Center seems to be addressing this point, at least for future encoding. A draft Japanese language specification for a Standard memory format of ISO/IEC 18000-based ucode tag [26] seems to make use of an encoding mechanism defined in ISO/IEC 15961-3 that can preserve domain separation using the same RFID technology as other naming authorities.

There are also claims that ucode can, for example, support the encoding of GS1 EPC codes, but this arrangement is not supported by the GS1 organisation.

Criticism levelled at ucode about the encoding of data in the bar code symbology, known as QR Code, needs closer examination. At present there are very few mechanisms that have been invoked to distinguish data from one domain and another – although they exist for most 2D symbologies [27]. So to cite ucode as being wrong is unfair because most domains do not use the distinguishing features that could be invoked. The ucode encoding rules for QR Code [28] offer two variants:

> The standard format, which has an explicit character string 12 characters long. Our assessment, based on the printable characterset of ISO/IEC 8859-1 is that the probability of a systems clash between a ucode and another identifier 1:192 ^ 12, so the risk of a clash with QR Code being used in an industrial application is fairly low. A long established unique string is in ISO/IEC 15434

messages using the sting "])>Rs", which has nearly a 1 in two trillion chance of a clash with non-15434 messages. The risks of a clash by ucode is trillions of times less.

The gateway format uses the "http://" prefix, which is prevalent in a lot of modern day applications for QR Code in magazines and billboards that is resolvable using DNS. The ucode gateway format has a string that is 43 characters long, so the risk of a clash with QR Code being used in another browser application is virtually impossible.

6.5.3 Session Identifier

Although ucodes can be encoded using many different data carrier technologies, there is no clear indication on whether general-purpose data capture devices can be used or whether this depends on the use of the so called Ubiquitous Communicator device. If general-purpose devices are used, then there would be a requirement for specific software or device interfaces to be used.

Most of the examples of the applications of ucode suggest a one-to-one relationship between data capture and look-up via the resolver system, not dissimilar to entering a single website address into a browser and receiving a single response. In such cases the ucode can double as the session identifier.

6.5.4 Addressing Protocol

Addressing the resolver is based on the ucode for the standard format and the url for the gateway format.

6.5.5 Resolving Process

The resolving process follows similar conceptual approaches to other models, but there are some differences that are worth exploring. There are three different resolver protocols:

- ucode resolution protocol
- ucode resolution gateway
- simplified ucode resolution protocol

Figure 8 illustrates how the simplified ucode resolution protocol works.

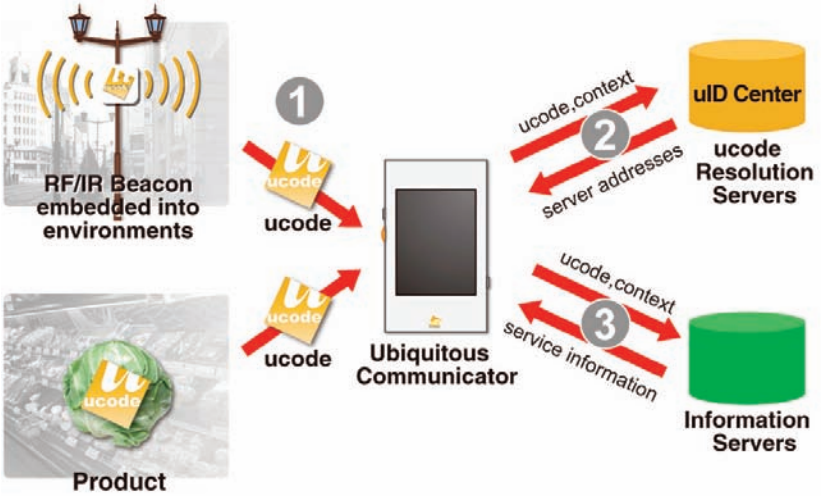


Figure 8: Ubiquitous Code Resolver

If we follow the flows of requests and responses in Figure 8:

1. Requires all the relevant ucode to be captured, possibly even from different data carrier technologies into the Ubiquitous Communicator.
2. Requires the relevant relational ucode to access the resolver servers. Based on the context of the enquiry, the link address to the information server is then returned to the Ubiquitous Communicator.
3. The Ubiquitous Communicator sends the ucode and the address of the information service. For example this can be an IPv4 address,IPv6 address, URL, e-mail address, or telephone number.

From this process, it can be seen that there are some similarities in the architecture used for the Ubiquitous Network and ucode with the Handle system and the DOI.

6.5.6 Information Service

The information service can be based on whatever address type is returned from the resolver. This includes specific data directly associated with the ucode.

6.5.7 SWOT Analysis

STRENGTHS	OPPORTUNITIES
Well established, particularly in Japan Has established resolver processes supporting different types of ucode	Uncertain because ucode has not been aligned with any major application domain.
WEAKNESSES	**THREATS**
Until recently had no signal in the data carrier to signal that the encoding is compliant with ucode	EPCglobal and ISO RFID Also the conception that ucode is seen as a code structure that clashes with long established codes

7 Conclusions

7.1 Overview

Having examined some very different examples of identifier schemes from fast moving goods to virtual things, the most significant conclusion that we reach is that the Internet of Things based on edge data capture technologies has to be considered as a heterogeneous system. The fundamental difference between the identifier schemes, their resolver systems and information services implies that unless such an approach is supported, the implementation of the Internet of Things will be delayed for such physical and virtual things.

7.2 Bar code and the Internet of Things

There are strong arguments for extending edge data capture for the Internet of Things to include bar code technology. This is clearly illustrated by the flexibility of applications employed by ucode. Including bar code technology as part of the Internet of Things may also be useful for existing and potential RFID applications in the ISO and GS1 EPC domains.

Most of such applications have an historic implementation base using bar code technology. Not only will this afford a means of accelerating the take-up of the IoT because of interoperability (as illustrated by the integration of RFID and bar code for IATA baggage handling) but also the low cost of entry will increase the scale. It might even result in some possible novel applications services because experimentation using bar code is a very low cost given the basic nature of mobile phones as data capture devices.

7.3 Data on the Tag versus Discovery Services

In Section 4, we showed that the development of Discovery Services standards had not progressed as originally expected. Three of the four examples that we have explored show little, or scant, development of such standards. The main exception is the Digital Object Identifier system and the way it works under the Handle system.

Although not discussed in the article, RFID tags and two-dimensional symbols have an increasing memory capacity that enables them to encode all sorts of attribute data that had been encoded at a previous event point. The use of sensors attached to RFID tags also provides a dynamic dimension to the updating of environmental data captured by the sensor. There are separate developments in place for different records to be encoded on the same RFID tag (also possible with 2D bar codes) and eventually for RFID tags to have separate securely accessible files.

All of this raises the question of whether an interim, or parallel, solution to the challenge of implementing Discovery Services is to consider some aspects being provided by encoded data on the data carrier itself. We are not suggesting that this bottom-up approach is necessarily a permanent solution, but it might be a novel way to accelerate some developments.

7.4 GS1 EPC

The GS1 EPC framework architecture shows a clear understanding of how elements link together from the edge to the Internet of Things. A risk is that because of the relative cost of RFID to bar code technology, migration to RFID will only be considered when it is cost-effective. Even then, it might be seen as being more applicable to particular sectors (we cite the recent accelerated growth of RFID in the clothing sector) before it becomes more widespread. Such economic consideration, and some constraints on the lifespan of encoding on an RFID tag, imposed by concerns about privacy, might restrict applications on an end-to-end basis.

Given that the original EPC system is considered, by some, to be the foundation of the Internet of Things, some of these constraints might result in it being just a better enterprise-based data carrier technology than a major force for the Internet of Things.

7.5 ISO RFID Object Identifiers

Although the basis of the ISO RFID data and software standards is to make use of object identifiers, the missing piece is a resolver mechanism. A resolver mechanism based on ITU-T standards and proposals presents a challenge.

As authors of a separate approach, we have argued differently but are not in a position to control the eventual outcome. The approach that we prefer is for a closer link between the edge data capture achieved by the ISO RFID registration process and information systems that are domain-specific. Until a technical and political solution can be found, then the vast majority of applications will be excluded from the Internet of Things.

Another major issue is the fact that in the specific domains using ISO standards, the concept of the Internet of Things is often not considered as being relevant to the sector. This is unusual given that for bar code and RFID, such domains are able to look sideways at the GS1 and GS1 EPC systems and draw comparisons. When it comes to the Internet of Things, there seems to be a lack of understanding. The majority of applications that make use of bar code and RFID have significant implementations in Europe. So there is certainly scope for a major education programme to make various sectors aware of the potential of the Internet of Things using bar code and RFID as edge data capture technologies.

7.6 DOI and the Handle System

Although the number of Handle transactions dealt with on a daily basis is probably low compared with the eventual Internet of Things, the number of Digital Object Identifiers is already significant. It follows that there must also be sufficient servers to support resolving the DOIs, probably significantly more than for any other currently deployed object naming system. The DOI as an identifier, or a new identifier based on concatenating the ISO RFID Object Identifer with a Handle prefix (as discussed in Section 6) needs further serious research. The upper layers of the Handle system for resolving and supporting domain specific Information Services provides

a viable benchmark for comparisons with the more conventional URN approach. It has obviously been proven to be scaleable in terms of the number of items, but what needs to be explored is its scalability with respect to a volume of traffic for an Internet of (physical) Things.

7.7 Ubiquitous Code (ucode)

The SWOT analysis (Section 6.5.7) for ucode is a clear indication of the issues concerning this system. On the very positive side, the ucode system has many components that make it suitable for the Internet of Things. Unfortunately, over the years, it has achieved negative publicity – sometimes self-publicity – because of its claims to support other identifier schemes. An example of this is the claim to support GS1 EPC codes – an action that is not sanctioned by that organisation.

In our analysis of ucode, we have made it clear that it can be clearly distinguished from other identifier schemes, so that risk of system clash is small. This is a view that we have reached after significant analysis. However, it is not necessarily the view held by experts in the ISO standards-making fields.

Effectively there is a need for ucode to indicate how it can offer a significant contribution to many applications. If this is not achieved, probably within the next year, then the opportunity to be the basis of IoT data capture in many industrial and commercial domains might be limited.

7.8 Next steps

In this chapter, we have only covered four major identifier schemes. From our work in CASAGRAS2 and the initial CASAGRAS project, we are aware of other naming schemes that have a potential function within the Internet of Things. The scope of this feature has not even considered M2M applications – a major topic in its own right.

One thing that is clear with the edge technologies is that there are gaps in component parts and in standards. There is certainly a lack of understanding of the potential of the Internet of Things being associated with edge data capture technologies. The only way this can be overcome is by an ongoing education and awareness programme combined with focused developments for implementation solutions and standards.

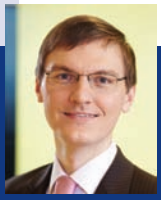
So, our final conclusion is that significantly more work needs to be done for conventional edge data capture technologies to be a reasonable foundation to achieve the Internet of Things.

References

1. http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=IoTGovernance
2. http://www.spec2000.com/index.html
3. oxforddictionaries.com/definition/latent: Lying dormant or hidden until circumstances are suitable for development or manifestation
4. http://www.readwriteweb.com/archives/cisco_50_billion_things_on_the_internet_by_2020.php#more
5. http://www.gs1uk.org/what-we-do/sector-solutions/food/Pages/default.aspx
6. http://en.wikipedia.org/wiki/SWOT_analysis
7. ISO/IEC 18000-6 Type C and ISO/IEC 18000-63 (as yet unpublished)
8. GS1 EPC Tag Data Standard 1.6
9. MIT-AUTOID-WH-002 "The Electronic Product Code (EPC) - A Naming Scheme for Physical Objects"
10. MIT-AUTOID-WH-006
11. US Patent 5457308: Bar code scan stitching
12. ISO/IEC 15420: EAN/UPC bar code symbology specification
13. http://www.edigitalresearch.com/news/item/nid/476207430
14. http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats
15. ISO/IEC 16480 Information technology -- Automatic identification and data capture techniques -- Reading and display of ORM by mobile devices (in development)
16. http://www.gs1.org/sites/default/files/docs/gdsn/stats/gdsn_adoption.pdf
17. GS1 EPC Tag Data Standard 1.6
18. Scalable ID/Locator Resolution for the IoT (DOI 10.1109/iThings/CPSCom.2011.66)
19. http://www.doi.org/factsheets/DOIKeyFacts.html
20. http://www.iso.org/iso/standards_development/maintenance_agencies.htm
21. Note that in our experimenting with the Handle system, we were able to use a single structured Handle prefix '10673'.
22. Source for Figure 7 and the associated procedure: http://www.handle.net/overviews/system_fundamentals.html#resolution
23. http://www.doi.org/factsheets/ISBN-A.html
24. http://en.wikipedia.org/wiki/Books_published_per_country_per_year
25. http://www.oclc.org/worldcat/statistics/default.htm
26. http://www.uidcenter.org/wp-content/themes/wp.vicuna/pdf/UID-00045-01.A0.10.pdf
27. Extended Channel Interpretations (ECI) see http://www.aimglobal.org/standards/symbinfo/eci.asp
28. http://www.uidcenter.org/wp-content/themes/wp.vicuna/pdf/UID-00025-01.A0.00_en.pdf

Paul Chartier [paul.chartier@praxisconsultants.co.uk]

George Roussos [g.roussos@dcs.bbk.ac.uk]




Privacy Concerns and Acceptance of IoT Services

By Tobias Kowatsch and Wolfgang Maass

This chapter summarizes the Internet of Things - Initiative (IoT-I) deliverable of Kowatsch and Maass (2012)

Abstract

Internet of Things (IoT) services provide new privacy challenges in our everyday life. Although privacy research has been addressed to a great extent in the Information Systems discipline, there still exists no robust instrument for the evaluation of IoT services. The contribution of this chapter is therefore to propose and test such an instrument in order to provide policy makers, IT developers and IS researchers with recommendations on how to design privacy-aware IoT services. The current research is based on utility maximization theory and integrates theoretical constructs from the Extended Privacy Calculus Model and the Technology Acceptance Model. An empirical study with 92 subjects is conducted to test this instrument. Results indicate that the acceptance of IoT services is influenced by various contradicting factors such as perceived privacy risks and personal interests. It is further assumed that legislation, data security and transparency of information influences the adoption behaviour. Further research will focus on these factors to enable the development of useful and secure IoT services in the very near future.

1. Introduction

With the increasing amount of Internet of Things (IoT) services, i.e. sensor-based IS services facilitated by identification technologies such as barcode, radio frequency, IPv6 or global satellite communication, people face new security and privacy challenges in their private and business life (Weber, 2010). For example, mobile applications such as Foursquare, Facebook Places, Google Places or Groupon track the location of their users to provide an added value by the underlying contract: give up a little of your privacy, and you get worthwhile information. In these examples, the tracking of location-based information becomes obvious to a user, as he/she is aware of it by intentionally using them. However, sometimes it is not obvious

which kind of information gets tracked at which time, e.g., when those services are running in the background or when the user forgets to terminate them.

Serious consequences can arise when, for example, that information is linked to Twitter or Facebook and is then used to commit crimes such as breaking into an empty home. Nevertheless, there also exist situations in which personal information is being intentionally tracked in the background. For example, a healthcare monitoring service must track constantly critical health parameters of an individual without notifying her about it all the time.

In this regard, it is therefore of the utmost importance to better understand usage patterns and perceptions from an end-user perspective so that IoT services can be designed with appropriate privacy and security standards in mind. Accordingly, the relevance of these topics has been addressed by prior Information Systems (IS) research (e.g. Bélanger and Crossler, 2011).

However, no empirical IS instrument has been developed and tested for the class of IoT services that reveals significant predictors of IoT service usage. IoT services differ particularly from other IT-related applications in traditional office or home office situations due to their ubiquitous and embedded characteristics that pervade our everyday life. Thus, privacy concerns due to unobtrusive data collection methods are more critical for this class of applications and appropriate evaluation instruments are required.

From a theoretical point of view, we ground the current work on utility maximization theory and the Extended Privacy Calculus Model (EPCM, Dinev and Hart, 2006). We suggest that as long as IoT services are perceived as being useful and the higher the individual or organizational interest in using them, the lower are the privacy concerns; and low privacy concerns are assumed to be related to high adoption rates of IoT services. This chapter aims to present results of an empirical study on privacy concerns, rationales and potential ways of overcoming the privacy fears of IoT services that are currently discussed in the European IoT community. For that purpose, a research model was proposed and empirically tested with 92 subjects. It comprised critical factors that predict usage intentions of IoT services and the individuals' willingness to provide personal information in order to use them.

2. Research Model and Hypotheses

The research model and hypotheses of the current study are depicted in Figure 1. The theoretical constructs and their relationships are primarily derived from EPCM. EPCM has been successfully tested in the domain of electronic commerce and proposes four constructs that influence the willingness to provide personal information for Internet transactions: perceived Internet privacy risk, Internet privacy concerns, Internet trust and personal Internet interest.

Additionally, two constructs from the Technology Acceptance Model (TAM, Davis, 1989) are considered in the current work. That is, perceived usefulness and the intention to use IT. Having its roots in the Information Systems discipline, TAM describes determinants of technology adoption and is rooted in the theory of planned behaviour (Ajzen, 1991), which states that individuals' beliefs influence behavioural intentions that, in turn, have an effect on actual behaviour. The target behaviour of interest in the IS community is then the adoption of IS artifacts.

Both EPCM and TAM have been incorporated in the current research in order to address critical privacy and technology constructs that are relevant for the acceptance of IoT services. The following construct definitions are adapted from Dinev and Hart (2006, p.64, Table 1), Davis (1989, p. 320ff) and Kamis et al. (2008) such that they apply to the concept of IoT services:

Perceived IoT service privacy risk reflects perceived risk of opportunistic behaviour related to the disclosure of personal information of IoT service users in general.

Privacy concerns against IoT service are concerns about opportunistic behaviour related to the personal information transferred to the IoT service by the individual respondent in particular.

Trust in an organization providing the IoT service summarizes trust beliefs reflecting confidence that personal information transferredto the IoT service organization will be handled competently, reliably, and safely.

- Personal interest in an IoT service reflects the cognitive attraction to an IoT service while overriding privacy concerns.
- Willingness to provide personal information for an IoT service reflects the degree to which individuals are likely to provide personal information such as location-based information or financial information required to complete transactions of a particular IoT service.

The following two constructs are adapted from TAM research whereby perceived usefulness was reworded as expected usefulness due to the prospective character of the current study:

- Expected Usefulness of an IoT service is defined as the degree to which a person believes that using that service would enhance his or her overall performance in every day situations
- Intention to use an IoT service reflects behavioural expectations of individuals that predict their future use of that service.

Two modifications were made in order to combine EPCM and TAM for the current study. First, intention to use was included as a construct that mediates the impact on the willingness to provide personal information for using an IoT service. The rationale for this relationship lies in the assumption that individuals would not provide her personal information without intending to use that service. Second, expected usefulness of an IoT service was added as a construct that influences the behavioural intention to use that service. That is, IoT services are more likely to be adopted when they are perceived useful.

In summary, the eight hypotheses as depicted in Figure 1 are derived from EPCM, TAM and the assumptions discussed above. In addition to these hypotheses, we have been able to investigate how three contextual factors, i.e. legislation, data security and transparency of information use, may also influence the acceptance of IoT services.

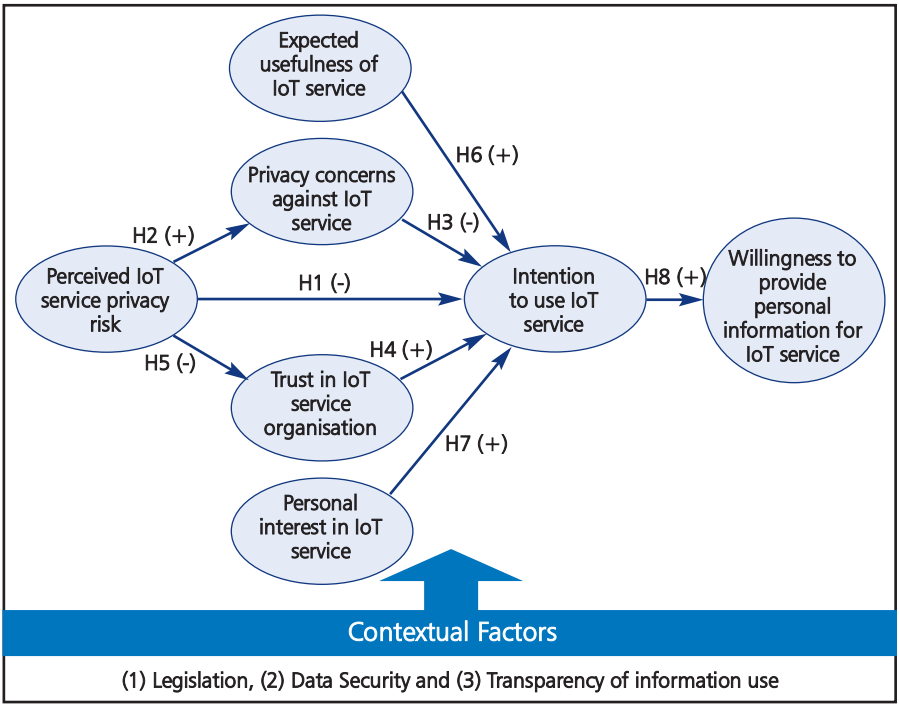


Figure 1. Research model. Note: Constructs are hypothesized to have either a positive (+) or negative (–) relationship

3. Method

In order to test the research model, an online survey was developed. For this reason, four relevant IoT services embedded in two business situations and two private situations were identified from a pool of 57 applications (Presser and Krco, 2011). The rationale behind this evaluation lies in the Situational Design Method for IS (Janzen et al., 2010).

Here, situational descriptions are one of the first steps towards the design of IT artifacts. The resulting IoT services are presented in Table 1.

The questionnaire items of the theoretical constructs have been adapted from prior research (Davis, 1989; Dinev and Hart, 2006; Kamis et al., 2008; Moore and Benbasat, 1991). Furthermore, items on legislation, data security and transparency of information use have been developed separately. Finally, variables such as technology affinity, age, gender and country have been incorporated into the questionnaire to account for technological and

socio-demographic biases. The exact wording of all items and details on the IoT service selection process can be found in the public IoT-I project (http://iot-i.eu) deliverable D2.4 (Kowatsch and Maass, 2012).

The sampling of subjects was conducted online through various media channels of the IoT-I partner organizations in March and April 2012. Thus, invitations to participate in the online survey were communicated via the project websites of IoT-I and IoT-A, Twitter, IoT LinkedIn groups or the Internet of Things Council. Each participant was randomly assigned to one IoT service from Table 1 and had to first read through the narrative of the IoT service and was then asked to evaluate this service.

No	IOT service	Situational description	Focus
1	Public Transport Payment Service	You are taking the bus to work and receive a message from the public transport company via your mobile phone. They offer you a payment service that charges you once you get off the bus based on the number of zones you cross. The information also displays the cost per zone. After your authorisation payment is performed automatically via your mobile phone.	Business situation
2	Navigation Service	You leave your home for a business trip and receive detailed information about traffic conditions including traffic accidents, traffic jams, weather conditions and parking possibilities directly integrated into your personal navigation service. It routs you, including driving, walking, public transport and car pooling, in the most efficient way and as close as possible to your destination. Persons (incl. you), cars and public transport share their location information together with other personal data relevant for the navigation service in the Internet cloud.	
3	Smart Energy Service	You live in a modern house and the Smart Energy Service manages your energy consumption. It combines data from outdoor and indoor temperature, weather forecast from the Internet, and user preferences. It also recognizes which appliances (e.g., washing machine, dish washer, water heater, heating system) are turned on at a given time and synchronises them to ensure the best energy efficiency taking into account pricing structure of the utility companies.	Private situation
4	Healthcare Monitoring Service	Recently the doctors have diagnosed that your health condition is taking a turn for the worse. As a result, you have upgraded the current health monitoring solution with sensor applications that enable the monitoring of your location, posture and general health condition at home and in the neighbourhood. As a result, you retain your private and social life, which is very important for coping with your condition and happiness.	

Table 1. IoT services, situational description and focus of evaluation

4. Results

Overall, 69 male and 23 female subjects participated in the online survey. The age of the subjects ranged from 24 to 62 with a mean value of 35.4 (Std. Dev. = 8.87). The majority of subjects live in Germany and thus, results of the current study are biased in this regard. Furthermore, subjects can be characterized as technically savvy, because with 6.11 the mean value of the technology affinity construct lies significantly above the neutral scale value of 4 on a 7-point Likert scale.

Statistic	Public Transport Payment Service	Navigation Service	Smart Energy Service	Healthcare Monitoring Service
Perceived IoT service privacy risk (5 items)				
Cronbach's Alpha	.819	.774	.920	.760
Mean	4.99	5.43	4.93	4.64
St. Dev.	1.12	1.00	1.49	1.16
Privacy concerns against IoT service (4 items)				
Cronbach's Alpha	.914	.867	.947	.913
Mean	4.96	5.49	5.05	5.10
St. Dev.	1.34	.91	1.60	1.46
Trust in organizations providing the IoT service (3 items)				
Cronbach's Alpha	.832	.645	.904	.782
Mean	4.83	4.23	4.96	4.46
St. Dev.	1.22	1.06	1.42	1.20
Expected usefulness of IoT service (4 items)				
Cronbach's Alpha	.915	.859	.865	.943
Mean	5.78	5.57	5.48	5.91
St. Dev.	1.25	.84	.89	1.29
Personal interest in IoT service (3 items)				
Cronbach's Alpha	.862	.861	.782	.645
Mean	4.20	4.04	4.32	4.49
St. Dev.	1.63	1.35	1.29	1.33
Intention to use IoT service (2 items)				
Cronbach's Alpha	.937	.798	.871	.938
Mean	5.09	5.02	5.28	5.41
St. Dev.	1.64	1.07	1.10	1.28
Willingness to Provide Personal Information (2 items)				
Cronbach's Alpha	.729	.615	.772	.682
Mean	3.87	3.76	4.27	4.52
St. Dev.	1.42	1.55	1.72	1.70

Table 2. Descriptive statistics. Note: n=23 for each service, 7-point Likert scales were used ranging from very low risk / not at all concerned / strongly disagree (1) to very high risk / very concerned / strongly agree (7)

Descriptive statistics of the theoretical constructs are listed in Table 2. Cronbach's Alpha lies over the recommended threshold of .70 (Nunnally, 1967) for all constructs with four exceptions, where the value lies between .615 and .682. However, to be consistent with prior research (Dinev and Hart, 2006), the corresponding items were not dropped from further analysis. Accordingly, aggregated values were calculated.

Pearson correlation coefficients with two-tailed tests of significance have been calculated to test the eight hypotheses. The resulting coefficients that are shown in Table 3 indicate that three hypotheses are fully supported by the empirical data, i.e. five for all four evaluated IoT services (H2, H4 and H7) whereas the other hypotheses are partly supported by at least one of the four IoT services.

Finally, statistics related to the questionnaire items on legislation and data security are presented in Figure 2. Results on the preferred level of detail and frequency of notifications on personal information use are depicted in Figure 3 and Figure 4, respectively.

Hypothesis	Public Transport Payment Service	Navigation Service	Smart Energy Service	Healthcare Monitoring Service	Results
H1: PR * IU	–.511***	–.504***	–.269 n.s.	–.426**	Partly accepted
H2: PR * PC	.815***	.626***	.826***	.793***	Accepted
H3: PC * IU	–.498***	–.169 n.s.	–.375 n.s.	–.398 n.s.	Partly accepted
H4: TO * IU	.567***	.578***	.523***	.588**	Accepted
H5: PR * TO	–.383 n.s.	–.351 n.s.	–.443***	–.065 n.s.	Partly accepted
H6: EU * IU	.714***	.239 n.s.	.592***	.327 n.s.	Partly accepted
H7: PI * IU	.785***	.621***	.415***	.546***	Accepted
H8: IU * WPI	.474***	–.045 n.s.	.111 n.s.	.726***	Partly accepted

*Table 3. Pearson correlation coefficients for the eight hypotheses. Note: n=23 for each service, * = p < .05 / ** = p < .01 / *** = p < .001, n.s. = not significant*

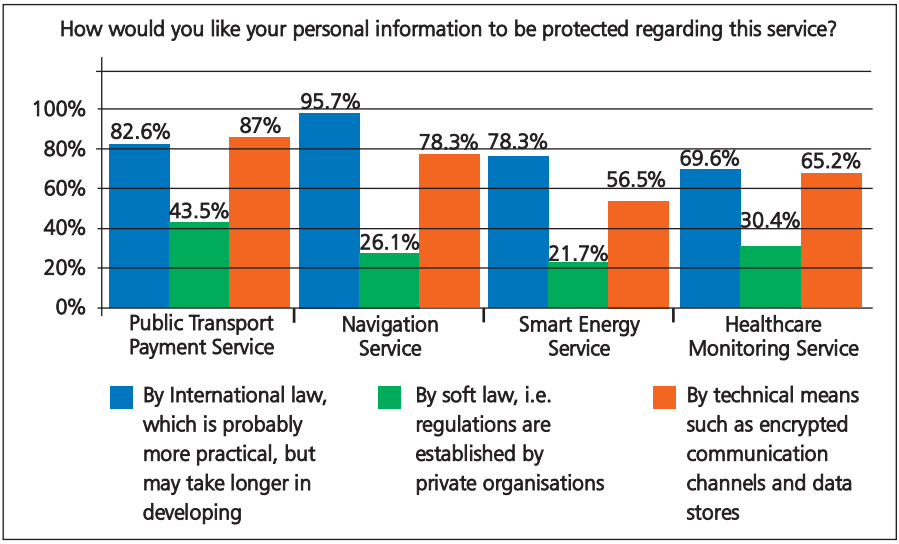


Figure 2. Legislation and data security (n=23 for each service)

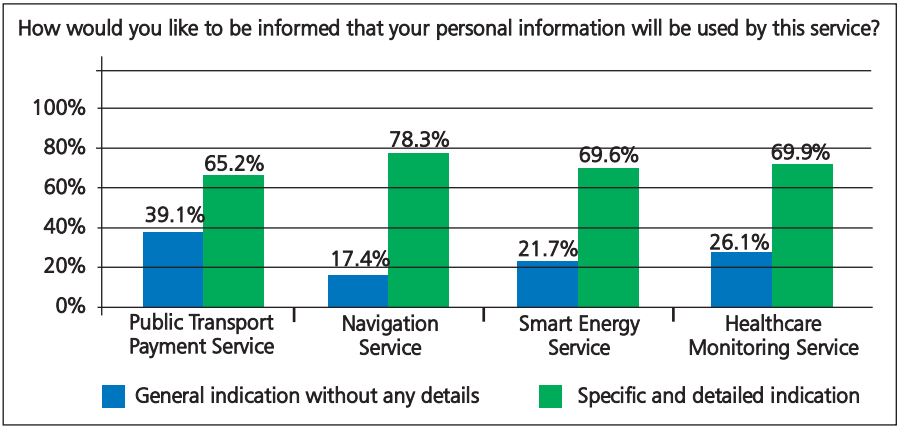


Figure 3. Preferred level of detail of notifications (n=23 for each service)

5 Discussion

Overall, the results of the IoT survey on critical privacy factors show that the empirical data of the 92 subjects support the proposed research model and corresponding hypotheses. A detailed discussion of the results is presented in the following.

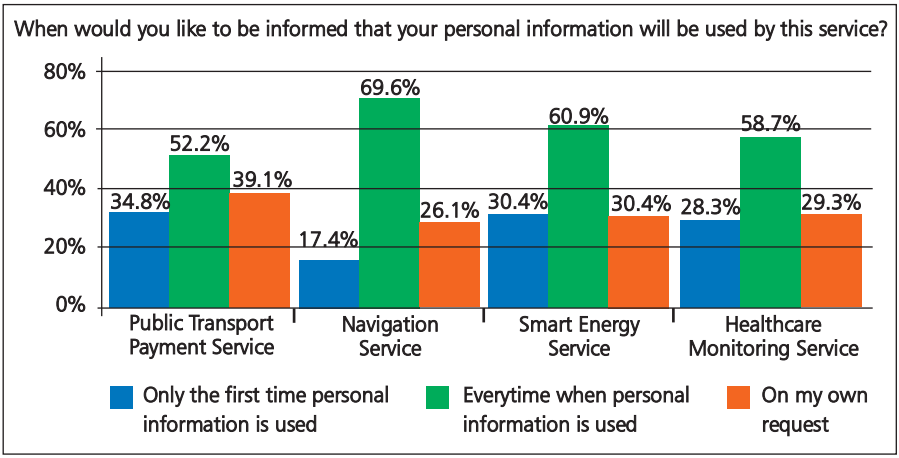


Figure 4. Preferred frequency of notification (n=23 for each service)

5.1 General implications

The current study has adapted the extended privacy calculus model (Dinev and Hart, 2006) to the IoT domain with a focus on IoT services. This model describes critical privacy factors. It was further extended with two constructs from the Technology Acceptance Model (Davis, 1989). All in all, the proposed research model was tested successfully. That is, all hypotheses are supported by the empirical data either completely – by all IoT services (H2, H4 and H7) – or at least by one IoT service (H1, H3, H5-6 and H8). It can also be stated that there are no obvious differences between the IoT services used in business situations or private situations. In particular, it could be shown that perceived privacy risk and privacy concerns have a positive relationship at the .001 level of significance. However, these constructs do not consistently predict the intention to use IoT services. By contrast, the intention to use IoT services is significantly influenced by trust in service providing organizations and personal interest at least at the .05 level of significance.

Thus, it can be concluded that trust and personal interest are more important factors for end users than privacy risks and privacy concerns. Accordingly, organizations should primarily address trust and personal interests in the development process and marketing activities of their IoT services such that the acceptance in the society can be increased.

Results on legislation and data security (Figure 2) as well as the preferred level of detail and frequency of notification of personal information use (Figure 3 and Figure 4) provide clear guidelines for the design and implementation of IoT services. Accordingly, approximately 82% of the subjects expect that their personal information should be protected by international law. In addition to these legislative aspects, personal information should be also protected by technical means as indicated by 72% of the subjects (cf. Figure 2).

Thus, state of the art encryption and security standards should be incorporated and advertised together with the pure functionality of IoT services. Additionally, 71% of the subjects made a point of requesting specific and detailed statements with regard to personal information use. Thus, brief and more general statements should be avoided when an IoT service is deployed (cf. Figure 3). Furthermore, the majority of subjects (approx. 60%) stated that they want to be informed every time when personal information is used by an IoT service (cf. Figure 4). Even though the default option should be a trigger that informs users of an IoT service every time personal information is forwarded to a third-party organization, this only makes sense for IoT services that are used rather infrequently, i.e. once or less a month. It is thus recommended to provide an option that allows changing the trigger of notification individually and to decide on the default option based on the frequency of average IoT service usage.

Finally, we recommend IoT service providers to conduct a privacy impact assessment as proposed in prior work for applications that use radio-frequency identification technology (RFID) (European Commission, 2011; Oetzel et al., 2011).

5.2 Limitations

The current study has three general limitations. First, results are biased in the sense that primarily male and technology-savvy persons have participated. Although these individuals may adopt innovative IoT services first, support from a more equally distributed sample would increase external validity of the findings. Second, results are also biased towards the origin of the subjects, i.e. almost 60% live in Germany. In addition to that, external validity of the results is restricted with regard to the textual descriptions of the IoT situations compared to, for example, drawings, video clips, lab experiments or field experiments that would all increase subjects' understanding of the IoT services and thus the quality of evaluations.

6 Conclusion and Outlook

The extended privacy calculus model (Dinev and Hart, 2006) has been combined with the Technology Acceptance Model (Davis, 1989) and was successfully tested in the IoT domain by conducting an online survey with 92 subjects. As a result, critical factors have been identified that influence the adoption of IoT services and thus, are critical for their design and implementation. Furthermore, several practical implications have been discussed with regard to legislation, data security and notification of personal information use.

Future work should test the current results with a wider data basis by conducting further studies. The overall objective should be then to cross-check the current findings by adding external validity and thus, to increase the quality of implications. Nevertheless, organizations should generally perform privacy impact assessments (European Commission, 2011; Oetzel et al., 2011) such that their IoT services are not only useful but also address the privacy concerns of their potential users.

References

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50 (2), 179-211.

Bélanger, F. and Crossler, R.E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly, 35 (4), 1017-1041.

Davis, F.D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13 (3), 319-339.

Dinev, T. and Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research, 17 (1), 61-80.

European Commission (2011). Privacy and Data Protection Impact Assessment Framework for RFID Applications.

Janzen, S., Kowatsch, T. and Maass, W. "A Methodology for Content-Centered Design of Ambient Environments," in: Global Perspectives on Design Science Research, 5th International Conference, DESRIST 2010, St. Gallen, Switzerland, June 4-5, 2010 Proceedings, R. Winter, J.L. Zhao and S. Aier (eds.), Springer, Berlin, Germany, 2010, pp. 210-225.

Kamis, A., Koufaris, M. and Stern, T. (2008). Using an Attribute-Based Decision Support System for User-Customized Products Online: An Experimental Investigation. MIS Quarterly, 32 (1), 159-177.

Kowatsch, T. and Maass, W. (2012). The Internet of Things Initiative (IOT-I) Deliverable 2.4 Social Acceptance and Impact Evaluation, FP7 ICT project, contract number: 257565

Moore, G.C. and Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. Information Systems Research, 2 (3), 192-222.

Nunnally, J.C. (1967). Psychometric Theory McGraw-Hill, New York.

Oetzel, M.C., Spiekermann, S., Grüning, I., Kelter, H. and Mull, S. (2011). Privacy Impact Assessment Guideline for RFID Applications, Bundesamt für Sicherheit in der Informationstechnik.

Presser, M. and Krco, S. (2011). The Internet of Things Initiative (IOT-I) Deliverable 2.1: Initial report on IoT applications of strategic interest, FP7 ICT project, contract number: 257565

Weber, R. (2010). Internet of Things - New security and privacy challenges. Computer Law & Security Review, 26, 23-30.

Towards a Framework of IoT Standards

By Paul Chartier

1. Introduction

In preparing this chapter, it was important to consider whether it is possible in 2012 to have a definitive framework of standards for the Internet of Things. A review of articles in previous IERC Cluster books suggests that there is still some uncertainty about a definitive framework for the Internet of Things. There are also very different views on the relevance of particular standards. It therefore seemed sensible to be modest and add the 'Towards a' as part of the title. This will allow the reader to agree or disagree and to consider alternatives. However, because this chapter is based on work that is being undertaken in Work Package 6 Standards and Regulations of the CASAGRAS2 project it is also possible to be realistic. Here the focus is on a specific task, which is also the main deliverable of the Work Package:

The key point here is the focus on building on what already had been identified, and addressing standards that exist or are in development.

> Task 6.2 : Standards and Regulatory Support Repository
>
> This task will build upon the outputs of CASAGRAS1 and GRIFS in establishing a repository of information on existing standards and regulations and those under development, that can be used for IOT projects support and as a platform for accommodating further information on standards and regulations arising within the project.

2. The Original GRIFS Database

One of the deliverables of the GRIFS project was to deliver a report on

> "an inventory/state of the art on the development and implementation of RFID standards, on a global scale, identifying the standards bodies, the geographical and technical scope of the work, opportunities and risks of collaboration, including gap/overlap analysis."

The GRIFS project overlapped with the initial CASAGRAS project, and a Memorandum of Understanding was established between the two projects, which also had an overlap of experts.

At the end of the first year a significant report was produced, but even in a downloaded format it was becoming out-of-date on a weekly basis. To overcome this, the GRIFS project produced an online repository for the final project delivery. The online database had details of 127 published standards and 48 that were being developed. These covered 18 subject areas from the RFID air interface protocol at the edge to relevant Internet standards, plus health and safety standards and emerging privacy regulations. It made sense to have this broad coverage, because of the fact that GS1 EPC (previously called EPCglobal) standards already had component standards directly relevant to the Internet of Things. Although there were gaps in the ISO RFID standards these too, had structures intended to be used with the IoT.

The categories that were covered, with the number of standards in ( ), were:

- Air interface standards (14)
- Application standards (10)
- Conformance and performance standards (21)
- Data encoding and protocol standards (often called middleware) (12)
- Data exchange standards and protocols (12)
- Data protection and privacy regulations (6)
- Data standards (3)
- Device interface standards (8)
- Environmental regulations (e.g. WEEE, packaging waste) (3)
- Frequency regulations (28)
- Health and Safety regulations (9)
- Internet Standards (25)
- Mobile RFID (5)
- Real time location standards (6)
- Security standards for data and networks (2)

Sensor standards (2)
The European Harmonisation procedure (3)
Wireless Network Communications (6)

There was some recognition that other standards would have an impact on the continued development of RFID implementations and developments. These topics, some of which were covered by the database, are shown in Figure 1.

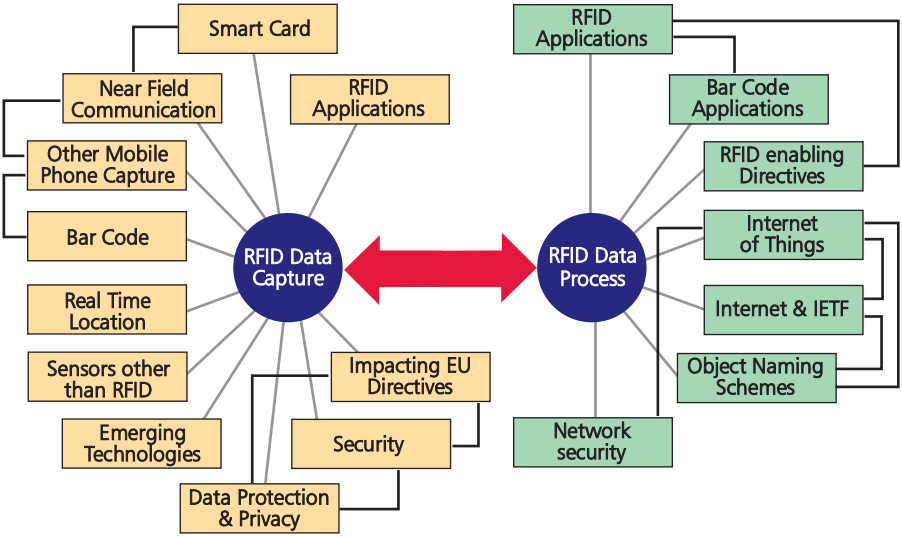


Figure1: Network of influencing developments

This figure is taken from the final GRIFS report, which is still available [1]. The point to draw from the figure is that the topics linked to the circle 'RFID Data Capture' are either alternative technologies or strong influences. The topics linked to the circle 'RFID Data Processing' are more associated with the data once captured.

Having established a publicly accessible on line database, it was a resource not to be wasted, even though one of the objectives of the GRIFS project was to involve many organisations in its on-going maintenance. The creation of the CASAGRAS2 project with its specific task to continue developing the repository provided the means to extend and update the database.

3. The IoT Standards Database

This is still work-in-progress. The current main screen is shown in Figure 2.

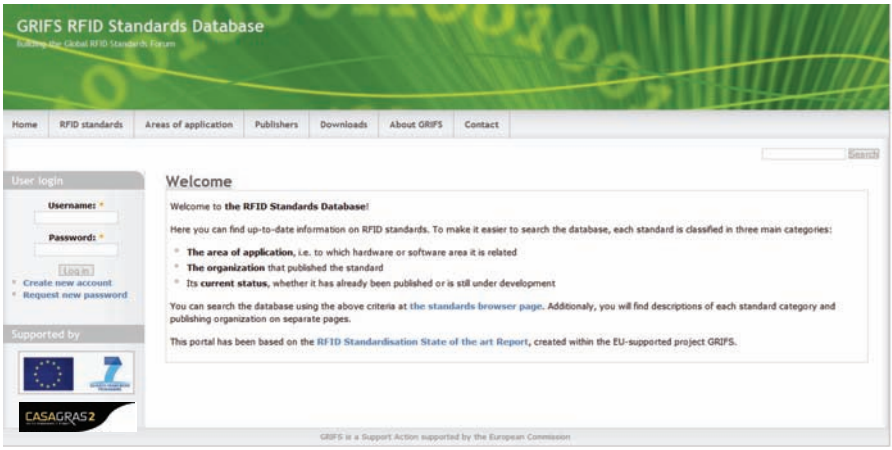


Figure 2: Home Page of the IoT Standards Database [2]

The database is undergoing some minor redesign but the main function will remain the same.

The broader scope has resulted in some standardisation topics (shown in bold text), with the original categories with modified names shown in italic text:

- *AIDC application standards*
- **Bar code conformance standards**
- **Bar code standards – linear symbologies**
- **Bar code standards – 2D & multi-row symbologies**
- *Data and identifier standards*
- *Data exchange standards and protocols*
- *Data protection and privacy regulations*
- **Environmental regulations**
- *Frequency regulations*
- *Health and Safety regulations & standards*
- **Information services and discovery service standards**

- **Internet standards – not otherwise covered**
- **M2M (Machine-to-Machine)**
- *Mobile RFID standards*
- **Near field communication standards**
- **Resolver specifications & standards**
- **RF-based identity card standards (inc Smartcards)**
- *RFID air interface standards*
- *RFID conformance and performance standards*
- *RFID data encoding and protocol standards*
- *RFID device interface standards*
- *RTLS (Real time location systems) standards*
- *Security standards for data and networks*
- *Sensor standards*
- *The European Harmonisation procedure*
- **Wireless network communication**

Each standardisation topic can be identified from this url:

http://www.iotstandards.org/?q=taxonomy/term/30

There are links to a descriptive page on the topic. The taxonomy has a flexible structure. This has been done deliberately to enable new standardisation topics to be added, some to be sub-divided, and most importantly for the list of standards to be assigned to the most relevant prevailing topic. If aspects of the Internet of Things are still unclear, then all that the database has as a certain solid foundation is that a relevant set of standards has been published or are in development. Where they belong in the grand scheme of the Internet of Things might be the subject of heated discussion. At any point in time, the standards associated with a given topic can be accessed by links on the website, such as this one for the RFID air interface standards:

http://www.iotstandards.org/?q=facet/results/taxonomy%3A15

Each standard is listed, with a link to a more detailed page for every entry. Superseded standards are retained on the database when they are associated, for example, with a standard to which hardware needs to

conform. This is to address the reality that when a new edition of a standard is published not all manufacturers will cease producing products conformant to the previous version. Certainly users cannot be expected to discard devices every time a new standardised feature is added. The database covers the known publication span of such standards, so that applications that depend on open systems can be aware of the different functionality.

Within the given standardisation topic, not all the candidate standards are included. This is generally based on consensus view of the experts working to compile the database. As an example, IETF defines a number of URNs. Some have been excluded because the purpose is unlikely to be associated with the Internet of Things. Others, such as the URN for the ISBN[3] might at first appear suitable for the Internet of Things. The author, having worked with the International ISBN Agency, is aware that there are virtually no implementations of this URN. Furthermore, now that the ISBN is a properly constituted code within the GS1 system, its resolution from edge data capture is more likely to be based on the URN for EPCglobal.[4]

4. Specific Framework Models

If a comprehensive IoT framework model is to be proposed, it makes sense to explore what others have proposed. A comprehensive literature search could be – and was – undertaken, but in most cases the emphasis was on a framework of technologies and is sometimes based on a given perspective concept of the Internet of Things.

As the objective is to try to define a framework of IoT standards, it is more logical to consider frameworks or architectures that have already been developed with this point in mind. In the next two sub-sections, we analyse two different approaches from two different organisations:

The GS1 EPC architecture model has been in place for a number of years with all but very minor modifications. The only significant changes year by year have been associated with the publication of a new component that was already defined in the architecture. The particular architecture is also relevant, because it shows an end-to-end approach for the IoT based on edge data capture.

The other model that we use is based on the ETSI M2M specifications work programme. This has the advantage of focusing on a different perspective of the Internet of Things, one that does not depend on RFID tags or bar codes being attached to physical things.

4.1 The GS1 EPC Architecture Framework

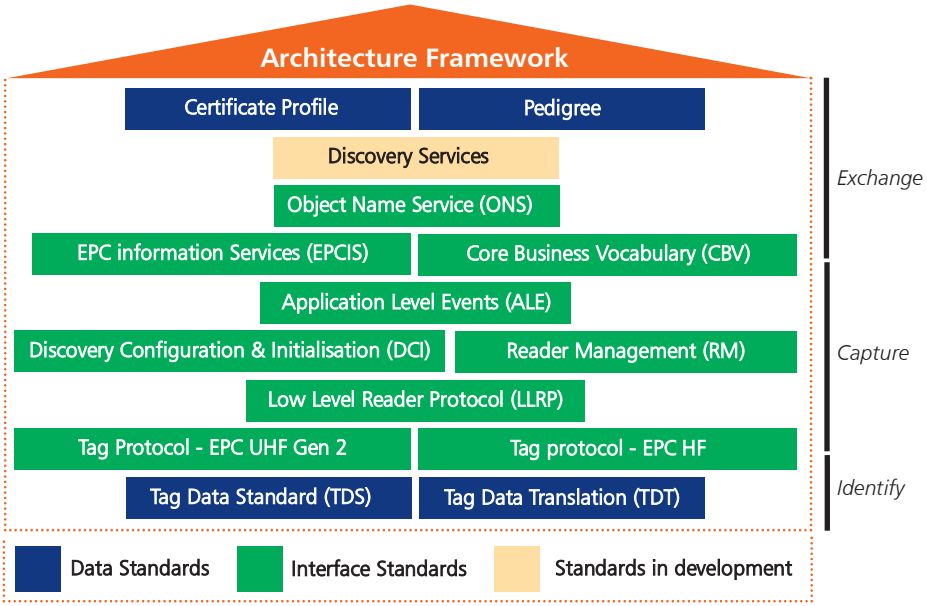


Figure 3: The GS1 EPC Architecture Framework

Figure 3 shows all the layers from the encoded data (the Tag Data Standard) through upper layers that define:

How RFID readers are specified to function when reading and writing with RFID tags, here shown as the tag protocol, but more correctly defined by the ISO term air interface protocol.

How readers communicate with upper layers, here shown as the Low Level Reader Protocol

Functions that configure the reader network (Discovery, Configuration & Initialization) and control this continually (Reader Management)

How to control the flow of data (Application Level Events)

The domain specific information system (EPC Information Services) and supporting attribute data (Core Business Vocabulary) *Note: In the GS1 EPC architecture the information service can reside below the resolver (i.e. cached within the enterprise) and externally accessed via the Internet*

The resolving system (Object Name Service)

The discovery services, the standard of which has still to be developed.

The uppermost layers, Certificate Profile and Pedigree support application-specific functions.

Although the framework is now stable, some of the original components from the MIT AutoID Center, such as Savant, have disappeared without being developed or implemented.

4.2 The ETSI M2M Specification Framework

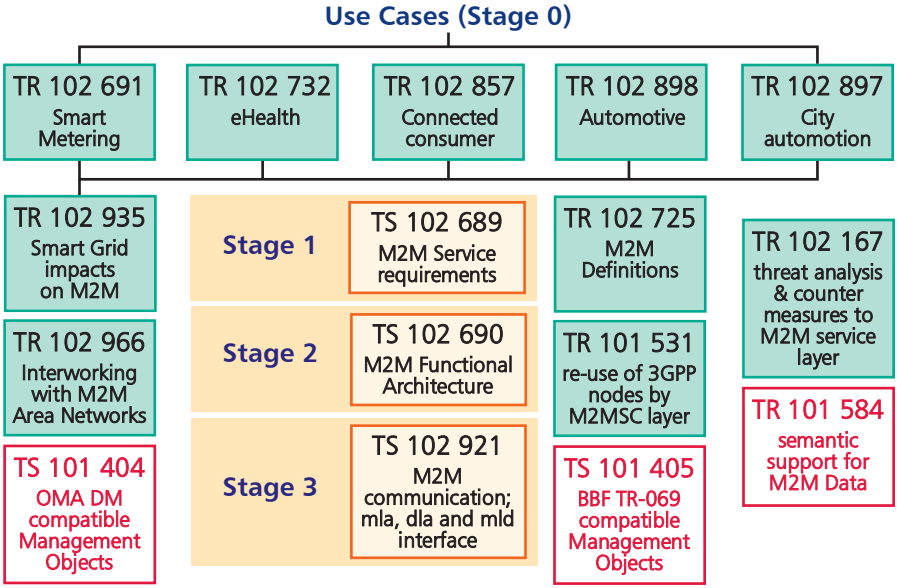


Figure 4: ETSI M2M Specification Framework

This is a model for work items, some of which have been completed, particularly the core Technical Specifications:

- TS 102 689 M2M Service requirements

- TS 102 690 M2M Functional Architecture
- TS 102 921 M2M Communications: mla, dla and mld interfaces

It is also clear that whereas there is a Technical Report for Smart Grid Impacts on M2M (TR 102 935), there are as yet no equivalents for eHealth, connected consumer, automotive, and city automation. Only time will tell whether these are potential gaps in the standardisation programme, or that an explicit standard is not required. This example highlights the fact that a framework might evolve as we learn more about a particular standardisation topic.

4.3 The RFID M436 Mandate on RFID Privacy

February 2012 saw the kick-start of work on the second phase of this EU funded mandate, covering ten standardisation activities:

Task A on Signage and Emblem (PT A)

- Task A.2.1 CEN Technical Specification (TS): Notification of RFID: The information sign to be displayed in areas where RFID interrogators are deployed.
- Task A.2.2 CEN Technical Report (TR): Notification of RFID: Additional information to be provided by operators
- Task A.2 European Standard (EN): Notification of RFID: The information sign and additional information to be provided by operators of RFID data capture applications

Task B on RFID Device Privacy (PT B) 1

- Task B.2 CEN Technical Report (TR): Privacy capability features of current RFID technologies.

Task C on Privacy Impact Assessment (PT C)

- Tasks C.3 and C.4 CEN Technical Report (TR): RFID PIA analysis for specific sectors.
- Task C.2 CEN Technical Report (TR): Analysis of PIA methodologies relevant to RFID.
- Task C.1 European Standard (EN): RFID Privacy Impact Assessment (PIA) process.

Task D on RFID Penetration Testing (PT D)

- Task D.2.2 CEN Technical Report (TR): RFID threat and vulnerability analysis

Task E on Extended RFID device security capability (PT E)

- Task E.3 CEN Technical Report (TR): Authorisation of mobile phones when used as RFID interrogators.
- Task E.4 CEN Technical Specification (TS): Device interface to support ISO/IEC 18000-3 Mode 1 and Mode 3 tags

These have been included for three reasons:

First, although there was a perceived need to address the topic of RFID privacy, the details of the work items were not established until mid-2011, and were the consensus view of experts on the European standards committee, CEN TC 225.

Secondly, there was no certainty that the European Commission would share the proposals put forward by CEN TC 225. In fact, not only were the work items supported, but the Commission extended the scope to cover non-contact payments using smart cards. Non-contact cards had been included within the scope for some time, even though this standardisation topic is outside the scope of CEN TC225; it is within the scope of CEN TC224 requiring increased collaboration in the development of the documents.

Finally as these standards are developed, they will serve as benchmarks for other gaps in the standardisation process with the RFID arena and beyond. Will the PIA standard be a model for a PIA for the Internet of Things? Time will tell.

5. Standards Framework Based on Logical Links

Figure 5 shows a mindmap based on the standardisation topics listed in Section 3. This is shown on the next page. The intention is to show all the standardisation topics in relation to the others. A constraint of this approach is that relationships are shown in a hierarchical structure. To create this, some headings (shown in green boxes) had to be created as parents of topics that are known to be required. This hierarchical structure has some advantages and some disadvantages:

The topic RF frequency regulations appears above NFC, RF-based personal cards, RFID and RTLS. While this is true, references to these regulations are generally in the conformance standards.

A disadvantage of such a hierarchical structure can be shown in many areas of the mindmap, but here are two examples. The direct

link from the AIDC data capture technologies to the IoT via resolvers is not clear. The topic Sensors is shown on the top line alongside RFID, but the standards that are covered under this topic can apply equally to RTLS technolgy. This category of sensor is very different from the type of sensor associated with M2M applications.

Putting aside the issue that a tool like a mindmap does not expose more complex relationships, an advantage is that it has the potential to compare hierarchies, hence some of the grey boxes, which identify potentially additional standardisation topics for the on-line database.

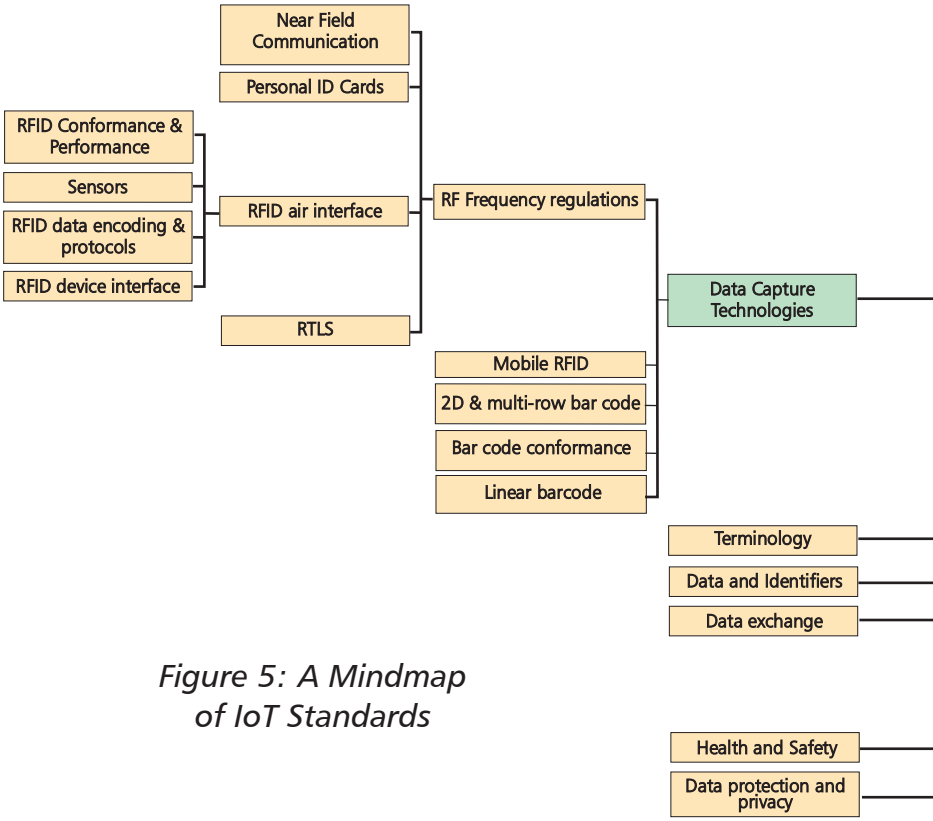
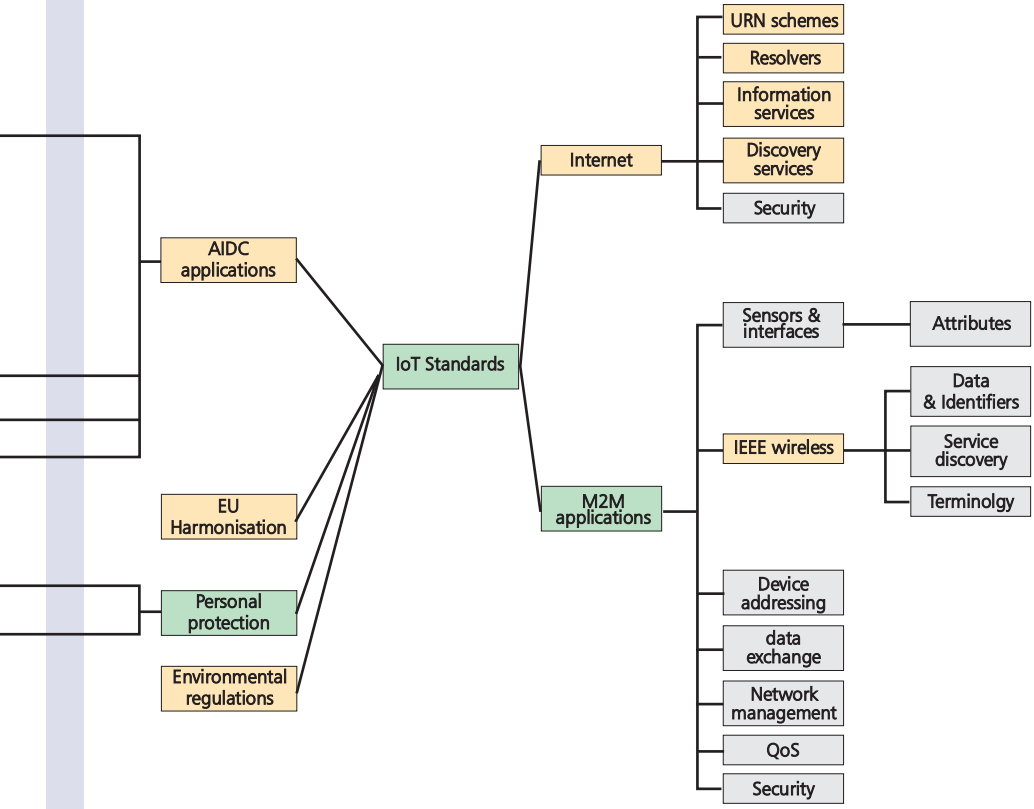


Figure 5: A Mindmap of IoT Standards

For this type of framework model to be really useful, the inter-relationships between topics needs to be shown. Such a framework model might be produced using the CMAP [5] tool, with which we are currently experimenting in CASAGRAS 2 Work Package 6. If the tool proves to be useful, then a working example of it will appear on the IoT standards website.



6. Layered Framework Model

This framework model (Figure 6) uses a layered approach, as used in the GS1 EPC architecture framework as discussed earlier, working from the applications (at the bottom) through to the Internet of Things.

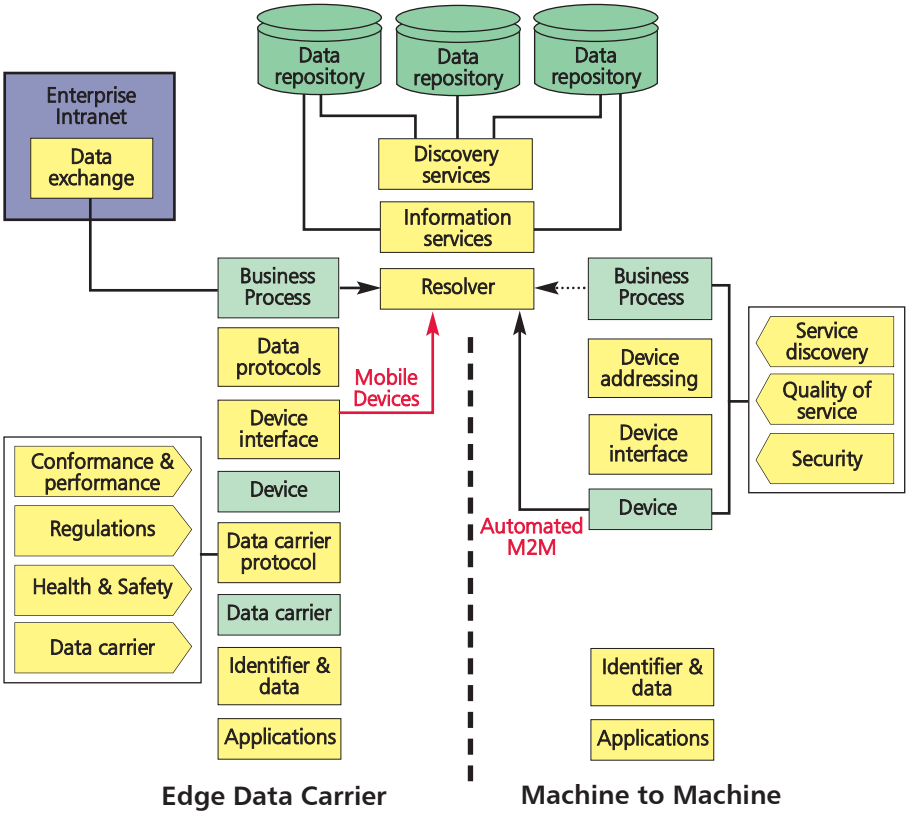


Figure 6: An IoT Standards Layered Framework Model

Because the CASAGRAS 2 project sees a distinct difference between some aspects of the Internet of Things based on edge data carrier technology and those of M2M applications, this framework model shows a horizontal split between these two major approaches. In each of them, a layer can not only be used to represent a number of standards, but it can also represent a number of standardisation categories. As with the GS1 EPC model, the layers follow the same relationship from the edge through to the internet.

One difference is that applications are placed at the bottom, not because this is their logical layer in any of the generally referenced models such as the ISO OSI 7-layer model, but because the specific application determines what identifiers and data are involved with the data capture process. As the Internet of Things is based on edge data carriers, specific application standards determine not only the identifier and data to be used, but also call out which data carriers are permitted to be used to achieve interoperability.

Layered elements

Some of the layered elements in the layer are shown in green to indicate that while these are key components in the structure, they are generally not defined by standards. One such layer is the data carrier. For the edge technologies this could be any of the bar code symbologies, NFC, RF-based identification cards, RFID, and RTLS. This shows that for this structure to be aligned with the mind map, it really needs to be presented in three dimensions.

The data carrier protocol standards also include all the data carriers and their associated reading devices. In this particular structure, the number of standards topics are shown to the left as those have varying degrees of influence on how the data carrier protocol can be implemented. Not all might be relevant to a particular data carrier protocol. For example, the equivalent of the air interface for bar code technology is not subject to any form of regulatory standard.

The device interface standard again varies by technology. The intention here is to show that they are the standardised means for data capture devices to communicate with higher levels and achieve interoperability. The arrow for mobile devices going straight to the resolver is because devices such as mobile phones and tablets have their own means of independently accessing the Internet (of Things).

The data protocol layer is relevant, particularly within the enterprise, for interpreting, processing and filtering this more complex data on the data carrier. Such an example is the EPC ALE standard. Another is the ISO standard for processing data from a sensor attached to an RFID tag.

Business processes, even those that might be standardised, are effectively considered to be out of scope in this framework of Internet of Things

standards. From here , there are two pathways to higher layers. One is to the data exchange, which is either for internal organisation processes or for using more traditional B2B communications such as EDI and XML messages. The other branch assumes a flow through a resolver, which is the doorway to the Internet of Things.

M2M path

In contrast, the machine to machine path whilst having similar components does avoid some of the layers. Although we have shown the device layer as outside the standardisation process but requiring a device interface communication protocol standard, this might vary by technology. In others the device might be the component that is specified and the interface being an API.

Because devices on the M2M architecture are in some form of network, standards for addressing different types of devices are more relevant and probably need to support multiple types of device.

The device topics and addressing protocols are also influenced by another set of standards (shown on the extreme right) covering topics such as service discovery, quality of service and security.

There are two pathways to the resolver. One might be from the business process but, in a true M2M environment, this could be based on direct communication between the device and its associated resolving process.

The common vertical sequence from the resolver upwards, while appearing to be similar, obviously represents some quite fundamental differences in detail. We see the conventional approach of the resolver linking to an information service that, in turn, accesses specific data repositories using standardised information services.

For a fully functional Internet of Things, individual information services need to be logically connected so that the data repositories associated with them can be addressed using discovery services. It seems that standardising this particular topic is proving to be a challenge with edge data carrier applications or M2M applications. However, later in this Chapter under the heading "From Identification to Discovery" we discuss some activity taking place in what might not be considered to be conventional IoT areas such as with Digital Object Identifiers.

7. Conclusion

At the outset of this article, there was a clear indication that it would be difficult to be prescriptive about producing a definitive framework for IoT standardisation. Until there is a clear, unequivocal, understanding of what is meant by the Internet of Things, developing such a standardisation framework might be like walking on an ice flow. However, taking into consideration some existing, more narrowly focused models, it is possible to at least identify the component elements of a framework.

Two models have been considered, each with its limitations. The mindmap model (in Figure 5) makes it extremely difficult to show more complex relationships between the standardisation topics. The hierarchical structure imposed by mindmap tools places some components at a logical distance too far away from where they should be placed. The layered model (in Figure 6) might be a better way to represent the framework, but it too has limitations. It certainly hides entire topics within a layered component, suggesting that there is a requirement either for a 3-dimensional framework or a generic framework being qualified by subsidiary frameworks dealing either with particular technologies or applications.

There is scope for significantly more detailed work to develop a more sophisticated framework. In the meantime, the IoT standards database (http://www.iotstandards.org/) still remains as a repository of standards that are considered to be relevant to the Internet of Things. The taxonomy of that database is such that it can be flexibly re-designed periodically as we develop a better understanding of the Internet of Things and the standardisation requirements.

References

1.http://www.iotstandards.org/sites/default/files/GRIFS%20D1.5%20RFID%20Standardisation%20State%20of%20the%20art_revision%203.pdf

2. http://www.iotstandards.org/

3. RFC 3187: Using International Standard Book Numbers as Uniform Resource Names

4. RFC 5134: A Uniform Resource Name Namespace for the EPCglobal Electronic Product Code (EPC) and Related Standards

5. http://cmap.ihmc.us/

Paul Chartier [paul.chartier@praxisconsultants.co.uk]

Foundations for IoT Governance

By Prof. Anthony Furness

Introduction

> In proposing and developing a framework for governance of the Internet of Things (IoT) it is expedient to consider the nature of governance in general terms. UNESCO defines governance as "the exercise of political, economical and administrative authority in the management of a country's affairs, including citizens' articulation of their interests and exercise of their legal rights and obligations."

Because of the global and societal nature of the IoT it is important to accommodate the elements of general definition for governance in framing a structure for IoT governance. Clearly there is a need to manage appropriate governance affairs, over and above country or state needs, with political, economic and legal underpinning and with appropriate attention to the views and rights of citizens. At a global level the need can be seen for inter-governmental cooperation to accommodate such rights and needs in relation to individual nations and where possible seek harmonisation.

Not surprisingly, privacy, security and ethics, and public consultation, assume significant dimensions within the remit for governance of this kind. That said, there are many aspects of governance structure and capability that are necessary to handle additional content in relation to IoT development and delivery.

An important precursor to specifying a framework for IoT governance is to understand the purpose and structure of the IoT. This has been one of the foci for CASAGRAS2 and its framework provides the basis for establishing an international foundation for Governance and associated legal underpinning.

Foundational Imperatives

Two unequivocal imperatives present themselves as the basis for the Internet of Things (IoT):

1. Integration within the existing and future Internet

2. Interfacing and interaction with the physical world through object- connected technologies and electronically accessible identifiers

They underpin the purpose of the IoT and the framework criteria for distinguishing IoT Applications and Services.

Purpose of Internet of Things - Given the foundational imperatives stated above, the purpose of the IoT may be considered to be 'The exploitation of the existing and future capabilities to interface and interact with physical objects of any kind, animate or inanimate, through automatic identification and object-connected technologies[1] and, through Internet and other computer, communications and network developments, derive and apply applications and services that serve the international economic community, knowledge and wealth creation, and the increased welfare and well being of human kind'.

The generalised nature of the statement allows for future influences of technological change and response to developments that may change the detailed nature of supporting structures and protocols, whilst retaining a cohesive conceptual framework that embodies the vision of an object-focused and responsible use of object-connectivity.

Underpinning for a Statement of Structure - The statement of structure for the IoT, given the above imperatives and statement of purpose, has to be based upon a detailed review of the imperatives, and the implications and opportunities they present. With the Internet being viewed as the core of the IoT development it is clearly important to view the capabilities it presents for linking with the second imperative of interfacing and interacting with the physical world.

In performing such a review it is also important to consider how the second imperative may also relate to new and parallel dimensions in network-of-network developments that could, in principle at least, lead to a bifurcated or multi-faceted Internet-independent or IP-independent structures for the IoT.

The Internet as a vehicle for the IoT – The Internet is generally viewed as a large, heterogeneous collection of interconnected systems that can be used for communication between connected entities [2], comprising:

- Core Internet – Internet Service Provider (ISP) networks
- Edge Internet – Corporate and private networks, often connected via Firewalls, application layer gateways and similar devices

Conventionally, the connected entities within the Internet are computers with human-computer interfacing and, in increasing numbers, computer supported entities such as portable data terminals and embedded data capture and sensor terminals. The former can be seen as a human-to-human platform for IoT distinguished applications and services and the latter to object-to-object and object-to-human platforms for IoT applications and services. Thus, the Internet can be seen to provide an existing platform for IoT development based upon the imperative of interfacing and interacting with the physical world. In order to extend and distinguish the IoT beyond being simply part of the existing Internet it is necessary to determine:

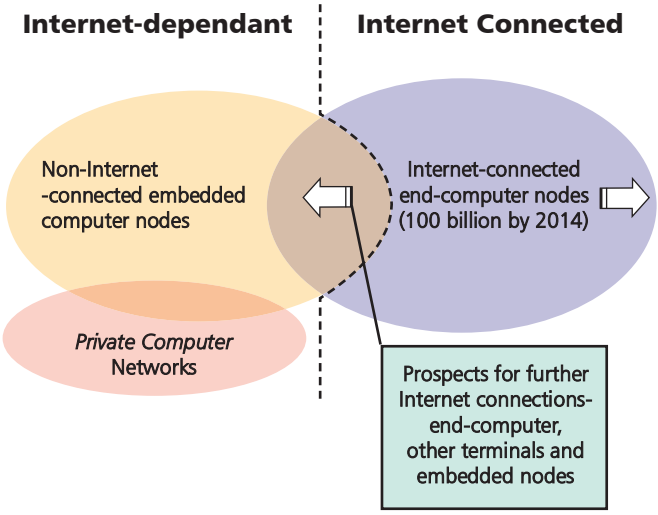
- The extent to which the Internet capability can embrace further computer-based nodes that interface and interact with the physical world.
- The extent and the implications of interfacing further with physical objects of all kinds through object-connected technologies and as a basis for supporting Internet-enabled applications and services.
- The extent to which the Internet application layer components, such as the world wide web, can be exploited and extended to accommodate IoT applications and services.
- The extent to which legacy automatic identification coding can be resolved to link with Internet Protocol (IP) addressing and discovery services.
- The extent to which the existing and future Internet capabilities can support the growth and diversity in IoT communication and transfer needs, commensurate too with needs in performance.
- The extent to which structures will serve activation and control needs within the physical world and accommodate important legacy systems, such as the supervisory control and data acquisition (SCADA) and distributed control systems (DCS) that have served, and continue to serve industry and the needs for automation.
- The extent to which physical identifiers will relate to virtual identifiers and virtual entities.
- The extent to which security, privacy and consumer needs will need to be enhanced to serve new and automatic systems for IoT support.

Clearly, the development of the IoT will need to progress through appropriate collaboration with Internet developers and the associated facilities for Governance. The expectation is that the number of nodes comprising the Internet will grow to well over 100 billion within a short period of time and by 2014 will be supporting some 42 Exabytes (10^{18}) per month of consumer Internet traffic [3].

Non-Internet (IP-independent) Connected Structures in the IoT

Independent, not connected to the Internet, are computer and sensor networks, private and public, that may or may not resort to Internet support or may exist and develop as Internet-independent or IP-independent structures. These structures may also interface and interact with the physical world and so relax the Internet imperative as the only network-of-network requirement for the IoT. The prospect is thus presented for an integrated IP/IP-independent structure [4] for the IoT and even the development of a new network-of-networks comparable with that of the Internet itself and governed by an extended set of principles, possibly more geared to industrial and business needs.

To what extent commercial developments relating to the Smart Cities and other Smart initiatives will influence both IP and IP-independent IoT progression is yet to be seen, but there is clear potential for progression either way.



Such a concept may be further supported in considering the object-connected technologies applied to physical objects that facilitate identification and connection with the Internet and non-Internet network structures through intermediary readers or read-write interrogators offering two-way data transfers. These may be technologies without embedded computers but capable of carrying machine-readable identification codes and offering various levels of functionality dependent upon type. Bar code, two-dimensional code and radio frequency identification (RFID) technologies are representative in this respect.

Adding the object-connected layers and the associated interfacing and interacting with the physical world, and the role of human linkage in structures, a view emerges of a prospective IoT structure that comprises IP and IP-independent components together with physical world intranet structures that have the prospect of linking with either of these components. The facility to accommodate future developments is also seen as a necessity in seeking a statement of IoT structure.

Important areas of legacy

Important areas of object-connected legacy that must be considered in IoT development are the supervisory and data acquisition (SCADA) systems and distributed control systems (DCS). In general terms SCADA systems usually refer to centralised structures which monitor and supervise the control of entire sites, often spread out over large areas, ranging from industrial sites to national support structures.

SCADA solutions often incorporate distributed control system (DCS) components and the use of the standardised control programming language, IEC 61131-3 (a suite of 5 programming languages including Function Block, Ladder, Structured Text, Sequence Function Charts and Instruction List), to create programs which run on remote terminal units (RTUs) and programmable logic controllers (PLCs).

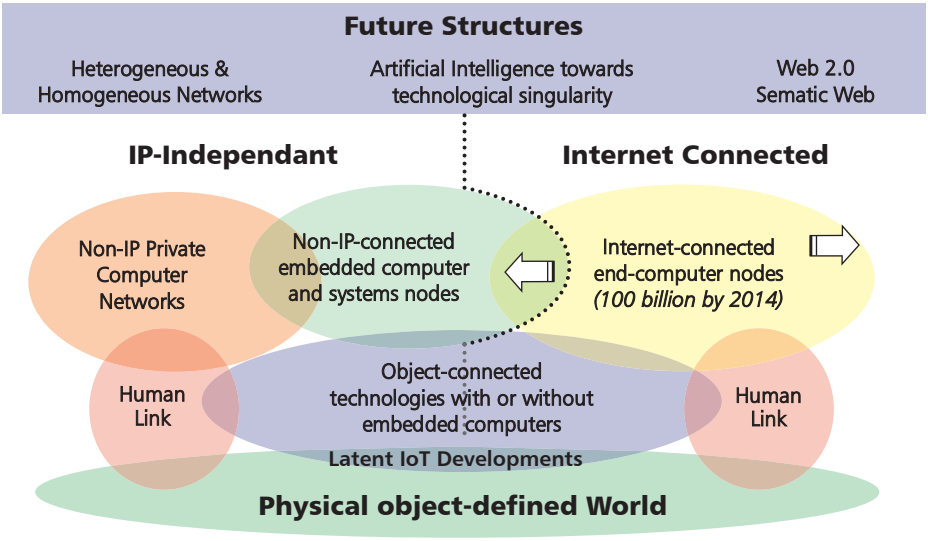
The Internet and wireless communications have clearly had an impact upon SCADA developments, with first generation monolithic systems giving way to second generation distributed systems and now the impact of a third generation of network systems predicated upon the use of IP and TCP based protocols.

Application specific SCADA systems, hosted on remote platforms over the Internet, are now being offered to end users, and thin clients web portals, and web-based products are gaining popularity as a consequence of Internet attributes for easing end-user installation and commissioning requirements. However, there remain concerns over Internet security provisions, reliability of Internet connectivity and latency.

While efforts will be clearly made to accommodate such concerns through Internet development per se other options residing in IP-independent structures may also be developed.

Framework for IoT Structure - While the Internet is taken as an imperative for IoT development, what emerges from the consideration of the Internet together with the imperative for physical world interfacing and interaction, is a prospect for both Internet and Internet-independent (or IP-independent) IoT developments. It has also raised the prospect of what may be described as Latent IoT developments, developments that initially have no link with Internet of IP-independent network of network structures but could well be linked in some way at a future date. Many automatic identification and data capture (AIDC) applications fit into this category of structure. Examples may also be seen to be arising from European IoT projects.

This schematic is an attempt to represent the holistic tri-state structure being here proposed for the IoT.



Overlap of ellipses in the above graphic signifies a combination of features, such as Internet connected computers linked to object-connected technologies on the right and private networks linked to embedded systems and object-connected technologies by overlaps on the left. Given appropriate quantitative data these ellipses and their overlaps could represent numbers of corresponding nodes. As indicated, without quantification, they simply signify, qualitatively the nature of such nodes.

Characterising Applications and Services - With prospective IoT structures partitioned into Internet, IP-independent and Latent IoT sectors of development, the prospect may also be seen for characterising applications and services in accordance with these sectors and subsequently into sub-sectors determined by the architectures and capabilities of the sector components. In the case of Internet structures this includes the capabilities offered by the networking and communication structures, generic top level domains and the Internet protocol stack (see below - Exploiting the Internet Component for IoT Applications and Services).

Statement of Structure for the Internet of Things - Based upon the consideration of imperatives so far, and the view that emerges, a statement of structure can be proposed that takes the following form:

> **''An integrated, internationally agreed and standards-supported network, communications, interface and actuation structure that exploits the existing and future Internet, existing and future, fixed and mobile telecommunications systems, existing and future object-connected technologies, coupled prospectively with non-IP private networks and associated communication, interface and actuation structures, organised to facilitate development of application and service layers specific to physical world, object-oriented needs and opportunities relating to the identified purpose for the Internet of Things'.**

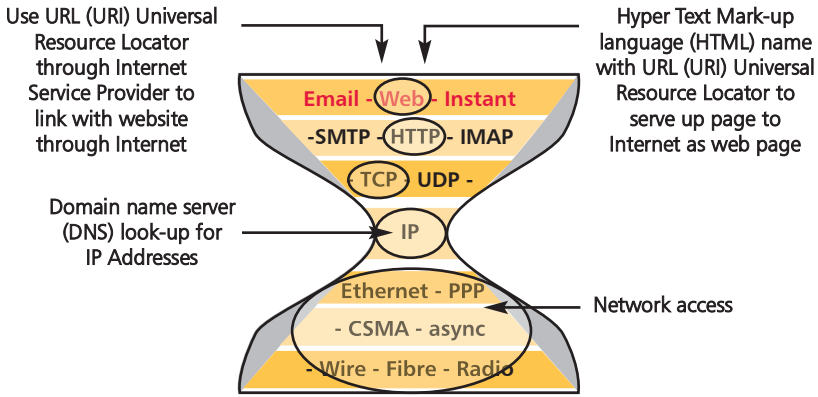
As with the statement of Purpose this too is a generalised statement directed at providing a flexible and extendable frame of reference to allow for change and technological developments. In contrast to definitions (although the differences may be slight) the platform for statement allows for further description and explanation of terms. For example object-connected technologies, may be described as those technologies that are intrinsic to, embedded-in, attached-to, accompany or are associated with tangible physical

entities of any kind and facilitate identification of the objects concerned together with other data capture and actuation functionality as appropriate for interfacing and interaction with the objects and as appropriate the environment in which they are situated. Automatic data capture, sensing, positioning and communication technologies are representative in this respect.

The platform for statement also allows for international input and consensus.

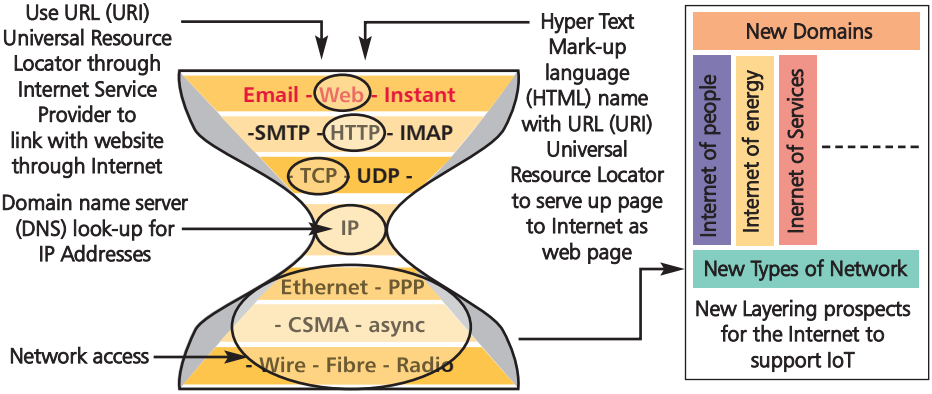
While the consideration of imperatives may be viewed as somewhat simplistic it does point to the clear prospect of a partitioning of contributory elements to the Internet of Things and a platform for considering application area layering with attendant consideration of area needs.

Exploiting the Internet Component for IoT Applications and Services – The Internet provides a protocol stack, on top of which is a 'generic' application layer. The world wide web (www or Web) is generally considered the most prominent of applications presented in this layer, with e-mail and messaging constituting further applications at this level. Applications and services that interface and interact further with the physical world can be expected to exploit these facilities and the associated Internet protocol stack and the Internet Protocol (IP) addressing (IPv4 and IPv6).



While different combinations of protocols from this stack and the generic application layer may be selected to support different domain level applications the prospect may be seen for other protocols and domain level

applications specifically developed for IoT purposes, including for example generic top-level domains for IoT. Layered application areas may be considered in this way to accommodate new Internet concepts such as those being proposed for Internet of People, Energy, Services and so forth; not as separate Internets but layered upon the Internet of Things and facilitated in part through developments in interfacing and interactions with the physical world. The question therefore arises as to whether the existing Internet structure can accommodate such developments both in terms of functionality and performance. By exploiting the generic domain principle the differing architectural needs could conceivably be accommodated through the domain providers and the responsibilities they would have in maintaining such domains. The question then arises as to the economic feasibility for such structures.



Along with these prospective developments may be seen the prospect for additional network types and associated access. Irrespectively, all such prospects will clearly require the cooperation of the Internet developers, such as the Internet Engineering Task Force (IETF) and the associated Governance bodies.

Resolving identifiers across the Internet – More than a prospect is the need to accommodate legacy numbering and identification systems, such as the GS1 numbering systems, electronic product code (EPC) and uCode and the various object identifiers (OIDs) and associated unique item identifiers (UIIs) within the IoT. This is because they are specifically concerned with identifying physical entities.

In many ways the GS1 and EPC constitute a special case being essentially proprietary codes for which GS1 and EPCGlobal have developed their own products and protocols and contributed to international standards to handle Internet-based applications. Other identifiers and their resolution requirements are part of the on-going CASAGRAS2 resolver developments.

Data carrier and transfer principles – The interfacing and interaction features of the IoT will exploit the object-connected technologies and the identification and carrier principles characterised by the body of knowledge and experience collectively known as automatic identification ad data capture (AIDC). This very important, extensive and growing body of knowledge has never been effectively introduced into main stream information and communications technology (ICT) curricula, yet constitutes a foundational underpinning for physical world interfacing and interaction. It can also be seen as a foundational underpinning for the IoT applications and services design and should be developed accordingly.

Very significant in this underpinning are the principles of identifying, carrying, caching and transferring data or information to meet particular application needs in a more flexible manner. Too often assumptions are made that the IoT will simply identify objects by numbers and through these numbers deliver data or link to information stored elsewhere and accessed via the Internet. AIDC and the broader base of object-connected ICT offers other options to practical data carrier, transfer, processing and storage that can enrich the capabilities of application solutions and ease the inevitable problems associated with connectivity and Internet traffic.[5] So too with applications requiring response and actuation wherein an Internet connection may not be a necessity, and may even constitute a hazard where safety and business-critical issues are concerned.

Communication Networks – The whole issue of Internet traffic is being brought into sharp focus by the growth in video streaming largely generated by social networking, content-rich sites such as YouTube and the on-demand services providing TV entertainment. From an IoT standpoint the situation may be further exacerbated by the edge-defined data streams and cloud-based developments. To what extent such developments will compare with video traffic is yet to be seen. However, the need can be seen for pre-empting capacity, latency and other network needs with respect to other data-intensive developments.

The success of cloud-based initiatives would appear to hinge on the use of public wide area networks (WANs), but with attendant concerns over entrusting data to external agencies, associated privacy and security, and growing demands on public network bandwidth. In addressing these concerns attention is being directed at contracting issues and trust, enhanced security, and performance enhancement opportunities such as WAN optimisation and effective use of caching in relation to Web servers, browsers and edge-defined functionality of networks.

The issue of 'private clouds' has also been muted where a shared private network infrastructure is advocated as a means of resolving some of the security issues through single firewall control. While such an approach may be considered fine in theory the practical challenge of providing a cost and beneficially effective solution may point to a hybrid or virtual solution where there is further consideration of security needs, shared resources and automation.

Such issues are illustrative of the networking considerations to be addressed in developing the IoT, and prospective partitioning of Internet and IP-independent areas of development.

Underpinning principles of Object-connected ICT and IoT applications and services design - In parallel with any development in the IoT must be a parallel positioning and development of object-connected ICT within mainstream ICT curricula.

While statements of purpose and structure may be derived in this way, the global nature of the IoT demands that they be considered, and as necessary modified to accommodate perspectives derived through international cooperation and collaboration, as points of reference in deriving a framework for IoT Governance.

Having considered the nature of purpose and structure for the IoT it is important to consider the nature and role of Internet governance, followed by the considerations of governance that go beyond those currently being accommodated by Internet governance. This is also required to facilitate a contribution to Internet development per se and to structure an appropriate strategy for collaboration with Internet governance bodies.

It is therefore important to review the aspects of governance for the Internet and the critical resources that underpin the success and continued success of the Internet.

Internet Governance and Critical resources for Future Internet and IoT

A significant foundation for the review of Internet governance is the report prepared by the Council of Europe Secretariat entitled, "Internet governance and critical internet resources" [6].

Based upon this report three important areas of consideration can be distinguished, which in turn may form the framework for a more in-depth study of the respective issues and how they may relate to the international framework for structure and governance of the IoT:

1. Evolutionary considerations
2. Critical Infrastructure
3. Protection in international law

In each case there is a need to consider the implications of IoT development in relation to the Internet and Internet-independent networks and with respect to the object-technology base that will facilitate the very important functions of interfacing and interacting with the physical world as well as providing foundational components for applications and services in their own rights, seen as independent or latent IoT. Critical infrastructure constitutes a substantially expanded area of consideration when viewed in relation to the object-connected, object-associated technologies that comprise the foundational components for interfacing and interacting with the physical world.

Evolutionary considerations - The Internet is essentially viewed as a large, heterogeneous collection of interconnected systems that can be used for communication between connected entities [7] . It has evolved over a period of some years to the point where its ubiquity and facility to impact beneficially upon all aspects of business and domestic life is imposing a critical reliance upon Internet resources and their sustainability. Stability, security and on-going functionality depend upon these resources and how effectively they are managed. Currently these resources, including root name servers, the Domain Name System (DNS), backbone structures and Internet Protocols, are managed by separate agencies and without any apparent overall approach to governance.

However, the need for governance is well recognised and a number of Internet-related agencies, although specific in their individual remits, contribute to governance activity. These agencies include [8] :

- Internet Engineering Task Force (IETF) – Protocol engineering & development
- Internet Architecture Board (IAB) – Overall architecture and advisory body
- Internet Engineering Steering Group ((IESG) – Technical management of IETF and Internet standards process
- Internet Society (ISOC) - Non-government, international professional membership body – standards, education and policy
- Internet Corporation for Assigned Names and Numbers (ICANN) – Responsibility for IP address space allocation, protocol parameter assignment, domain name system management and root server system management functions
- Internet Research Task Force (IRTF) – Promote Internet researchWorld Wide Web Consortium (W3C) – To develop common protocols that promote Web development and interoperability

Additional to this list is the Internet Commerce Association (ICA) which, in recent months, has been active in criticising the US Department of Commerce (DOC) over a letter to ICANN's Government Advisory Committee (GAC) regarding provisions concerning new generic top level domains (gTLDs). The nature of the DOC disagreements concerning the gTLD provisions has raised an important issue over the future of gTLDs. "If ICANN's Board were to acquiesce to the positions advanced by the DOC it would not only mark the end of a new gTLD program that envisions an unlimited number of applications and approvals, but the practical end of ICANN as a private sector-led entity in which policy is developed through a bottom-up consensus process" [9] . It would seem that the US government is proposing to convert ICANN into an organisation in which the GAC (which exercises oversight over the ICANN process for developing new gTLD rules) would move from advisory role to a supervisory role with the power of exercising ultimate veto over any new policies being considered by ICANN [10]. This clearly has implications for the Internet development and the development of an Internet-dependent IoT, not only in respect of domains but also in respect of international governance.

Hinging upon an appropriate domain structuring and governance are a number of primary and burgeoning evolutionary constructs:

1. Internet of Things (IoT) – for which this framework proposal is a strategic component in helping to identify a coherent structure for IoT development.

2. Social Networks and the manifestation of an Internet of Services – exploiting developments towards an increasingly participative Web (Web 2.0), enhanced automation and the Semantic Web. Each of these developments, particularly automation and the Semantic Web, may be seen to have relevance and positioning with respect to the IoT.

3. Technological and Media Convergence onto the Internet – wherein telephone, television and video technologies are converging onto the Internet, at content level developments in respect of video-on-demand and television over Internet Protocol networks (IPTV) and at the business and service level integration of Internet, television and telephone services. relevance can be seen in each of these areas with respect to the IoT.

4. Mobile access technologies – exploiting the increasing range of portable Internet access-supported devices, such as mobile telephones, portable televisions, personal digital assistants (PDAs), portable computers, GPS-supported devices and gaming consoles. Such devices may be considered an integral part of the object-connected or associated edge technologies for supporting IoT applications and services.

5. Data Transfer Technologies – responding to the predicted increase in demand in Internet services and associated needs in respect of speed, volume and reliability of data traffic over the net, recognising the potential impact that convergence, mobility and the IoT will have in relation to data traffic and associated architectural needs.

As the Internet evolves still further, with the expectation of escalating growth in connectivity, complexity in structures, technological developments and attendant risks in respect of privacy, security and safety, the need is being seen for more formalised governance, with protection of Internet values and standards on democracy, law and human rights viewed as a priority .[11]

Critical Infrastructure

As far as the Internet is concerned there are a number of critical resources that define the existing infrastructure and areas of consideration for its development. They comprise : [12]

Root servers – essential part of the architecture for providing a stable and secure globally operable Internet, wherein 12 operators running 13 root servers service the underlying domain name system, provide an authoritative directory for ensuring Internet services, answering well over 100,000 queries per second, and take responsibility to maintain adequate hardware, software, network and other associated resources. Presently, the root server operations are performed without any formal relationship with any authority. They have no clearly defined responsibilities and accountability, especially in relation to stability and secure functioning of the Internet. The current geographical distribution of root servers is uneven which in consequence raises issues of significant degraded performance within the area concerned should one of them fail.

Backbone structures – comprising the many different large network structures that are interconnected and serviced by backbone providers, often by individual Internet Service Providers (ISPs). These providers generally supply and handle connection facilities in many cities and are themselves connected to other backbone providers through Internet Exchange Points (IXPs). Only 79 countries around the world have operational IXPs, yet their importance will grow as critical infrastructure as Internet data traffic increases and traditionally-based analogue services are digitised. The IXPs are essentially governed through a mutually-owned membership organisation.

Broadband access – is seen as an important communications enabling technology of international significance in supporting the growth of Internet connections and in promoting developments towards faster access and lower costs of access, both fixed and mobile. Presently there are substantial differences in broadband access among different countries with many factors influencing the take-up and use of broadband which if sustained will create a greater digital divide and prospective information exclusion through lack of access facility. For the future Internet and associated developments broadband may thus be seen a critical resource

requiring governments around the world to strengthen still further their programmes for high-speed broadband network proliferation.

Network neutrality – with a move towards bundling of television and Internet services with fixed and mobile telephony, concerns are arising over preserving neutrality as it evolves. With associated developments in traffic management techniques there are concerns over anti-competitive practices predicated upon unfairly slowing, prioritising traffic flows and even blocking data flows. Currently, few countries around the world have in place regulations to ensure that access providers exercise a duty to provide neutrality.

Internet system for names and numbering – constitutes a critical resource in respect of Internet Protocol address space allocation, protocol identifier assignment, country code and generic Top Level Domain (ccTLD & gTLD) name system management and root server functions. The resource is effectively governed by ICANN.

As the Internet develops to accommodate the IoT requirements there will be a need to accommodate legacy numbering and identification systems, such as the GS1 numbering systems, electronic product code (EPC) and uCode and the various object identifiers (OIDs) and associated unique item identifiers (UIIs).

Manifest as the Internet these infrastructural components need to be protected in order to ensure security, stability and effective exploitation as a global resource comparable with other global resources such as water and energy [13]. As with other resources the Internet is subject to accidents and incidents that compromise capability and must therefore be protected against such accidents and incidents, and appropriate to user needs and human rights. Similarly, the IoT will reveal other infrastructural components that will also require protection, particularly in respect to autonomous and self-functionality, such as self-diagnosis, self-repair and self-defence against infrastructural attacks.

Protection in international law

In recognising the Internet as a critical resource there is an intrinsic need to protect the resource in much the same way that other critical resources may be protected. Being an international resource it also follows that it requires an international cooperative approach to protection using

international law. The protection is in part grounded in accountability which in turn requires a legal framework for providing regulations and sanctions to handle non-compliance with accountability requirements.

The nature of the entities for protection that is required relate to:

Technical risks, to both accidental and intentional incidents resulting in damage to the infrastructure of the Internet or detrimental trans-boundary effects upon the Internet.

Cyber attacks, characterised by deliberate attempts to disrupt or damage Internet functions, services and applications.

Inter-state conflict, characterised by issues arising during times of crisis in terms of stability and security within a country relating to important resources. While protection can be seen as a requirement under such circumstances it is likely that this will not be ensured through international law. Consequently, other measures are almost certainly required to facilitate protection in those situations in which conflict cannot be resolved through process of law.

These issues are not mutually exclusive and each have a bearing upon the stability, security and safety of the IoT as well as the Internet per se, potentially to the extent that additional protection measures may be required.

In all these areas concerning the Internet and Internet governance and their relevance to IoT there is a need to delve more deeply into their nature and possible impact upon the governance of the IoT. The critical resources that characterise the Internet must be borne in mind in pursuing the proposed staged approach to structuring a framework for IoT Structure and Governance.

Moving beyond the bounds of today's Internet Governance

Because of the IoT imperative for interfacing and interacting with the physical world there will be aspects of critical infrastructure that arguably go beyond the bounds of what is considered Internet governance, particularly in relation to:

- Implementation, maintenance and development of the IoT physical world infrastructure (Internet linked or Internet-independent) characterised by object-connected and other edge-technologies that are used to interface and interact with physical world entitiesand systems, including wireless sensor networks and control systems.
- Environmental disruption and impact associated with deployment and maintenance of fixed position IoT object-connected devices, systems and networks, and the end-of-life recycling or disposal of devices, systems and networks; exacerbated by an expected exponential growth in use of object-connected and other edge-technology devices.
- Environmental and societal impact of mobile devices and fixed in-mobile devices and networks such as in-car engine and other management systems.
- Attendant implications of extensive populations of object-connected and integrated system devices and networks with respect to functionality, reliability, safety and responsible deployment and use of such devices and networks.
- Energy and materials conservation including the control and recycling of object-connected and other physical edge-technology e-waste.
- Privacy (including corporate privacy) and security associated with object-connected data or information contained in object-connected and other edge-technology devices, additional to those characterised by radio frequency identification (RFID) and including optical-based data carriers, smart card devices, mobile phones, tablet media devices and so forth.
- Privacy (including corporate privacy) and security of communications between object-connected and other edge-technology devices and data transfer systems.
- Security of infrastructure, applications and services, particularly in relation to autonomous systems communications and functionality where current Internet capabilities may be viewed as inadequate.
- Functionality and performance demands in relation to physical world interaction that may be beyond the capabilities of existing

- Internet support, particularly where critical safety and critical business functions may be put at risk and where latencies, delays, loss of synchronisation and issues of temporal decomposition may impose problems.
- Accommodation of Internet-independent network and communication structures and prospects of new infrastructural developments that are IP-independent and exploiting the physical world interfacing and interaction capabilities of object-connected and other edge-technologies.
- Standards and regulatory recognition and developments to accommodate the broader based vision of the IoT and its significant object-connected and other edge-technology base.

Ethical and issues of responsible usage of resources will also need to be addressed in the governance arena. The often promoted notion of every object being connected to the IoT is not only ludicrous but irresponsible in principle. Only objects that need to be connected should be connected and ostensibly only when required to be connected. Unnecessary object connectivity must clearly be seen as a drain on material resources and energy, particularly if numbers are of an astronomical scale.

Legal Perspectives on the Internet of Things -[14] addresses a number of the legal aspects relating to the IoT and provides a set of foundational considerations for Governance of the Internet of Things. A general approach to the legal framework suggests a self-regulating structure using soft law and a model for social protection controls and an international legal framework based upon global and regional legislator representation and substantive international principles. Strong attention to privacy and security is advocated within this legal framework.

A structure is proposed in the publication for governance of the IoT with attention to establishing a Governance Structure, together with considerations for legitimacy and inclusion of stakeholders, transparency, accountability and allocation of critical resources. However, it is referenced to a model of the IoT that is largely predicated upon RFID and EPC with the Global Legislator, EPCglobal, ICANN and the International Telecommunications Union being identified as the only bodies subject to governing principles. By recasting the model to a more inclusive one the principles can be readily applied to define a more inclusive Governing Structure.

As far as the content for governance is concerned there is the need to consider what is significant for IoT in relation to technical, policy, economic, institutional and legal matters, and with initial reference to the recommendations from CASAGRAS1.

Drawing upon the recommendations of CASAGRAS1 - The Internet itself continues to need the guidance and direction of the IGF and through its deliberations will impact the conceptual approach that governments will take concerning the evolution of the Internet. Governments will invariably draw upon the IGF concepts in developing policy, law and controls within their jurisdiction. It is therefore reasonable that they will also draw upon such concepts in seeking a governance platform for the Internet of Things. This may be considered even more so when viewing the Internet of Things as integration with the existing and evolving Internet. The global nature of the exercise demands an international, IGF-linked, platform structuring governance platform for the IoT.

A range of issues will need to be accommodated in realising such a platform. The European Commission consultation process on RFID revealed that 86% of respondents supported the need for a "governance model that is built on transparent, fair and non-discriminatory international principles, free of commercial interest".

While the core of the Internet, the governance structure, has not been subject to legislation, countries around the world, and within Europe, have introduced laws to ensure that Internet usage does not conflict with national laws and international rights and conforms to the norms and values of societies in general.

Issues of legislation will undoubtedly arise with respect to the IoT, particularly where concerns arise that are of a privacy and security nature.

With respect to RFID, concerns have been expressed over openness and neutrality of database structure that are used to hold unique identifiers. This is also of direct relevance to the IoT and global coding. Ethical and secure systems management is required with processes that are interoperable and non-discriminatory .[15]

These considerations provide lessons for considering the governance requirements for the IoT.

With the scale that data traffic is being proposed for the IoT and the associated prospect of an emerging federated service infrastructure that

could possibly emulate the growth potential of the world wide web, public policy issues are likely to present significant governance considerations for which no one country could be seen to have authority. Social and economic dependence points to the need for a regional based approach[16]. Benhamou[17] views the IoT as an emergent critical resource and advocates the need for different countries and regions to progress work on different options to meet the governance needs.

In view of the latent requirement for integrating the IoT with that of the Internet it is important that proposals for governance and other issues are considered in cooperation with relevant authorities and organisations involved with parallel developments of the Internet. Within Europe the European Future Internet Assembly is an example of such an organisation in which one of its aims is to develop the tools and approaches harnessing the potential of the IoT.

A further aspect of governance requiring attention is the need to consider whether a registration authority is required for identifiers and the management of a global scheme for resolving them.

All this begs the question as to whether the IoT should be governed separately from the Internet or as part of the Internet governance. The logic and the existing Internet Governance framework suggest that it should be an integral part of Internet governance. However, the needs for governance and how they may differ from the issues for the Internet demand further research and consideration.

Given the nature and status of these disparate considerations the obvious recommendations in respect of governance for the IoT, as far as the recommendations of CASAGRAS 1 are concerned, are:

- To establish an international IoT Development and Governance Forum that can influence Internet Governance and undertake rapid research into the issues for ensuring and agreeing appropriate and effective governance, including the revenue and registration schemes that will be needed and the political framework that will be necessary to facilitate appropriate international collaboration.
- Agree an initial federated structure for the IoT and initiate an international programme of application and services development.

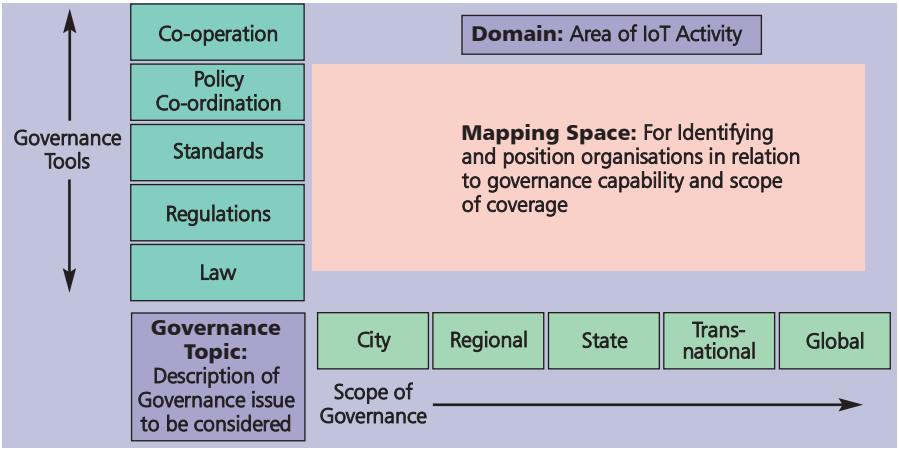
In view of the multi-dimensional nature of the governance issues the need may be seen for an overarching programme of research and development

geared to accommodating all the necessary socio-economic, business and technical dimensions, including the protection of such a network against attack and abuse.

Scope and Tools for IoT Governance

The global nature of IoT naturally prescribes an international scope to the reach of IoT governance, but with the provision to influence governance matters with respect to global, trans-national, state, regional and even down to city governance levels. The broader physical and socio-economic implications of IoT over existing Internet interaction with physical systems point to this need.

A basic model provided by MacLean [18], and subsequently modified through the CASAGRAS2/IERC workshop on IoT Governance, effectively covers broad to narrow scope of international governance, as depicted in the schematic presented here. It also presents the range of tools that can be effectively used in governance, ranging from cooperation soft tools, to hard regulatory and legal tools. It is also useful for positioning organisations in respect of these two dimensions. The model may be used as part of a methodology for management of governance issues.



As a template for considering and planning the management of governance issues the model allows an issue (Titled in the Domain box) to be defined (Governance Topic box) and supported by linked information gathered and retained in associated databases. Participants in dealing with the issue identified are declared in the Mapping Space along with their coverage of scope and tools, along with links to appropriate information. By taking this harmonised approach governance issues may be handled, recorded and used to assist in on-going governance through appropriate comparisons and shared attributes.

Clearly, as far as the IoT is concerned the required tools for governance must embrace the needs in respect of cooperation, policy, coordination, standards and laws and regulations. So too in respect of scope and the need to embrace exchange of services and products, use of common resources, development of technologies, networks and services, and applications for equitable, sustainable global development. Ideally, for a global legislator for IoT, the organisation concerned should fill the mapping space. In the absence of such an organisation the prospect may be seen for strong linkage with the IETF and possibly with the WTO. These are essentially matters to be decided by an IoT governance task force with appropriate international representation.

Global Issues, IoT and Governance

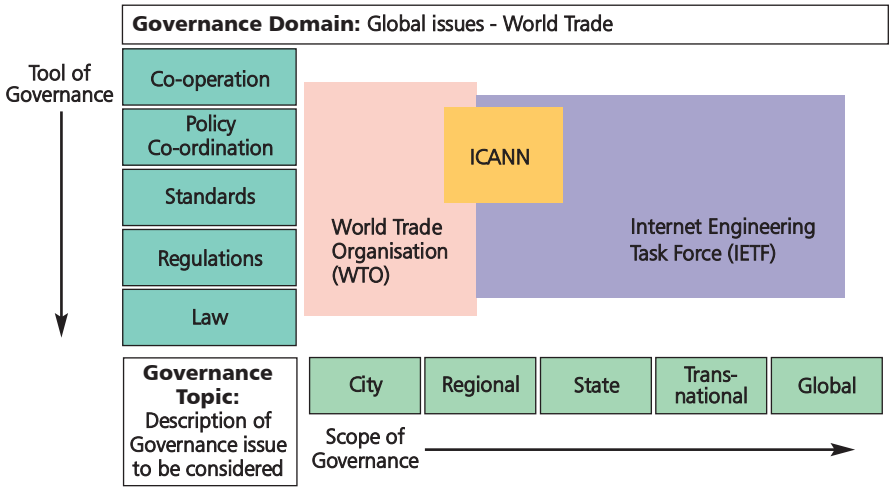
Despite the considerable investments that have already been made in Europe, there is still a significant degree of fussiness and fragmentation associated with developments that are being viewed as 'Internet of Things' (IoT). Presently, there seems to be more emphasis on islands of application and value propositions which may exhibit technological innovation and demonstrate economic benefit but do little to contribute to a coherent framework for standards and governance supported development of the IoT. One worry is that disparate incidental developments of this kind could also precipitate problems of interoperability and contention that could also compromise the potential for contributory developments and lead to market driven monopolies with unintended negative political, economic, commercial and social effects (Santucci G 2011) [19] . Governance may be viewed as a vehicle for avoiding or mediating such problems, particularly where specific areas of application have global significance.

In considering the dimensions for supporting IoT governance in terms of tools and coverage or scope it is useful to address the model presented by MacLean [20] in respect of legal quality of regulations (soft to hard law) and the scope of international governance (narrow to broad) as depicted in the following schematic. It is also useful for positioning organisations in respect of these dimensions.

As a precursor for formalised IoT governance it is possible to consider cooperation in relation to the full scope of governance. This should commence by addressing issues of cooperation with respect to global developments and with the aim of not only influencing organisations depicted in the model but seeking to identify and influence other organisations that will have impact upon IoT development and governance, including the European Commission.

It is envisaged that future workshops on governance will see a move to other aspects of scope, including:

- Development of technology, networks, services in all countries
- Use of common resources
- Exchange of services & products between sovereign nations
- Applications for equitable, sustainable global development



The 'mapping' space on this schematic simply depicts three organisations and their relative coverage of the dimensional elements, with the World Trade Organisation covering most of the governance tools in relation to

exchange of services and products between sovereign states, whereas the IETF covers policy coordination and standards with respect to broader aspects of governance.

Viewed in respect to its most inclusive interaction with the physical world, Internet and associated networked structures, the IoT can be seen to offer significant opportunities for supporting a range of global developments, in which governance can also be seen to have a strategic role to play. Notably these areas of development include:

- Securing Sustainable Food
- Securing Sustainable Water Supplies
- Healthcare, Nutrition and Wellbeing
- Social Mediation, Capital and Persuasion
- Energy Conservation, Production and Distribution
- Sustainable Economy and Management of Resources
- Sustainable Agriculture and Precision Integrated Farming
- Climate Change and Environmental Protection
- Disaster Prediction, Management and Prevention
- Global Trade and Anti-counterfeiting
- Law and Order and Forensics
- Standards and Regulations
- Data Protection and Privacy

The list is not exhaustive and while such topics may be viewed as potential content for IoT Governance, with actual content to be determined by the appropriate governing body, the argument may be levelled for consideration and debate as a precursor to the realisation of IoT Governance in practice and a useful source of opinion for a practicing Governance body to address.

With this prospect in mind a series of area-specific workshops is proposed that could bring together experts in the areas of application or issues identified with experts in dealing with the principles and practice of governance. While Standards and Regulations are seen as topics in this series it is also seen as an important element in each of the topics identified.

Consequently, it is seen as important that standardisation bodies are appropriately represented in these workshops.

The aims of these workshops are:

- To identify and bring into sharp relief issues of global significance in which the IoT can be seen to offer a profound foundation for development and in relation to which governance can also be seen to have a strategic and highly beneficial role to play.
- To deliver initial face-to-face workshops in which experts in IoT development, governance and the subject or issue concerned are brought together to facilitate a subject-specific platform for supporting IoT governance needs and IoT development.
- To deliver a workshop report that summarises the key elements and recommendations in relation to IoT prospective governance in areas concerned.
- To establish through the workshop delivery a voluntary, international group for ongoing considerations within the area concerned and as a basis to advising an IoT Governance body on governance issues once it is formed.

Such groups may also constitute a group for stimulating research in areas concerned and for contributing to annual events, such as conferences, on IoT development and with particular reference to governance and, very importantly contributing to the identification standardisation needs and on-going development of standards.

Each workshop will be high profile, appropriately focused and supported by informed documentation and leadership support in delivering target outcomes in accordance with declared objectives.

Each workshop would require an incisive foundational document to be drafted that distinguishes the importance of the subject or issue concerned, the role that IoT is having or is expected to have and the role that governance would play in strengthening its impact as a globally relevant development.

Taking Food Security as an example the following summary provides insight into the importance of food provision and distribution from a global perspective, the importance of IoT and precision farming in addressing these requirements, whilst also attending to the needs of energy conservation, environmental protection and climate change.

Illustrative example of approach

IoT Governance in Securing Future Food Production and Distribution

The world population is increasing rapidly. The Food and Agriculture Organisation of the United Nations estimate that by 2050 the population will have increased by 35% to a staggering 9.1 billion, compared with 6.7 billion in 2008[21]. The demands for food, including food proteins in the form of meat [22], will rise accordingly. These increases in population and demands for food pose major challenges for securing future food production. Added to these challenges are challenges for considering environmental and global climate change in relation to food production needs and issues of nutrition. A recent study[23] claims that:

> **"Increasing population and consumption are placing unprecedented demands on agriculture and natural resources. Today, approximately a billion people are chronically malnourished while our agricultural systems are concurrently degrading land, water, biodiversity and climate on a global scale. To meet the world's future food security and sustainability needs, food production must grow substantially while, at the same time, agriculture's environmental footprint must shrink dramatically ."**

The outcome of this study has formed the basis for a five-step global plan [24] that could double food production by 2050 while greatly reducing environmental damage. The five steps presented in this global plan are:

1. Controlling the agricultural footprint
2. Improving the yields of existing farmland
3. More effective and efficient use of resources
4. Shifting diets away from meat
5. Reduction in food wastage

Improvements in conventional farming are required to reduce adverse impact on the local and global environment, to achieve better efficiencies per unit input of resource, to achieve better ecological (holistic)

management, and to find a better correspondence between food demands and supply, both locally and globally. The advancement of precision farming (PF) as a discipline for developing physical science-based tools and practices that provide interventions to improve farm productivity is fundamental to tackling these challenges.

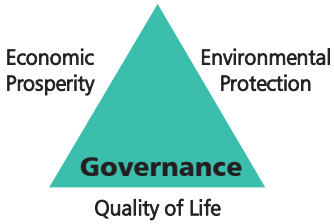
Equally significant is the role that the Internet of Things (IoT) and governance could play in meeting these challenges on a global basis, particularly in respect of the five step approach, with perhaps a sixth dealing with issues of distribution.

An international workshop would, in each case, place particular emphasis on how the IoT could assist in meeting the challenges, the role that governance could take in realising effective implementation and the need for national and international standards in such developments:

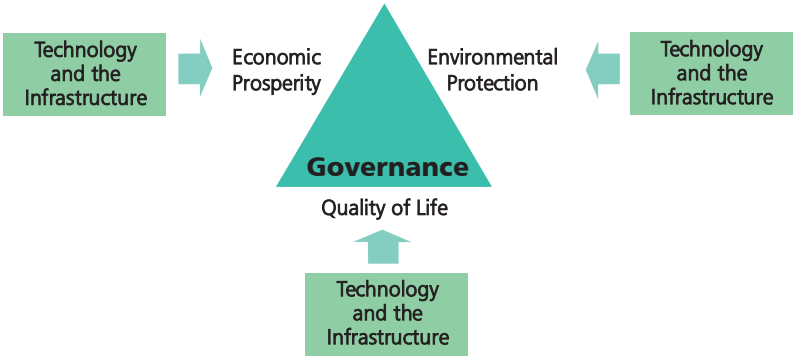
Linking IoT Governance to Smart City developments

An important manifestation of IoT development will be in the realisation of 'Smart' cities. Such developments are inevitable, with growth in city populations (with the tipping point in urbanisation being reached in 2009)[25] and developments already being seen through the roll out of broadband to the community and applications exploiting mobile communications. To exploit the digital capability to the full, bearing in mind too the continuingly changing landscape for digital products and innovation, it is important to take a strategic approach to the design and realization of smart city infrastructure. It is also important to align such an inclusive model and 'smart' developments with a well-founded socio-economic and governance paradigm for city development. Such a paradigm is to be found in the Hazel model.[26]

The Hazel report, which focused upon the infrastructure of megacities – cities that account for a disproportionately high share of national economic growth and generate a significant percentage of global gross domestic product (GDP), was based upon a survey of 525 city leaders (politicians and decision makers). It yielded a theory of city governance predicated upon three commanding considerations; quality of life, economic prosperity, and environmental protection.



City Governance, through the Hazel report, was seen as the means of balancing these three functional goals. Such a model has significant links to infrastructural developments that exploit technology for achieving socio-economic goals. Such a model may also be argued to have significance with respect to smaller city complexes and city regions in providing a governing oversight with respect to technological intervention with respect to infrastructure, and its potential with respect to economic power, interlinking with the global economy and attraction for investment. Technology can and will impact on all aspects of city infrastructure and with outcomes determined by the governance model.



In the drive towards smart digital cities there will be an inevitable social backlash, pointing to the limitations and detrimental impact that such change can engender. Where personal identification and data is concerned there is often fear of the unknown. Appropriate design and protection measures, derived under appropriate governance, can allay such fears. Without such protection measures we would not now be exploiting the ubiquity of smart cards and other carriers of personal identity and activities such as on-line financial transactions; protection that will be enhanced as further technological measures are introduced to combat identity theft.

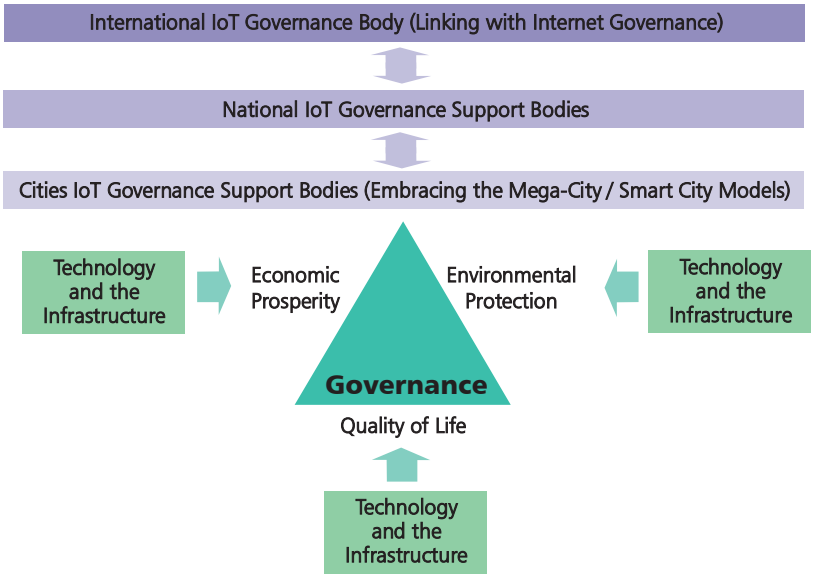
Putting aside for the moment the social issues, the concept for an inclusive model for digital cities can be summarised in a framework that:

- Distinguishes the various components of the physical city infrastructure (buildings, roads, underground facilities and so forth) on or in which digital technologies can be exploited to serve the city complex and its organisational and social support components of the infrastructure.
- Distinguishes the communications and physical resourcing and utility structures that support city life that can benefit from digital intervention and innovation.
- Distinguishes the infrastructure for security, surveillance and emergency services.
- Distinguishes communications infrastructure and public support hubs, and very significantly the role and impact of Internet-enabled services.
- Distinguishes the various components of mobility within and between city infrastructures that can benefit from digital intervention and innovation.
- Distinguishes the various components of city functionality and city services that can benefit from digital intervention and innovation
- Distinguishes the various dimensions of digital intervention for identification, data and information exchange, location and positioning, timing, sensing, actuation and control.
- Distinguishes an extendable framework of technology drivers for implementing digital developments.
- Distinguishes a standardisation framework for facilitating the needs for interoperability and scalability in city developments and inter-city integration and communications.
- Distinguishes a progressive strategic agenda for determining city needs that could benefit from digital intervention and innovation, including those of a socio-economic nature.

This ten point framework, along with a governance model, can form the basis for positioning and considering open innovation proposals for future IoT-enabled services in “smart” cities.

The governance model seeks to assure that applications and services, be they Internet-based, IoT-based or other provision, contribute to the prosperity, protection and quality of life. By applying the model to the considerations of Internet- or IoT-enabled services, confidence may be gained in their relevance to city requirements and city acceptance, the rationale being how a proposed service or services relate to the three areas of governance concerned.

The Smart City governance framework seen below links to IoT governance through national IoT governance supporting bodies.



Staged Approach to An International Governance framework

To accommodate the wide ranging needs associated with an international framework for governance that contrast and yet integrates with Internet governance requires a careful staged approach to its formation. This staged approach proposal, and the associated requirements for completing each stage, are summarised as follows, together with the liaison and work requirements to be undertaken to realise the objectives for each stage.

Preparation of IoT Statement of Purpose and Structure - These statements are seen as forming an initial reference document for developing international framework for IoT Governance, wherein the statements are appropriately qualified to explain scope and meaning of any potentially ambiguous terms that may be used.

Identification of an international IoT Governance Stakeholder Group - Appropriate identification and representation of stakeholders are important requirements for realising both an effective governance body and a body to liaise with the Internet governing bodies. In terms of sector representation the Working Group for Internet Governance (WGIG) identify three stakeholder sectors:

- Government - geared towards creating an environment for encouraging developments in ICT and development, as appropriate, of laws, regulations and standards, to foster the exchange of best practices and engage in oversight functions.
- Private sector – geared to promoting industry self-regulation and the exchange of best practices, developing policy proposals, guidelines and tools for policy makers and participation in national law making and fostering of innovation through its own research and development.
- Civil society – geared to mobilizing and engaging in democratic and policy processes, network building and consideration of other views.

The World Summit of the Information Society (WSIS) has indicated a slightly different sector identification (implied in Article 49 of the WSIS declaration), with the addition of a fourth sector embracing international organisations. Here the sectors are recognized as:

- States - as agents for policy authority for Internet-related public policy issues (including international aspects).
- Private sector – geared to the development of the Internet, both the technical and economic fields.
- Civil society – geared to dealing with Internet matters, especially at community level, intergovernmental organisations and the coordination of Internet-related public policy issues.
- International organisations – geared to the development of the Internet-related standards and relevant polices.

For the purposes of IoT governance the four sector model, coupled with the gearing identified in the WGIG delineation of stakeholders, may be considered more appropriate, particularly if the scope of IoT development embraces both Internet and Internet independent components as suggested in a CASAGRAS2 discussion paper. The prospect may also be seen for reformatting specific roles within these sectors. With significant corporate developments being seen in large international organisations with respect to 'smart cities', 'smart planet' and other smart-based developments there are significant prospects for an Internet-parallel network-of-networks as part of the IoT vision. This being so the role of the private sector and international organisations will assume even greater prominence in IoT governance.

Within the four-layer model for stakeholders the States and Civil Society representatives will undoubtedly assume increasing importance in dealing with physical world infrastructural matters and associated matters, addressed earlier, concerning:

- Implementation, maintenance and development of the IoT physical world infrastructure.
- Environmental disruption and impact associated with deployment and maintenance of fixed position IoT object-connected devices, systems and networks, and the end-of-life recycling or disposal of devices, systems and networks; exacerbated by an expected exponential growth in use of object-connected and other edge-technology devices.
- Environmental and societal impact of mobile devices and fixed in-mobile devices and networks in transport structures.
- Attendant implications of extensive populations of object-connected and integrated system devices and networks with respect to functionality, reliability, safety and responsible deployment and use of such devices and networks.
- Energy and materials conservation including the control and recycling of object-connected e-waste.
- Privacy (including corporate privacy) and security associated with object-connected data or information contained in object-connected devices and communications between object-connected devices and data transfer systems.

- Security of infrastructure, applications and services, particularly in relation to autonomous systems communications and functionality.
- Functionality and performance demands in relation to physical world interaction.
- Standards and regulatory recognition and developments to accommodate the broader based vision of the IoT.
- Accommodation of Internet-independent network and communication structures and prospects of new IP-independent infrastructural developments.

As part of the requirements for identifying any of the stakeholders there is a need to determine the responsibilities and accountability of stakeholders.

There are clearly some important issues concerning structure, roles, responsibilities and accountabilities to be considered in formulating the stakeholder group for IoT governance that need to be addressed within the IERC Activity Chain and the international forum to be set up by IoT-i in collaboration with CASAGRAS2. The physical world infrastructural matters and associated matters listed above will not only require consideration from a stakeholder standpoint, but also consideration as components of content within the governance agenda.

Identification and recruitment of an International (or Global) Legislator and Regional Legislators and the Governing Body - While the term legislator has intrinsic legal implications, the prospective roles of international and regional legislators may be proposed to have a broader meaning in relation to governance and regulation. However, it must be seen as an important component in establishing an international legal framework. For an international development of the size envisaged for the IoT the international legislative role will need to be an organisation that is knowledgeable of IoT developments and Internet governance. This would suggest an existing organisation rather than a new organisation, albeit that the form and function of the IoT is not as yet completely defined. Suggestions [27] being proposed for the role of International Legislator include the World Trade Organisation (WTO) and the Organisation for Economic Co-operation and Development (OECD).

However, the need can be seen for further research and consideration of the International Legislative role, eligibility requirements and prospective contenders. Similarly, the Regional Legislators, with consideration as to what would constitute a regional entity, for example continental or by country.

In specifying the need for an International Legislator the question arises as to its relation to the Governing Body. It seems logical that the organisation providing the international legislative role should feature significantly in the Governance process, along with regional legislators and Stakeholders. It also raises questions of costs and funding formula for such a body.

The issues concerned here for international and regional legislators are such that it requires informed expert attention to define roles and eligibility requirements. Ideally it requires expertise that spans the technical, governance and legal issues relating to the IoT. From a technical and international standpoint the need can be seen for considering IERC Activity Chain input to the derivation of roles and suggestions for fulfilling the international and regional Legislator requirements. Suggestions may also be presented for the formation of the Governing Body and the funding strategy required to support its formation, functionality and sustainability.

Legislator/Stakeholder agreement on Regulatory approach - The regulatory approach to IoT governance is seen as a matter for Legislator and stakeholder agreement. However, in drawing upon collective wisdom on governance, suggestions may be made for such an approach. Self-regulation with subsidiarity (central authority or trans-governmental network having subsidiary function in handling tasks or issues that cannot be handled by the self-regulatory authority) is perhaps seen as a logical choice. A possible alternative would be by international agreement, but would probably be rejected in preference for self-regulation, because of the often protracted nature and long time intervals for achieving and applying such agreements.

While the regulatory approach is a matter for agreement at the Legislator/Stakeholder level suggestions may be provided to assist in this process, Together the Legislators and Stakeholders, or representatives there of, will form the principal part of the Governing Body for the IoT and as such will implement the regulatory processes and procedures. The IERC Activity Chain may assist in suggesting a regulatory approach, processes and procedures along these lines and in so doing inject the necessary expertise in IoT developmental matters.

Rules for Governance - In looking at the rules for governance it is useful to delineate:

- Those required for effecting governance within the governance body and its affiliated links, in the case of IoT extending to grass-roots national and city governance.
- Those that relate to content and in particular to operational aspects of governance and relating to structural matters.

Rules in this context are viewed as regulations or principles governing conduct or procedure within a particular area of activity. In both cases the specification of actual rules are seen as the responsibility of the governing body. However, in considering the scope of such rules it is useful to consider the model described above under tools for governance, based on that of MacLean [28] in respect of legal quality of regulations (soft to hard law) and the scope of international governance. It is also useful for positioning organisations in respect of these two determining dimensions.

Clearly, as far as the IoT is concerned the required tools for governance must embrace the needs in respect of cooperation, policy, coordination, standards and laws and regulations. So too in respect of scope and the need to embrace exchange of services and products, use of common resources, development of technologies, networks and services, and applications for equitable, sustainable global development. Ideally, for a global legislator for IoT, the organisation concerned should fill the mapping space. In the absence of such an organisation the prospect may be seen for strong linkage with the IETF and possibly with the WTO. These are essentially matters to be decided by an IoT governance task force with appropriate international representation.

Legislator/Stakeholder review and agreement on IoT Statement of Structure and Purpose - With a Governing Body in place it will be necessary to establish a frame of reference for IoT through the statements of Purpose and Structure. It is therefore essential that these statements are well founded, clearly and unambiguously stated and present the overall vision of the IoT. They must also have a precision that assist the development of an associated legal framework for underpinning governance.

The IERC Activity Chain has a role in developing these statements as a foundation for IoT governance. It may also be seen to require a multi-disciplinary input to the development to ensure an appropriate balance of technical and societal reach.

Legislator/Stakeholder agreement on an international legal framework - There are many aspects to defining an international legal framework for the IoT, including the basis upon which various governance instruments are formulated. Parallels may be drawn with the legal aspects of Internet Governance wherein [29] attention may be directed to:

- Legal issues per se, including cybercrime, intellectual property rights, data protection, privacy rights, and consumer rights;
- Legal mechanisms for addressing Internet governance issues, including self-regulation, international treatise, and jurisdiction"
- Cyberlaw vs Real Law – WSIS/WGIG discussions emphasise the need to use existing national and international legal mechanisms for regulating the Internet.
- Global regulation – while desirable in many aspects, national and regional regulations are assuming greater relevance.
- Variable geometry approach to governance – recognising it as a method of differentiated integration which acknowledges differences within the integration structure and separation between integration units.
- Differences between International Public Law and International Private law – recognising the significance of public law in the context of Internet governance.
- Harmonisation of National Laws – supporting the need for global regulation, resulting in one set of equivalent rules at global level
- Elements of International Public Law – that could be effectively applied to Internet and IoT governance, including:
- Treaties and conventions
- Customary law
- Soft law – frequently encountered in governance debate

Soft Law may be seen as a useful vehicle for deriving instruments for governance. While it refers to quasi-legal instruments, which are not legally

binding or otherwise somewhat "weaker" than the binding force of traditional law, soft law is generally associated with international law and used to assist in deriving:

- Resolutions and Declarations
- Statements, principles, codes of conduct, codes of practice often found as part of framework treaties;
- Action plans
- Non-treaty obligations

Soft Law would also appear to have some additional benefits in formulating international contributions to legal framework proposals, including:

- Not legally binding – cannot be enforced through international courts or other dispute resolution mechanisms
- Contain principles and norms rather than specific rules – usually found in international documents such as declarations, guidelines and model laws
- Used for building mutual confidence, stimulating progress, introducing new legal and governmental mechanisms
- Less formal approach, not requiring official commitment of states, reducing potential policy risks
- Flexible, enough to facilitate the testing of new approaches and adjustment to rapid developments
- Greater opportunity for multi-stakeholder approach than does an international legal approach restricted to states and international organisations

While these features may give some direction towards formulating an international legal framework for IoT it has to be recognised that it is a specialist legal task to complete such a framework. Ideally it requires expertise that spans the technical, governance and legal issues relating to the IoT. From a technical and international standpoint the need can be seen for considering IERC Activity Chain input to the derivation of the legal framework.

Legislator/Stakeholder Identification and positioning of trans-governmental networks for IoT Governance and liaison with Internet Governance Developers - In developing the IoT the prospect may be seen for the establishment of trans-governmental networks tasked

with dealing with IoT matters and promotion at the governmental level, including input into governance. A role may therefore be seen for Legislators and Stakeholders (or more formally the IoT Governing Body) identifying and positioning trans-governmental networks for IoT in the strategy for IoT governance.

The IERC Activity Chain may assist in helping to define the role and networking capability of these trans-governmental networks.

Legislator/Stakeholder development and agreement on governance content requirements - In considering the requirements for IoT Governance and how it differs or could differ from Internet governance, content is clearly a critical distinguishing factor requiring careful attention to what is required. While it may be considered that governance is more about the operation and usage of the network than its structure, aspects of structure will naturally have a bearing upon governance issues. Structural and operation issues are therefore important aspects of governance content and may be usefully considered in relation to technical, economic, institutional, policy and legal perspectives [30]. The items of content viewed in relation to technical, economic, institutional, policy and legal perspectives provide the basis for a matrix approach to presenting and considering content for governance. It is also dynamic in the sense that content can be added and considered as appropriate to IoT developments.

Aspects of governance relating to structure will draw upon the items listed above in respect of stakeholder considerations and include:

- Physical world object-connected infrastructure for IoT, and associated policy and provisions
- Security policy and provisions
- Safety policy and provisions
- Energy conservation policy and provisions
- Regulatory policy and provisions
- Standardisation policy and provisions

Aspects of governance relating to operational and usage will include:

- Physical world deployment, maintenance and usage of object-connected technologies and associated policy and provisions
- Accommodation of object-connected e-waste and recycling and associated resource management

- Environmental disruption, impact and management policy and provisions
- Global Numbering issues and Resolver schemes for identification and discovery
- Social Capital, Privacy, Security and Identity management policy and provisions
- Ethical and user protection policy and provisions
- Cyber-crime protection policy and provisions
- Intellectual Property protection policy
- Performance Indicators, rules and norms for IoT operation
- Developmental policy

The matrix approach may be considered a useful tool for assisting Legislators and Stakeholders in identifying and considering content for governance and the IERC Activity Chain may assist in structuring an initial matrix of content viewed in relation to technical, economic, institutional, policy and legal perspectives.

Legislator/Stakeholder agreement on foundational substantive principles for governance and governance procedures - In determining the foundational substantive principles for IoT governance and governance procedures it is clearly sensible to consider those being applied for Internet governance. This aligns with the need identified above for collaboration with Internet Governance developers. However, it is also important to consider particular needs in relation to IoT structure and functionality, and the very important issues concerning physical world infrastructure for the IoT.

In recognising the importance of Internet governance in respect of principles and procedures it is important from an IoT perspective to list, describe and consider their significance in relation to IoT development and governance requirements. This is a precursory activity that could be fulfilled within the IERC Activity Chain to assist Legislators and Stakeholders in pursuing their roles in governance.

Legislator/Stakeholder agreement on infrastructural requirements and policy for on-going consideration - IoT infrastructure and associated policy for on-going consideration of IoT infrastructural developments is a significant governance requirement with a need to

address robustness, availability, reliability, interoperability, transparency and accountability. The technical nature of these requirements demands appropriate technical support.

This is a further precursory activity that could be fulfilled within the IERC Activity Chain to assist Legislators and Stakeholders in pursuing their roles in governance.

Legislator/Stakeholder agreement on access to governance procedures and liaison with Internet governance developers - In recognising the Internet as one of the foundational imperatives for the IoT it is essential that any Governing Body for the IoT liaises effectively with organisations influencing Internet Governance. A number of such organisations exist, with varying responsibilities for Internet development and associated governance, including:

- Internet Engineering Task Force (IETF)
- Internet Architecture Board (IAB)
- Internet Engineering Steering Group ((IESG)
- Internet Society (ISOC)
- Internet Corporation for Assigned Names and Numbers (ICANN)
- Internet Research Task Force (IRTF)
- Internet Commerce Association (ICA)
- World Wide Web Consortium (W3C)

While not an exhaustive list it is representative of the significant effort and areas of influence upon Internet governance.

The need may be seen for deriving a strategy and hierarchical approach to implementing collaboration and cooperation for governance purposes. An incisive study may be required to best determine the role of each of these influential bodies and the best way to effect the collaborative role, ideally in a synergistic way. The multi-disciplinary nature of these Internet groups suggests the need for trans-project considerations within and across the IERC Activity Chains.

Legislator/Stakeholder agreement and pursuance of governance and legal agenda on governance requirements - The manner in which governance is pursued and in which collaboration is achieved with Internet governance bodies is an important consideration for which a strategic

agenda is required. Each must be well founded from a legal perspective and agreed from an international stakeholder standpoint. Again the need can be seen for considering the approach that is adopted in pursuing Internet governance. As far as the legal agenda is concerned that must be seen as a specialist legal activity requiring appropriate legal expertise.

Deriving an account of Internet governance procedures may be considered a further precursory activity that could be fulfilled within the IERC Activity Chain to assist Legislators and Stakeholders in pursuing their roles in governance.

Moving Forward with IoT Governance

While a framework has been specified for IoT governance this is only a precursor to fully defining the role of IoT governance, its relation to Internet governance and a roadmap to achieving a globally acceptable IoT. This framework is to be supported with information to be derived from a CASAGRAS2/IERC international survey on IoT Governance which will be reported later in 2012.

The global nature and scope of IoT governance suggests the need for an electronic or e-platform for supporting IoT governance. The European Commission has promoted the use of e-governance as "basically the application of Information and Communication Technology to the processes of Government functioning in order to bring about 'Simple, Moral, Accountable, Responsive and Transparent (SMART) governance." It is also seen as a means of achieving "wider participation and deeper involvement of citizens, institutions, civil society groups and the private sector in the decision-making process of governance.

E-governance - Notable benefits of using e-governance include:

- Ease of accommodating wide ranging issues of global significance where the IoT has relevance and governance is required.
- Ease of collaboration in respect of Internet governance.
- Wide-ranging access to information and quality services for citizens, including public consultation, bearing in mind the issues of digital divide and the need to accommodate them.

- Ease of achieving simplicity, efficiency and accountability in and between governments and with respect to IoT stakeholders at large.
- Ease of positioning citizens in IoT developments and associated governance issues.

International Forum and Roadmap to IoT Governance

- Establish international forum for IoT Governance
- Facilitate an international survey on IoT Governance
- Establish e-governance network
- Implement the framework for IoT Governance and collaboration with Internet Governance
- Institute a programme on international workshops dealing with global IoT-related issues and associated governance requirements.
- Institute an international platform for Public Consultation.

Governance conclusion

Governance must be regarded as perhaps the most important international collaborative requirement for the development and management of the IoT if it is to realise its full potential and tackle many of the social and economic vagaries and problems that are associated with the existing Internet and those envisaged for the evolving IoT, including:

- Many aspects of cyber crime and invasions of privacy and security
- Many implications of physical interaction on the scales envisaged for the IoT and in respect of issues such as environmental impact, energy conservation and exploitation of natural resources
- Many aspects of corporate and governmental impact upon IoT development
- Many aspects of social impact through smart objects, applications and services
- Many aspects of standardisation and regulatory control

Much of this relates to content for governance and its reach with respect to global, interstate, national, regional, city, industry and even domestic issues. The many aspects of physical interaction take the governance requirements for the IoT well beyond those of the existing Internet, and are truly dynamic in terms of the IoT deployment and accommodation of change.

While much of the structure and rules for governance are well defined for other areas of governance the need can be seen for further development of tools to accommodate the dynamics of content and change relating to physical world interaction, virtual world exploitation and the myriad of issues concerning social interaction and enterprise.

The CASAGRAS2 initiative has touched upon these requirements and tools to assist the governance processes in respect of content and change. It has possibly gone as far as its brief and duration allows. The need is now seen for the setting-up of an international body, linked to the Internet governance bodies, which can move forward in a much more authoritative manner to achieve an effective governance facility.

References

1. Object-connected technologies are those technologies that are embedded-in, attached-to, accompany or interact to derive data or information concerning the object itself (image capture, speech recognition and natural features, such as fibre patterns, for example), the objects being tangible physical entities of any kind.

2. Internet Engineering Task Force (IETF – Mission statement – RFC3935, 2004)

3. FIArch Draft Document (2011) Fundamental Limitations of Current Internet and the path to Future Internet.

4. Note: by referring to IP/IP-independent rather than Internet/Internet-independent structure, structures and protocols, particularly at the physical edge (such as Ethernets), may be considered that can form commonality between the two.

5. Cisco annual Visual Networking Index (VNI) suggests that Internet traffic will quadruple to 767 Exabytes (767 x 1018 bytes) by 2014.

6. Council of Europe (2009) Internet governance and critical internet resources, Media and Information Society Division, Directorate General of Human Rights and Legal Affairs, Council of Europe, April 2009.

7. Internet Engineering Task Force (IETF – Mission statement – RFC3935, 2004)

8. Rappa, M (2010) Managing the Digital Divide - http://digitalenterprise.org/government/gov_text.html

9. Corwin, P (2011) – on behalf of the Internet Commerce Association, "The ICA Blasts The Department of Commerce Letter to ICANN Committee: "May Mean the End of New gTLDs"" http://www.thedomains.com/2011/02/02/the-ica-blasts-the-department-of-commerce-letter-to-icann-committee-may-mean-the-end-of-new-gtlds/

10. Ibid

11. Council of Europe (2009) Internet governance and critical internet resources, Media and Information Society Division, Directorate General of Human Rights and Legal Affairs, Council of Europe, April 2009.

12. Council of Europe (2009) Internet governance and critical internet resources, Media and Information Society Division, Directorate General of Human Rights and Legal Affairs, Council of Europe, April 2009.

13. Council of Europe (2009) Internet governance and critical internet resources, Media and Information Society Division, Directorate General of Human Rights and Legal Affairs, Council of Europe, April 2009.

14. Weber, R H & Weber, R (2010), Internet of Things – Legal Perspectives, Springer

15. Wolfram, G et al, (2008) "The RFID Roadmap: The Next Steps for Europe", Springer.

16. Ibid

17. Benhamou, B (2007) A European Governance Perspective on the Object Naming Service, Proceedings of the Portuguese EU Presidency conference on RFID: The next step to The Internet of Things.

18. Cited in Weber, R (2009), Shaping Internet Governance: Regulatory Challenges, Springer.

19. Santucci G 2011 – the Internet of Things; the way ahead in 'Internet of Things – global technological and societal trends' (editors Ovidiu Vermasan and Peter Friess – River Publishers).

20. Cited in Weber, R (2009), Shaping Internet Governance: Regulatory Challenges, Springer.

21. Food and Agriculture Organisation of the United Nations – FAOSTAT – FAO Statistical Database

22. ter Beck, V (2009) Optimising production efficiency is the key, Pig Progress vol 25,9, -6

23. Foley. J A et al., (2011) Solutions for a cultivated planet, Nature, 478, 337-342, Oct 2011

24. Foley, J A (2011) "Can we Feed the World and Sustain the Planet – A five-step global plan could double food production by 2050 while greatly reducing environmental damage", Scientific American, November 2011.

25. United Nations report (2009)

26. Prof George Hazel report entitled "Megacity Challenges", MRC McLean Hazel Consultancy.

27. Weber, R H (2011, Accountability in the Internet of Things, Computer Law & Security Review, (2011) 133-138.

28. Cited in Weber, R (2009), Shaping Internet Governance: Regulatory Challenges, Springer.

29. Kurbalija, J Internet Governance and International Law in Reforming Internet Governance: Perspectives from WGIG, 106-115

30. Kurbalija, J Internet Governance and International Law in Reforming Internet Governance: Perspectives from WGIG, 106-115

Acknowledgements

Professor Furness wishes to acknowledge the many CASAGRAS2 and IERC discussions and workshops that have contributed to the content presented in this chapter

Professor Furness is the Technical Coordinator of CASAGRAS2
anthony.furness@btconnect.com

'The Internet of Things – Where is it Going?'
A GLOBAL OVERVIEW

The European Commission is playing a major role in addressing the key issues relating to the development of the IoT. It has recognised the need for authoritative, ongoing International co-operation in respect of its agenda for taking the concept to reality.

CASAGRAS2, a co-ordination and support action for global activities and standardisation has been one of the key conduits for taking the EU aspirations to the next steps in International collaboration. This project identified a broad base for International co-operation with partners in Brazil, India, China, Japan, Korea, Malaysia, Russia and the USA along with Europeans and other IoT experts from various parts of the world.

CASAGRAS carried out fact-finding missions across Asia, South and North America, Europe and into Africa and the Middle East. They organised conferences and supported workshops, seminars and academic symposiums from Medellin in Colombia to Wuxi in China and collected many snapshots of IoT perceptions along the way.

This chapter focuses on brief reports from around the world. You will read of different interpretations. Different challenges. The differing views confirm the decision of the European Commission to take a lead in supporting and developing a significant global harmonisation programme through the ongoing activities of the European IoT Research Cluster, the newly established International IoT Forum and the European IoT Alliance.

We also asked a number of major multi-National commercial companies to outline their own strategic agendas for the developing Internet of Things including future prospects and challenges. You can read their views later in this chapter

The one very clear outcome of our two year journey is that the Internet of Things is definitely 'on the move' across the world!

Africa

By Fahmi Chelly

The rapid improvements in communication networks all over the world, together with the explosion of ubiquitous devices, have paved the way to the emergence of a novel paradigm that is the Internet of Things (IoT). The basic idea of this concept is to enable new forms of interaction between people and things, and between things themselves to reach common goals. Various application domains ranging from Green-IT and energy efficiency to logistics are already starting to benefit from IoT concept (Coetzee & Eksteen).

This paper shows how far Africa is in the uptake of IoT Technologies. If we look at the whole region, we might say that Africa is likely to be slow in the uptake of IoT technology compared with European and other developed countries, but if we scrutinize African countries separately we find interesting success stories from Africa that show Government awareness of the benefit of IoT to society, economy and environment. The Tunisian Government, for example, has recently showed its strong commitment to institutionalize a national Research-Development-Innovation (RDI) program that responds to the evolving needs of ICT market with respect of Tunisian context. The underlying program stresses three priorities in terms of technologies and infrastructures: future network, Internet of Things and Internet content and recommend the Smart City, among four application domains. South Africa, also, has quickly recognized the importance of IoT and demonstrated how IoT applications could impact on energy conservation and load optimization, environmental control and inclusion, information dissemination to society, etc.

In addition, various small-scale IoT initiatives across the African continent have been proposed to respond to specific needs of African people.

For instance a Tanzanian logistics firm is currently employing an RFID-based system to help assure the distribution of oil products to its proper customers in East and Central Africa.

Nigeria has recently launched a product verification initiative, via RFID, in an effort to secure the integrity of the drug supply chain and reduce the counterfeiting of drugs.

It is expected that RFID adoption will be increased in the coming years and supply chain management is expected, among the sectors, to increase Africa's demand for RFID applications. Additionally, wireless sensor technologies have also brought effective solutions to healthcare, natural disasters, and environment control – which are the major problems faced in Africa.

For example, in Ethiopia a health application was developed to monitor antiretroviral drug therapies for AIDS. A research group in Kenya developed an application based on heat sensors to detect a fire and automatically relays the information to a forest station through mobile phone technology to limit fire disasters. A system to monitor water quality in Malawi is under development at the Royal Institute of Technology in Sweden.

Although existing initiatives show that IoT offers green field opportunities to Africa's needs across all sectors (supply chain management, healthcare, environment monitoring, etc.), the adoption of IoT technologies remains very slow. Investigations on the barriers that hinder the adoption of IoT are needed and the way to leverage from successful experiences should be also considered.

Fahmi Chelly (Fahmi.Chelly@cert.mincom.tn)
www.cert.tn

AFRICA

South Africa

By Dr. Louis Coetzee

South Africa is entering an exciting period for Internet of Things (IoT) activities.

Current State

Commercial vertical solutions without broader integration are being planned and implemented. These include the Gauteng highway e-tag tolling based on RFID, and planned initiatives with multi-nationals to 'smart' retrofit major South African cities.

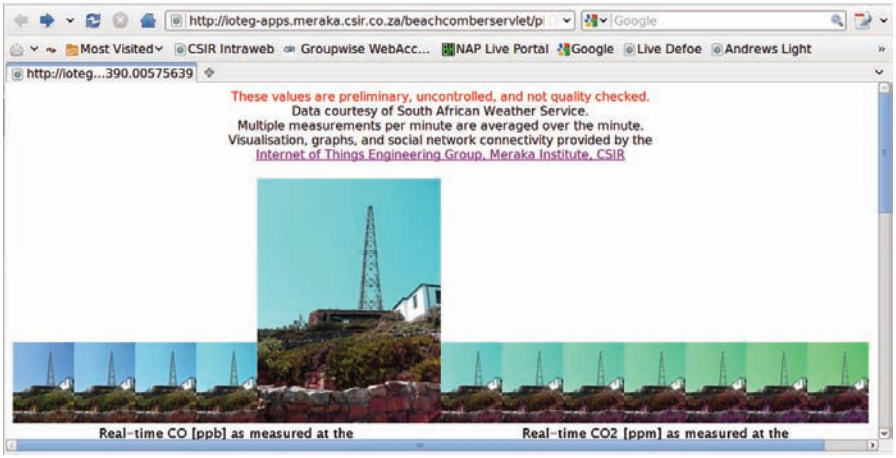
Eskom, South Africa's public electricity utility, is developing technology known as the 'Utility Load Manager', a residential load management system that allows the utility to limit residential loads and to integrate end-use consumption data with back-end systems.

Existing technology research in South Africa is providing important enabling building blocks for IoT. These include: the South African Nano Technology initiative and the associated National Centre for Nano-structured Materials; the Sensor Science and Technology Group in the CSIR Materials Science & Manufacturing unit, conducts research in smart structures and materials, electro-optic sensing and imaging, and ultrasonics. The CSIR Meraka Institute's Advanced Sensor Networks Group, with the University of Pretoria, conducts research in wireless sensor network architectures and protocols. The CSIR Meraka Institute's Earth Observation Science and Information Technology Group has developed capability associated with Sensor Web Enablement of Earth Observation Data Resources.

Recognition of the national importance of IoT led to a strategic intervention: the formation of the Internet of Things Engineering Group (IoTEG) at the CSIR Meraka Institute. IoTEG is positioned to leverage the mentioned enabling building blocks with the aim of building a national IoT competence.

IoTEG is researching middleware needed for large-scale IoT solutions. The group has created an event-driven protocol-agnostic framework (Beachcomber) that connects the physical world, and people, to cyberspace. In this connected world, services make sense of received data and initiate actions. Beachcomber has been applied in the natural environment (linking

carbon observation sensors to social media), built environment (creating cyber presences for dams) as well as other demonstrators, including a smart enabled office and a smart domestic environment aimed at improved energy efficiency.



Local Drivers

IoT's uptake is driven by a national need to improve service delivery, increase quality of life, and enable sustained economic growth. These needs were highlighted by the South African Department of Science and Technology's National ICT RD&I Roadmap initiative. This roadmap has, amongst others, identified 'smart infrastructure' (such as sensor and network technology) as a mechanism for addressing environmental and resource sustainability as well as asset management challenges.

National research capacity has been enhanced by two National Research Foundation funded Sensor Networks research chairs being awarded to the University of Pretoria.

The continued roll-out of broadband and enhanced mobile, and wireless communications capability is creating a rich environment for IoT. Tertiary education institutions are offering research topics associated with the IoT.

Local Inhibitors

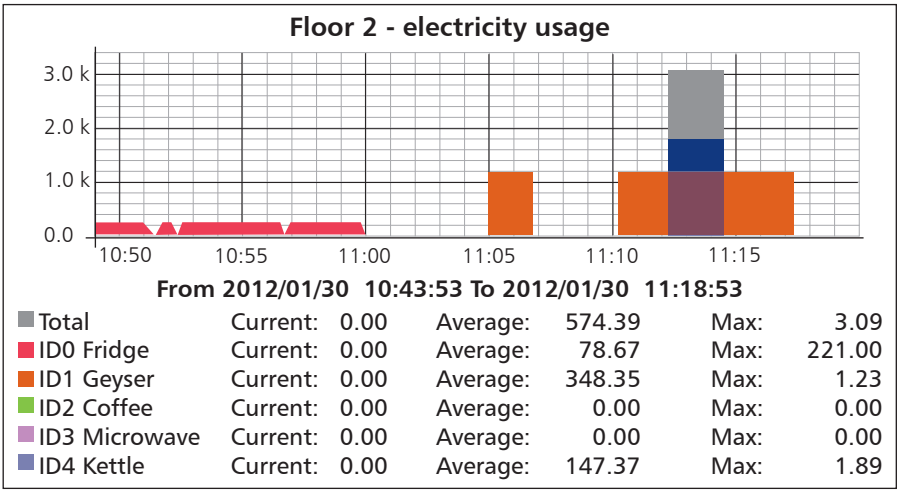
Despite these activities inhibitors remain to the creation of an environment conducive to IoT uptake. No national policies, nor governance models, exist yet for the broad-based uptake of IoT. This, linked to constraints in data sharing and unresolved issues such as privacy, is challenging.

The costs associated with connectivity and technology, in general, are significant inhibitors. Most significant though is the limited number of skilled and experienced researchers and the lack of a well-defined human capital development pipeline. Significant vertical solutions are planned or being rolled out (e.g. the Gauteng RFID e-tag initiative), but no plans are in place to utilise the investment by integrating these vertical solutions.

Prospects

Several prospects for large-scale IoT research, development and innovation exist. South Africa is bidding to host the Square Kilometre Array (SKA), the world's most powerful radio telescope. Through the SKA, large-scale data science and associated skills in large databases and Cloud computing will be main-streamed. This will have a positive knock-on effect for IoT and IoT-related skills. The CSIR, through its drive to create more impact, has embarked on national flagship initiatives in Health, Water and Safety domains. These flagships are positioned as public-private-partnerships. IoT has a significant role to play if these domains are approached from a 'smart' (instrumented, sense-making and controlled) perspective.

IoT in South Africa is in its infancy, but the potential is clear. Significant existing capabilities, combined with a conducive and enabling context, is positioning South Africa to be a major IoT role player in Africa and beyond.



Beachcomber controls a kitchen environment to equalize energy load 4.

Dr. Louis Coetzee (lcoetze1@csir.co.za)

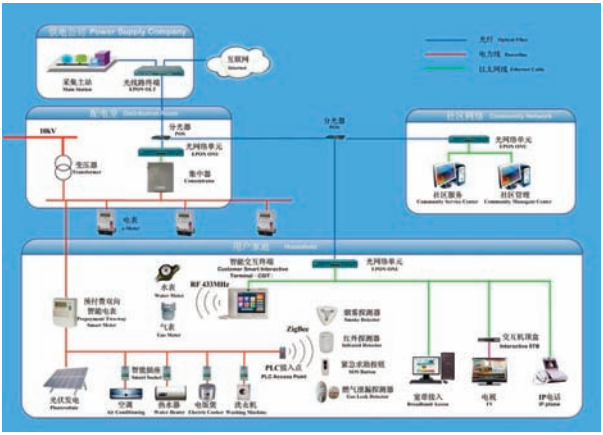
China

By Shirley Zhang

The Internet of Things (IoT) has become the important driving engine of economic development in China. It is considered one of the emerging industries and for three successive years it has been selected as one of the top 10 key ICT words in China.

In 2011, China carried out a series of successful pilot and demonstration applications in areas such as smart grid, intelligent transportation system, food safety, and M2M.

Smart Grid. Intelligent power distribution networks are under construction in 23 cities of China. Some 58 million intelligent electric meters have been installed, and 38 million kw. wind power and 450 thousand kw. solar power have been connected to the national Grid.



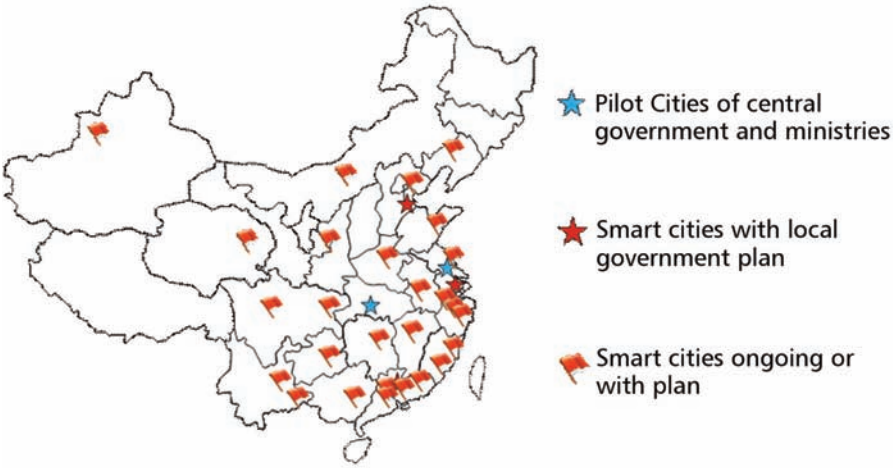
Smart Grid Application Scenario - Based on Fiber and PLC

Intelligent Transportation Systems. IoT was firstly used in the railway system, and now begins to be used for applications in city transportation, highways and water carriages. By the end of 2011, about 2,500 ETC stations had been opened in 22 provinces, covering 80% of the length of the express highways, with more than 2.2million ETC users. City intelligent transportation has also become a key point of development of ITS.

Food Safety. The Ministry of Commerce and Ministry of Finance invested ￥4 billion for a food tracing system covering 36 cities in 2011, to plan and construct a central, provincial and city level tracing and management platform.

M2M. There are about 16 million M2M terminals in China.

The Smart City has become an important opportunity for the deployments of IoT applications in China. By the end of May 2011, eighteen first-tier cities in China had formulated their detailed smart city plans, and over 80% of the second-tier cities clearly stated their objective to develop smart cities. Local Governments' target, as a result of the smart city plan, is to increase the sense of happiness of their citizens, by promoting IoT applications in economic, civil life, government management, infrastructure and cultural environments.

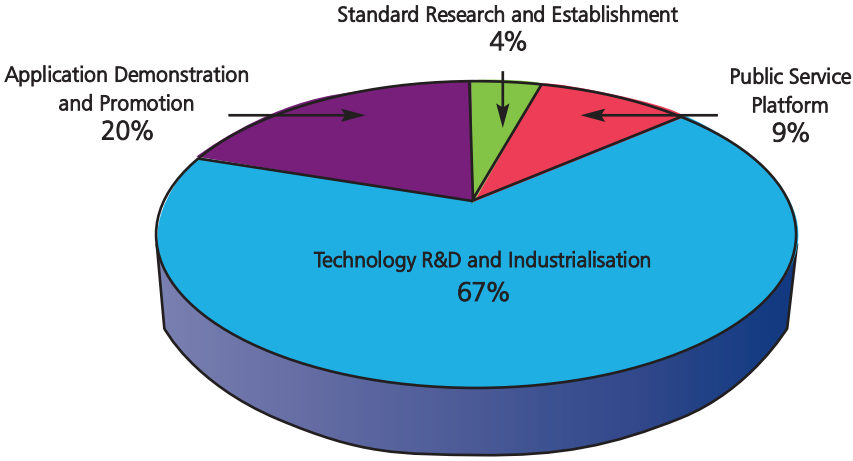


To support IoT development, the Chinese government has been paying increasing attention to the IoT since 2009. National funding has been available to support R&D of IoT via national programs such as the National High-Tech Research and Development Program (863 Program), the National Basic Research Program (973 Program), National Natural Science Foundation of China, Science and Technology Mega Projects, etc.

Since 2011, the IoT Development Special Fund has been set up to support IoT development, which includes technology R&D and industrialization, standards research and formulation, application demo and popularization, and a common service platform.

In 2011, ￥500 million was made available. 67% of this funding was used to support technology R&D and industrialization.

Distribution of Special Fundas in Project Categories



The standardisation of the IoT has been universally recognised as an important subject in China. Chinese research bodies and enterprises are actively engaged in the international standardisation process with various bodies including ITU-T, ISO/IEC, 3GPP and ETSI. The national IoT standardisation programmes are being driven by the China Communications Standards Association (CCSA) TC10, China Standardization Working Group on Sensor Networks (WGSN), and the RFID Standardization Working Group. Industry sectors including power and transportation are cooperating with relevant SDOs to develop IoT standards appropriate to their Industry needs.

To support long term development of IoT, the Ministry of Industry and Information Technology (MIIT) has released China's 12th Five-Year (2011-2015) Plan for IoT at a national level. This will enhance the capability of core technologies R&D, study and formulate key standards, set up and complete the industry chain, and support nine major applications, which are Intelligent Industry, Intelligent Agriculture, Intelligent Logistics, Intelligent Transportation, Smart Grid, Intelligent Environmental Protection, Intelligent Security, Intelligent Medical Treatment, Intelligent Home.

Shirley Zhang
zhangxueli@catr.cn

ASIA

The R&D of the IoT in Japan: 2011 Perspective

By Chiaki Ishikawa

Japan has led a number of the IoT experiments with both existing and prototype systems. Some were reported in the 2011 IERC book. This article focuses on subsequent developments including:

- **EIoTA MOU Signing**
- **Comeback of RFID**
- **Interest in Healthcare**
- **ICT to Cope with Disaster: Great East Japan Earthquake**

EIoTA MOU Signing

European IoT Alliance. A group of European organizations has signed an agreement with Japan's YRP Ubiquitous Networking Laboratory (YRP UNL) to promote technologies developed in Japan for the IoT such as

- **uID architecture**
- **T-Kernel**

The signing took place during the annual TRONSHOW in Tokyo. It was the achievement of the year in the field of IoT R&D planning for the future and you can read about the vision in Chapter 8.

Comeback of RFID

After the hyped expectations in the early 2000's, and the general lack of visible progress in areas where people had predicted deployment, the interest in RFID has surged back in the general business community.

The main reasons are

- **longer reading distance**
- **smaller size**
- **lower cost**

For example, at the 3rd T-Engine Forum Symposium "What Has Become of RFID?" on 21 June, 2011 (http://www.t-engine.org/blog/2011/20110621-sympo.html), Fujitsu reported four times longer reading distance, 30% smaller size, and cost reductions of 75% between 2006 and 2010.

Such significant improvements of RFID tags, coupled with new tags that can be washed and read off metallic surfaces, etc. have brought about new applications. Another favorable factor is the maturity of backend devices and support software and middleware.

Such interest has also raised interest in uID architecture that helps users to use different types of tags across various applications.

Healthcare

Healthcare has attracted a lot of attention lately. Industry consortium such as Continua has become very active in promoting healthcare devices at home and elsewhere.

There is a movement of collecting and analyzing the data from these small sensor devices in the cloud servers.

One issue is to identify each data coming from such devices. uID architecture that assigns a unique code to objects and places has also attracted attention from the implementers in the field.

Applications

Coping with Disaster

After the Great East Japan Earthquake on 11 March, 2011, the interest in using ICT to cope with issues of relief and recovery during and after the disasters has reached a hitherto unparalleled level in Japan.

YRP UNL had already undertaken its share of R&D in this field with its industrial and academic partners.

Securing Communication Path after an Earthquake

Securing a communication path during and after a disaster when the ground-based communication lines are all blacked out is very important in the age of the IoT. No matter how many sensors you may have, if you can

not read the sensor values, they are useless. Also, victims in the affected areas want to obtain information quickly, and send out their whereabouts to their loved ones. Hospital staff need to advise their requirements to the outside world as quickly as possible.

Securing a communication path using a communication satellite and a very small communication unit that you can plug into a mobile terminal called Ubiquitous Communicator, has been tried and shown to work well.

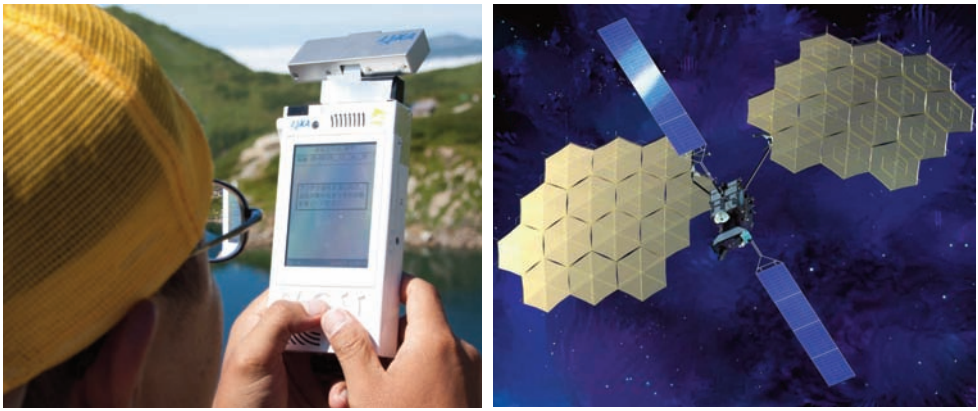


Figure 1 - (left) Ubiquitous Communicator with satellite communication unit, (right) Japan's KIKU (ETS-VIII) satellite.

Although the experiment had been formally completed, the satellite communication unit aboard KIKU (ETS-VIII) satellite was turned on again after the earthquake, and a ground communication unit was installed at the city office of Ofunato to establish the Internet access until the ground-based communication was restored. It offered valuable services. Japan is now exploring wider application possibilities.

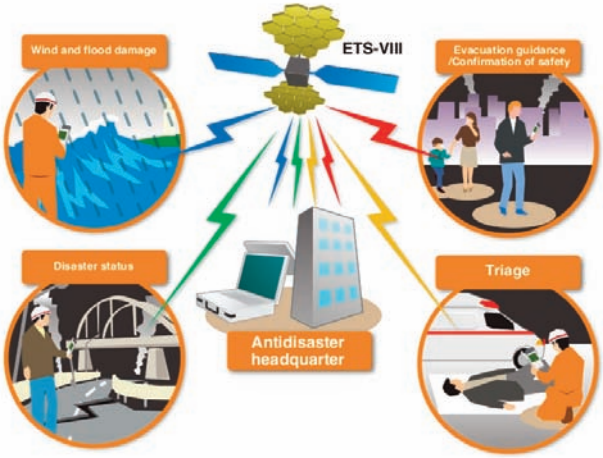


Figure 2 Usage Scenario in case of disasters

Privacy and Security Issues during Emergency

Prototyping systems to use an IC-based security card for identification and reporting of locations of the victims had been considered before the earthquake.

Emergency situations pose a very interesting issue of "Privacy vs Needs to Know."

Figure 3 - (left) People's ID and whereabouts were recorded during an evacuation exercise. (right) A manual input is possible on Ubiquitous Communicator. Date shown, 1 September (9月1日) is a memorial day of the Great Kanto Earthquake of 1923 that killed more than 100,000 people in Tokyo and Yokohama area. An evacuation drill is exercised all over Japan on this day.

Usually people want to hide their identity and whereabouts from the probing network. However, immediately after an emergency such as a big earthquake, people may want to leave their identity and whereabouts to a public database (with proper access control). This enables their family and loved ones to learn the safety status more easily.

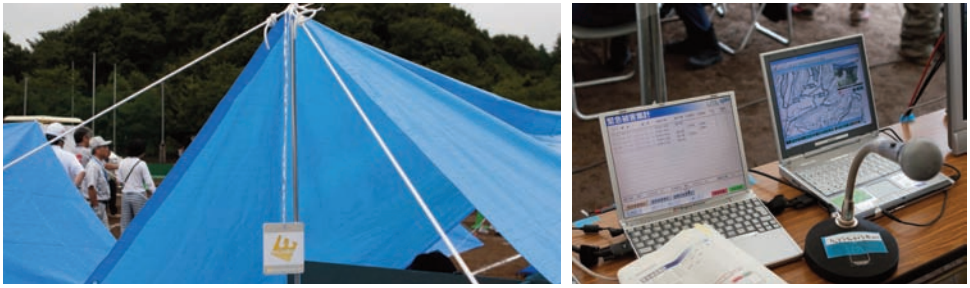


Figure 4 - (left) Shelter is identified by tags., (right) Collected data can be monitored by make-shift relief desk in the field. (These photos are from evacuation exercises)

Checking the Structures along Expressway

Japan has performed UWB-based remote sensoring of large structures along the expressway for structural stability. Quick assessment of such structural stability will be very useful after an earthquake.

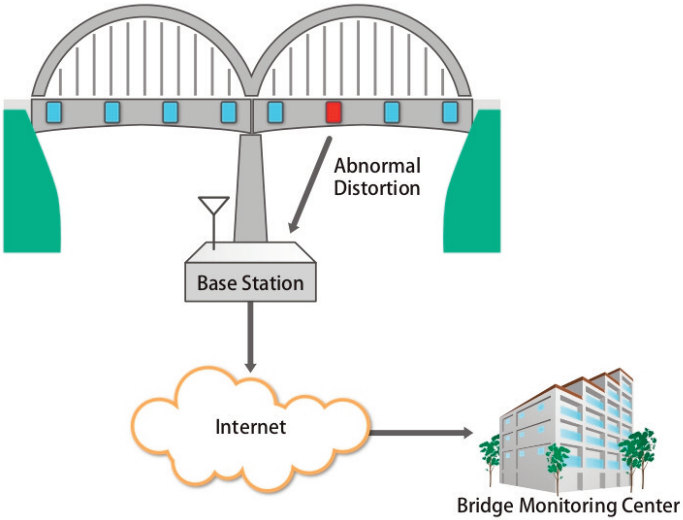


Figure 5 - Monitoring of structures along the expressway using UWB tags and sensors

Smart Grid / Smart Metering

The earthquake shut down many electric power generating plants. Planned rolling blackouts occurred as a result to avoid a large-scale unexpected blackout. Electric power utility companies chose areas one by one and cut off electricity supply to the area so that the overall grid would not be overloaded.

This caused great problems for medical professionals: patients in many small hospitals, and individuals who were resting at their homes using respirators and other medical devices that rely on electricity, were put into danger.

In the long term, we may want to see more intelligent control of the power grid. For example, by monitoring the electricity usage at device level, giving priorities to the devices such as medical ones, and only shutting down non-prioritized devices to avoid overloading the power grid in case of emergency.

In order to do so, we need to monitor the device level usage, collect such data and make intelligent decisions. A Smart Meter concept will be useful.

We have been experimenting with such a set up in Japan for some time now. The photo and the diagram shown are taken from a prototype in Matsuyama.

Figure 6 - (left) Monitoring of electricity usage at home, (right) Smart Meters in a room

Systems Used Daily

Aside from the R&D activities, especially the ones promoted for coping with disasters, there are other systems which are used daily that are based on the IoT. In our approach, we try to build an infrastructure that can be used for both daily use and usage during and after a disaster. Most of the location information systems explained below can be used to offer route guidance to emergency shelters in case of fires and earthquakes.

Ueno Zoo Sightseeing Guidance System

At Ueno Zoo, visitors can monitor the unseen behaviour of animals, birds and fish, and much more background information using a hand-held terminal while they stroll inside. The service has proved very popular among young visitors.

Figure 7 - A guide terminal at Ueno Zoo

Hama-rikyu Gardens Sightseeing Guide

A large Japanese garden in downtown Tokyo facing Tokyo Bay is an interesting sightseeing spot for a visitor to Tokyo. A hand-held terminal will guide you along the paths and explain the history of what you see in the garden.

The use of radio markers and hand-held terminals has lessened the needs of big billboards which would destroy the tranquil atmosphere of the garden.

Figure 8 - Guidance in Hama-rikyū Gardens

Observatory of the Tokyo Metropolitan Government Building

The Tokyo Metropolitan Government has promoted the Tokyo Ubiquitous Technology Project for the last several years, and uses the IoT for offering sightseeing guidance on the observatory.

Figure 9 - Scenery from the observatory and the guide terminal

Tokyo Midtown Ubiquitous Art Tour

Tokyo Midtown, a large business-residential complex in Tokyo, has 500 ubiquitous markers on its premises and uses these to offer a guided tour to objects of art placed inside and outside the buildings. The guide offers the background of the objects of art, the movie of the objects being created, and the interviews with the artists.

Figure 10 - Photo: Midtown Ubiquitous Art Tour

Tokyo Ubiquitous Technology Project in Ginza

Ginza street has been tagged with radio markers, passive tags, etc. to offer sightseeing guidance and guidance for people in wheelchairs.

Figure 11 - (left) Tag along Ginza street, (right) Reading it with a mobile phone with NFC tag reader

Traceability Systems

There are many traceability systems in use today.

The photo shown is one from the Center for Better Living. They have issued certification seals that are used to tag housing components that meet some standards. For example, some smoke detector units used in homes now carry such seals with an RFID tag inside so that the installer can easily record the position and installation date. The service company can send the notice of battery replacement if requested by the home owners.

Figure 12 - Smoke detectors are scanned to record the installation place and date

A pharmaceutical company has started tagging bottles of one of its drugs. This has helped them in tracing the drug bottles for safety and production quality monitoring.

Figure 13 - Tracking drug bottles by RFID tags on the bottom

Conclusion

The progress of the IoT research in Japan has been steady. A highlight has been the signing of EIoTA MOU with UNL at the end of 2011. We hope this paves the way for greater cooperation between EU and Japan in the field of the IoT.

However, the sheer size and impact of the Great East Japan Earthquake on 11 March, 2011 did not leave the R&D of the IoT alone, and thus more requests for the use of ICT, especially the IoT, for coping with the relief and recovery during and after the disaster have been voiced and seriously evaluated. The impact of the earthquake on the R&D atmosphere will be felt for years to come.

References

For more examples and background, readers are encouraged to read the last year's IERC book [IERC2011], and the materials from uID Center, especially the documents called Ubiquitous ID Technologies 2009 and Ubiquitous ID Technologies 2011, both available from uID Center web site: http://www.uidcenter.org/. (Click the lower-right yellow rectangle "More on Ubiquitous ID Technology.")

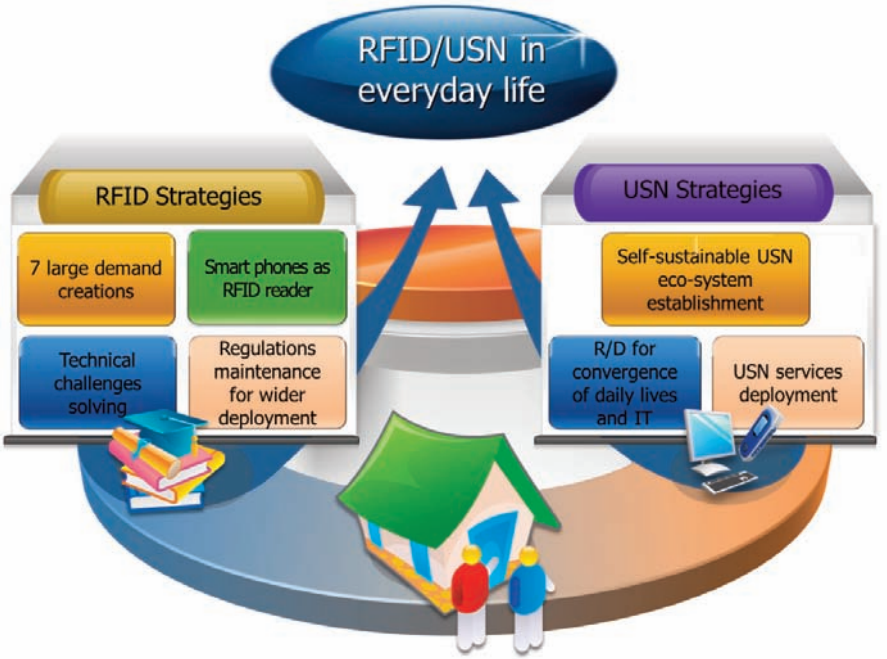
ishikawa [chiaki.ishikawa@ubin.jp]

Korea

By Yong-Woon KIM

ASIA

Two Korean ministries have been involved in the promotion and deployment of IoT visions, R/D activities and use cases in terms of RFID, USN (Ubiquitous Sensor Network) and M2M (Machine-to-Machine) which are recognised globally as the enabling technologies for IoT. Korea shares those views and visions domestically. Thus every IoT-related development and deployment in Korea has been carried out in terms of RFID, USN and M2M so far. The new IoT keywords however, seem to be **" IoT for the future direction."**



[Vision of a Korean ministry for RFID/USN]

One of the two ministries is responsible for the manufacturing industries in Korea. The visionary goal is to make RFID/USN penetrate everyday life of people to deliver a better quality of living. Large demand areas of RFID were identified: alcohol/liquor, medicine, food, apparel, home appliances, parcel delivery, and car. Smart phones may be a ubiquitous terminal for reading

RFID tags everywhere. Regulations will be adjusted for a wider deployment of RFID.

Since the price of the RFID tag is critical to wide deployment, this technical challenge will be tackled with a target price of 0.03 US dollar in 2014.

Even though sensors and corresponding automatic controls are popular and their industry can live in a profitable eco system, USN services have become more complicated and sophisticated by integrating various stakeholders and the existing social infrastructure which have been established in public domains and their industry feels it will take more time for its eco system to become sustainable, resulting in a strategic issue.

In order to achieve those strategic goals, about twenty deployment projects have been carried out via promotion associations: RFID-based production and supply chain management in the car industry and medical industries; RFID-based solar panel logistics system; hybrid-sensing based parcel delivery; alcohol/liquor logistics system; RFID built-in cell phone-based consumer information service zone; remote power transformer monitoring and control system; distributed smart farming; smart ticket system for EXPO 2012 YEOSU KOREA; steel supply chain management.

[Vision of a Korean ministry for IoT/M2M]

NOTE – "IoT" in the vision diagram was made by translating Korean keywords. "M2M" is used instead as English keywords.

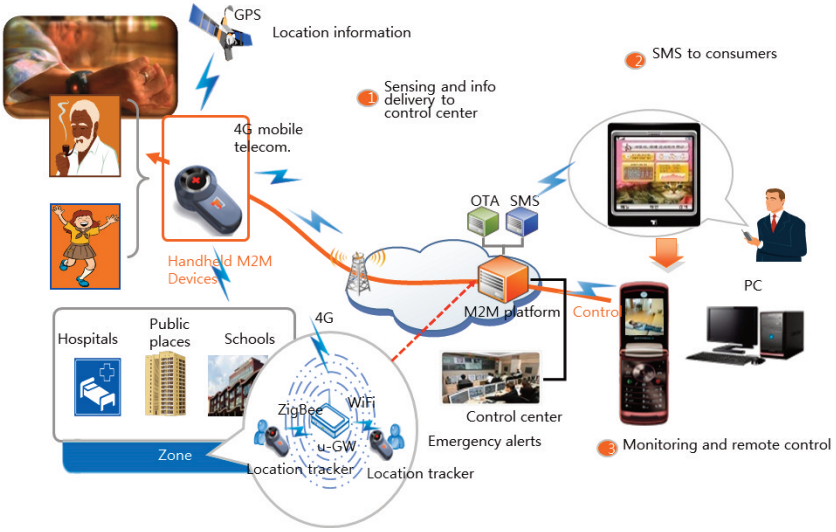
The second ministry is responsible for the telecommunication infrastructure and relevant service provisioning. It may be said that the two ministries have different views: bottom-up and top-down where some overlaps are inevitable and negotiations and collaborations have been established.

The ministry has four goals:

- **Smart Korea;**
- **Safe Korea;**
- **Competitive Korea**
- **Sustainable Korea.**

Those visions have promoted various deployment projects exploited from the following perspectives: Smart Korea via sensing and situational intelligence; Safe Korea via sensing, personal security and care and disaster management; and Sustainable Korea via sensing and environment monitoring and management. The Competitive Korea vision will be realized by technology innovations of relevant stakeholders such as manufacturers, solution vendors, and service providers.

Example deployment projects are monitoring and maintaining public facilities like water supply; urban information services such as local weather, air quality, car traffic, public bus information, and nearby geographic information; nation-wide meteorological observations; secure zone services for children and women; and healthcare.



An application view of M2M-based healthcare

qkimqkim@gmail.com

South East Asia

By Amir Sidek

South East Asia is an increasingly integrated trade area of 600 million people. ASEAN is the association of South East Asian Nations comprising Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar (Burma), Philippines, Singapore, Thailand and Vietnam. CASAGRAS2 partners were guest speakers at the fourth co-operation forum on the Internet of Things co-ordinated by the SEACOOP EU project in Vietnam last year. Participants from across ASEAN agreed that the IoT goal for the region should be:-

'IoT to stimulate new value-chains to achieve societal and economical benefits in the Asean region'

It was felt that this goal should address all stake holders – business, citizens and Government, for sustainable growth.

In terms of exploitation the following use cases were identified:

- Improving healthcare services e.g. patient pathway in Malaysia, IP-based medical devices in Thailand, SMART workplace in Singapore
- Disaster early warning and management – e.g. tsunami, flood warning (dam monitoring) in Thailand, landslide warning (or slope management) in Philippines and Malaysia.
- Environmental control – CO2 emission, pollution control in schools, pollution controls during de-forestation season.
- SMART (or advanced) Agriculture – precision agriculture in Malaysia, greenhouse monitoring in Thailand, environmental monitoring in Brunei.
- Capacity building due to IoT – Asean as a region for outsourcing from EU (or the Rest of the World) as IoT evolves and becomes ready for commercialisation.
- ASEAN as an R & D partner – offering itself as a test-bed for the EU.

The ASEAN group were anxious to collaborate with the EU and hoped for more regular visits from EU experts; improved e-communication on the Internet of Things; accessibility to the IERC; and harmonisation of policies, governance etc in the Global IoT domain.

amir@custommedia.com.my



Taiwan

ASIA

By Ko-Yang Wang, Grace Lin & Shuo-Yan Chou

Taiwan is well known globally for its ICT industry and manufactures more than 50% of the world's ICT products, including notebook computers, motherboards, LCD monitors, PDAs, mobile phones, servers, tablets and many others.

Since 2002, the Taiwan government has launched a series of ICT initiatives, including e-Taiwan (digital Taiwan) and m-Taiwan (mobile Taiwan), which has laid a good foundation.

Between 2006 and 2010, Taiwan launched a series of RFID pilot projects under the u-Taiwan (u stands for ubiquitous) initiative to raise the interest of various industries to venture into this fast growing area. These initiatives were jointly supported by Taiwan's device manufacturers, and the academic and research organizations. The awareness of the potential values and related research capacity were developed along the way.

In 2011, Taiwan's government launched another series of science and technology projects under the i-Taiwan (intelligent Taiwan) initiative, focusing on intelligent living. The key infrastructure and core technologies of intelligent living are exactly the same as the Internet of Things.

In addition to the ICT industry, six emerging industries have been highlighted —bio-tech, medical tourism, medical care, green energy and refined agriculture—each has a strong relationship with IoT.

The two main practical government research arms, Institute for Information Industry (III) and the Industrial Technology Research Institute (ITRI), for software/services and hardware, respectively, have placed significant focus on the IoT development. III has a number of projects focusing on Smart IOT applications in Healthcare, care of the elderly, Medical Tourism, Smart Micro-Grids, Smart Green Buildings, AMI, etc.

It is also implementing a common platform, called Smart System Services, for building Smart IOT solutions based on the integration of big data analytics, BPM, system engineering, cloud computing, sensor networks, etc.

Since IoT implementation requires a much broader scope of technologies from the industry side, Taiwan's hardware and software companies have formed several alliances to collaboratively develop IoT solutions. Broader but small-scaled adoptions of IoT solutions have been increasing steadily in Taiwan. It is recognized, however, that the mass adoption of IoT products and solutions needs to be realized in a larger economic entity such as China, EU, US or the global market. Some Taiwanese companies are working with Chinese partners to find a model to support further deployment of IoT solutions in China. With the maturity of the infrastructure and great local supply of hardware products, Taiwan is well positioned to serve as a test bed for many advanced IoT scenarios, for China as well as for the EU.

Taiwan's academic community has been active in IoT research. Integrated development projects for intelligent living supported by the government can be found in three universities. Other technical and business scenario research can be found in various research centers in universities. Major international firms such as Intel and IBM have also established key research cooperation with academic institutions in Taiwan.

sychou2@me.com

AUSTRALIA

Australia

By Dr Slaven Marusic

The realisation of IoT in Australia is gaining momentum with initiatives across multiple domains providing platforms for fundamental research; testbed and real world deployments; industry participation; support infrastructure and consumer uptake of emerging technologies.

Utilising IoT as a platform for creating a Smart Environment, the University of Melbourne leads two new projects in collaboration with Arup, City of Melbourne, University of South Australia, Queensland University of Technology, Deakin University and others for a smart city testbed facility spread across Melbourne, Adelaide and Brisbane, modelling the conditions of a city-wide distribution of sensors and data collection applications. It joins WSN expertise of the Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP) research network, and the cloud computing of the CLOUDS Lab to deliver smart new ways of urban monitoring using ubiquitous sensing and data analysis for city management and sustainability, through the development of energy-efficient sensing, cloud computing for sensor networks and high level analytics to detect and interpret events.

Target applications include: noise and environmental monitoring; intelligent transportation; and structural health monitoring. This integrates participatory sensing, complementing work at the University of New South Wales. The program links the Australian Urban Research Infrastructure Network (AURIN) that supplies aggregated datasets and information services for real time information sharing, as well as the UniMelb MUtopia project, a GIS based visualisation platform for urban modelling.

Australian involvement in EU IoT initiatives includes the UniMelb-ISSNIP team in the SmartSantander and IoT-i projects, as well as the Commonwealth Scientific and Industrial Research Organisation (CSIRO) in the OpenIoT project.

Infrastructure for enabling Internet of Things

With over 60% of Australians owning smart phones, the associated telecommunications infrastructure is being enhanced with the rollout of 4G LTE networks. Importantly, the infrastructure to underpin the IoT is being rolled out as the government funded National Broadband Network (NBN) to deliver high speed broadband to 100% of Australian premises (93% at one gigabit per second). The Smart Grid-Smart City Initiative is establishing a commercial scale NBN enabled smart grid demonstrator.

WSN Deployments

Australian IoT work continues from a strong platform of WSN research and deployments from across Australia. Significant WSN deployments over the past few years, undertaken primarily by Government entities and Universities include:

Marine: The Australia wide Integrated Marine Observing System (IMOS) with WSN deployments in the Great Barrier Reef Ocean Observing System (GBROOS) is delivering real time scientific marine data to understand and protect this critical ecological environment. The Smart Environmental Monitoring and Analysis Technologies (SEMAT) project is investigating new architectures for building and operating the marine sensor networks including under water communication.

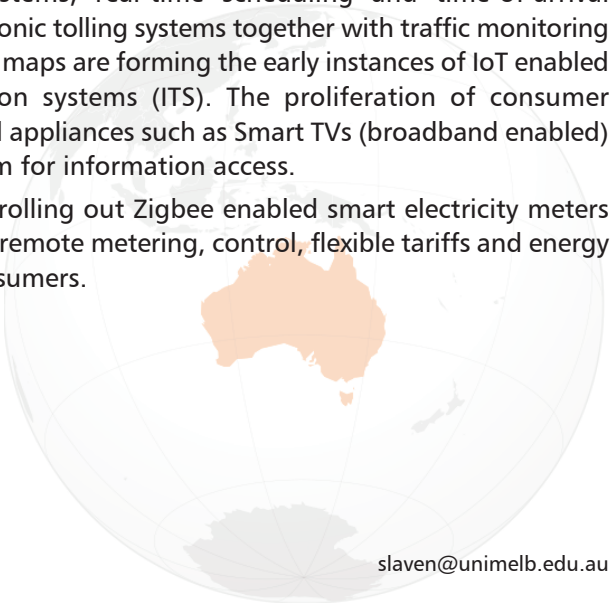
The system was deployed in Moreton Bay to measure the impacts of the 2010 Queensland floods.

Rainforest: Similar WSN systems were deployed in the far north in Queensland's Daintree Rainforest as well as a hydrological observation network in the Mitchell River catchment by James Cook University researchers. The CSIRO has also deployed a WSN in Mt Springbrook to monitor rainforest regeneration in addition to a deployment in the South Esk River catchment in the north-east of Tasmania, in collaboration with the Bureau of Meteorology and others.

Water management and agriculture: CSIRO and Seqwater developed an integrated intelligent wireless sensor network to monitor Lake Wivenhoe and its catchment that supplies the majority of south-east Queensland's drinking water. Efficient water management through sensor networks is also being developed by UniMelb, Rubicon, National ICT Australia (NICTA) and Uniwater for water information networks and irrigation control. At the same time companies such as Observant are actively supplying WSN technology to the agriculture sector for: irrigation, soil moisture and weather monitoring for crop management; water management for livestock; urban water usage metering; and managing environmental flows.

Urban Deployments: Urban IoT related deployments include WSN parking meter systems, NFC payment systems in the retail sector, while public transport systems are incorporating advanced functionality through electronic ticketing systems, real-time scheduling and time-of-arrival updates. Highway electronic tolling systems together with traffic monitoring systems and congestion maps are forming the early instances of IoT enabled intelligent transportation systems (ITS). The proliferation of consumer products and household appliances such as Smart TVs (broadband enabled) provide another medium for information access.

The State of Victoria is rolling out Zigbee enabled smart electricity meters to all premises allowing remote metering, control, flexible tariffs and energy usage feedback for consumers.



slaven@unimelb.edu.au

EUROPE

Finland

By Prof. Heikki Ailisto

Finland is actively embracing the possibilities of the Internet of Things. The strong competence in mobile and wireless communication technology is seen as a valuable asset.

Current State

Finland has a strong technological background in wireless communication technology due to the Nokia cluster and related academic research. This is seen as a great advantage when entering the IoT age. Other strengths include high competence in smart industrial machines and the energy sector, which will both benefit from the applications of IoT.

The most significant commercial deployment of IoT technology in Finland is the smart electricity metering project. All households and other consumers will have remote readable meters by 2014. Already, a major number of consumers have smart meters up and running. Other deployments are related to intelligent traffic systems (ITS), such as roadside cameras and weather monitoring. Future plans include an ITS corridor between Helsinki and St Petersburg in Russia. Home security packages including surveillance cameras and fire alarms with M2M capability are also selling well.

The Finnish R&D community has reacted to the rising importance of the IoT. The national funding organisation launched a seven-year program on ubiquitous computing and communications (Ubicom) in 2007. The program created readiness also for M2M and IoT topics.

VTT Technical Research Center sees the IoT as an important research area with significant impact and has favoured IoT related work for some time. As a consequence VTT has taken an active role in building co-operation with leading Japanese actors, such as UNL in the University of Tokyo. VTT is also a founding member in the European IoT Alliance, which fosters co-operation and advances such IoT technologies as uCode based unique identification of objects and T-Kernel embedded OS.

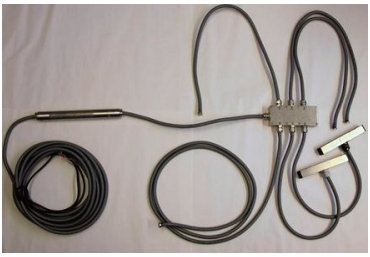
Recently, national Public Private Partnership organisation Tivit, with the support of Tekes, launched a four year IoT programme with an estimated budget of ca. 60 M€. The program is driven by multinational companies

Ericsson, Nokia, Renesas and Metso alongside a number of SMEs and research partners. VTT is the largest research partner involved, others include the University of Oulu, Aalto University and TUT. The program includes work packages for business and applications research.

Future Prospects

The IoT will have a strong impact in various industries and society. What exactly these impacts will be and which industries will change first is not yet known, but some forecasting can be done. Since the deployment of the IoT is driven by telcos and mobile communication equipment manufacturing companies, it is likely that the first wave of IoT relies on (mobile) telecommunication technology including M2M solutions using SIM cards for identification and security and GSM, GPRS, 3G and 4G technologies for communication infra. The telcos will have a significant role in opening the market due to their large customer base and ability to manage complicated billing systems. Major deployments are expected in such fields as remote metering, security and safety applications, intelligent traffic systems, retail and logistics, remote management of buildings and facilities as well as intelligent machines. Helping the elderly to live independently is seen as an important application area for the future. Experience and competences in communication technology as well as a strong base with certain industries gives the Finnish industry good position in entering the IoT business.

The Finnish research community is active in national and European arenas. VTT is not only a major partner in the national IoT program, but also very active in the European IoT Alliance, the ARTEMIS PPP initiative, EU joint research projects as well as in co-operation with Asian and American partners.



Structural Health Monitoring Unit

Energy efficient sensor module - VTT node

heikki.ailisto@vtt.fi

Germany

By Eldor Walk

EUROPE

There are various German research activities regarding the Internet of Things (IoT). Universities, research organizations, enterprises and public authorities participate in projects elaborating the future use of IoT. These projects are sponsored by federal ministries, industry organizations and even labour unions.

Application orientation characterizes German IoT research activities. Research projects especially focus on the development of scenarios, pilot applications and first practice implementations, rather than on global and more general questions, such as addressing schemes, inter-operability and standardisation issues. Notably, applications in the field of production, logistics and transport and the development of modelling and simulation techniques and tools are the center of interest. However, as part of pan-European IoT research teams German researchers also work on rather general IoT questions, such as architecture and modelling approaches. For example, there are six German partners participating in the IoT flagship project IoT-Architecture and four German organizations working in the European project IoT-Initiative.

There are four main categories of IoT activities in Germany:

1. Architecture approaches and models,
2. Application scenarios and pilots,
3. IoT enabling technologies and
4. Governance issues.

Architecture approaches and models

There are only a limited number of German activities in the field of architecture and model development for the IoT. For instance, the University of Bremen promotes the topic in cooperation with other European research institutes. This year an edited book on 'Architecting the Internet of Things',

was cooperatively published by the University of Bremen, the ETH Zurich and the University of Cambridge. It provides a general concept for a future architecture of the IoT. Definitions and frameworks are presented, research demand is identified and practical guidance for researchers and practitioners is derived.

The part project SmartOR (part of the superior AUTONOMICS project), founded by the Federal Ministry of Economics and Technology (BMWi)) aims at the development of communication and network architectures for modularised and integrated operating theatres of the future. Here 14 partners work on the development of a demonstration platform for the evaluation of technologies planned for 2013.

Application scenarios and pilots

Application-oriented research characterizes German IoT activities. Research institutes and universities as well as companies and associations aim at the development of business models, tools and strategies for future products and services enabled by the IoT.

Within the scope of the AUTONOMICS project the BMWi funds the development of a new generation of smart tools and systems that are able to network via Internet, identify situations, adapt to changing operating conditions and interact with users on their own.

With this initiative, the Ministry wants to promote research and development activities to speed up the development and broader use of ICT-based technologies and services along the whole supply chain to enhance the autonomy of user systems. Sub-projects, such as AGILITA, DyCoNet and AutoBauLog, are three examples for application-oriented research activities funded in the scope of AUTONOMICS: AGILITA aims at the development of a flexible and efficient materials flow system for use in production in small and medium-sized enterprises (SMEs) The research aim is to respond quickly to rapidly changing market situations and shrinking product lifecycles by means of flexible production capacities. DyCoNet aims at the development of new solutions to improve the general availability of logistics data in dynamically changing and international supply networks.

The project aims to utilize technologies, such as GSM/UMTS and GPS, for the transboundary networking of logistic objects. This allows the energy of self-sufficient logisitic objects, such as containers, packages and documents

to autonomously communicate with each other to create an autonomous material flow. AutoBauLog aims at integrating building machines in large civil engineering construction projects. The building machines are equipped with sensors, communication devices and intelligent software to cooperate with other 'machine team members' and to autonomously proceed to the machine-based construction processes. As a result enabling self-organisation allows building machines to respond to their current situation, improves the machines' utilization and thus, accelerates construction projects.

Next to research activities German companies autonomously explore the IoT. Companies build up the necessary knowhow and develop intelligent products based on IoT usage. For many companies this means, that they have to enter new markets and fields of activities. One example for German corporate activities in the field of IoT is the German automotive supplier Bosch. Bosch have invested more than ten million Euro in a software company and currently seek other suitable ventures. Fostering the software development for intelligent products was announced as the goal of these activities. In future, Bosch plans to connect not only cars, but household items, such as fridges to the internet. Bosch wants to do the programming for these future products independently from other actors.

There are other companies that prepare their products for use in the IoT. SAP in cooperation with the Deutsche Post; BMW with a freight container that documents and communicates the inside temperature; Siemens is exploring the development of machines, that autonomously create maintenance orders.

IoT enabling technologies

Several German companies work on technologies that enable the vision of IoT. In Germany there are several hardware providers offering RFID technology (such as Feig Electronic, Phg, Reiner SCT), satellite technique (such as OHB Systems AG) and sensors (such as Balluf, Siemens, Sick, Pepperl + Fuchs) with relevant market positions. Many of these companies participate in or support other research projects.

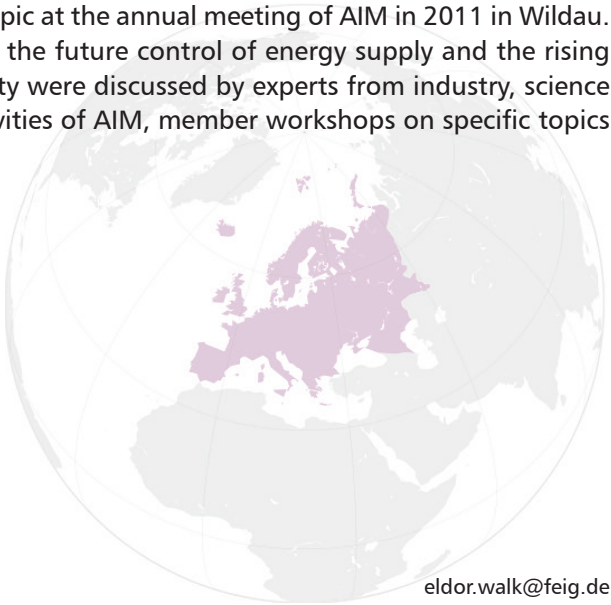
Governance Issues

Governance of the IoT is a topic that receives much attention. In Germany. The BMWi as well as the Federal Ministry of Education and Research (BMBF) have been working intensively on the topic for several years.

The ministries fund research projects and foster the industrialisation to generate economic growth. The German ministries held several events with a focus on the IoT, such as the regular cross-functional RFID-dialogue. In 2007, during the German EU Council Presidency, the conference 'Internet of Things' was hosted. Here a paper on the 'European Policy Outlook RFID' was developed. This was the first time that a framework for European policy for the IoT was defined.

In Germany, the Association for Automatic Identification, Data Gathering and Mobile Data Communication (AIM) fosters the activities in the field of IoT. Furthermore, the Informationsforum RFID (organization of German RFID users and technology providers), BITKOM (Federal Association for Information Technology, Telecommunications and New Media) and BITMI (Federal Association for IT in medium sized companies) promote IoT issues by providing information to industry, science and public institutions by means of internet, events and publications.

The IoT was the main topic at the annual meeting of AIM in 2011 in Wildau. The meaning of IoT for the future control of energy supply and the rising meaning of data security were discussed by experts from industry, science and policy. Further activities of AIM, member workshops on specific topics are planned.



eldor.walk@feig.de

United Kingdom

By Ian Smith

The Internet of Things is creating a great deal of discussion and interest in the UK. The Government's Technology Strategy Board (TSB) is investing £500,000 in preparatory studies to develop strategies for moving towards a converged and open application and services market place in the Internet of Things. Following these preparatory studies the TSB will invest up to £4 million in a competition for a demonstrator which will address collaboratively the convergence challenges and encourage the emergence of a market place for applications and services in the UK.

The funded projects cover a wide range of topics including:

The MyHealthTrainer project will develop a business case for the provision of free e-health and a fitness web/mobile application to improve wellbeing.

IoT Enabled Converged and Open Services for Transport and Logistics – demonstrating how the Internet of Things will enable the Transport and Logistics sector to become increasingly smart.

Cross Domain IoT Interchange Broker. This brings together stakeholders from the Telemedicine, Transport, Environmental Monitoring and Energy sectors and examines as a case study how data they hold individually can be securely shared to minimise theeffects of a 'severe weather episode' on individuals, the utilities, transport and wider UK economy.

Intelligent City Transportation – Infrastructure. The project will undertake a preparatory study into issues relating to an Internet of Things demonstrator in the area of Metropolitan Transport and Traffic data.

How Can SMART Home Data and Systems improve assisted living services – exploring how the future internet will facilitate convergence between home energy management, home security and telecare and lifestyle monitoring services.

The SMART Streets project will explore in detail the potential for connecting highway assets such as street furniture, road surfaces and gullies to the Internet of Things.

Consumer Convergent Retail – exploring the convergence scenarios with retail environments, stores and shopping centres.

Value Chain Analysis of the Internet of Things for the brewing industry. Loss of empty containers is an annual £50 million problem for the UK brewing industry with a lack of knowledge on where the casks are and who are their rightful owners. To address this problem a convergence of technological solutions and human involvement is seeking to tag, track and recover casks.

The TSB have also established a British Internet of Things Special Interest Group which aims to provide a forum for the promotion of business ideas and opportunities.

The SMART Identification Association is another active IoT player in the UK. They have been the co-ordinators of both the CASAGRAS1 and CASAGRAS2 EU FP7 projects and are founder members of the European IoT Alliance. In September they will stage the 'SMART IoT Summit' at Manchester United's Old Trafford Conference Centre, a high profile leading edge forum for researchers, PhD students, engineers and practitioners from around the world to present state of the art advances and innovations in the theoretical foundations, systems, infrastructures, tools and applications for the IoT as well as identifying emerging research topics which will help define its future. (www.smart-iot.org)

Many leading British Academic Institutions and commercial organisations are also playing an active part in a range of European projects.

ian@smartidentification.org

India

By Rajeev Prasad
& Balamuralidhar Purushothaman

The Global ICT Standardisation Forum for India (GISFI) has been set up with a vision to be an ICT standards forum in India. It plans to develop standards to meet the Indian requirements, as well as contributing to the evolution of global standards. The Internet of Things (IoT) is one of the many themes of focus for standardisation in GISFI.

Focus

Internet of Things is an integrated part of the future Internet and envisaged to provide a dynamic global network infrastructure with self-configuring capabilities linking physical and virtual objects through the exploitation of data capture and standard and inter-operable communication protocols.

The development of an IoT framework based on a reference architecture (c.f. Figure 1) to enable systematic capture of requirements, identification of gaps and a focussed proposal development for standardisation is in progress. The reference architecture specifies the IoT architecture and its associated interfaces aiming at an efficient end-to-end delivery of IoT services. It is aimed to identify and specify key architectural components and interfaces so that multiple stakeholders providing products and services at different layers of the stack will be able to integrate and operate together.

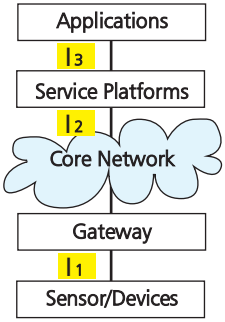


Figure 1: IoT Reference Architecture

The major focus is to develop reference architectures and specifications for protocols & APIs for enabling IoT services which have potential for mass deployment and impact in the country. Some of the use cases being considered include personal health monitoring, agriculture, food supply chain, smart metering, public safety, and transportation.

Challenges

There are several challenges arising out of India's specific requirements including (i) supporting scalable cost-effective IoT services to cater for the geographical, cultural and socio economic diversity of India, (ii) supporting non-uniform, unreliable infrastructure networks for IoT backhaul connectivity, and (iii) supporting the large number of devices and applications which have different capabilities and sophistication level (iv) robustness against impact of high device density and dynamics on the network infrastructure.

From a technology perspective related challenges include robust end-to-end data transport, flexible but efficient data exchange protocols, energy efficient communications, negotiable security and privacy and self configuration.

Future Prospects

The formulation of the IoT framework based on the reference architecture including a requirement and gap analysis with respect to specific vertical applications is in progress. Furthermore the work plan is to progress towards developing specific proposals and subsequently specifications for addressing those gaps. A reference implementation of the defined IoT framework is also part of our future plan.

rajeev.prasad@gisfi.org

Russia

By Georgij Serebryakov

Internet of Things in Russia

IoT is more a subject for "Items of News" and discussions in Russia rather than part of the reality. Actually there are no projects currently in Russia where smart tags interact with each other via preset interfaces. However at same time since the RFID technology is one of the basements of Internet of Things (IoT), and the RFID technology is in use for many popular applications in Russia, then, it can be concluded that IoT in Russia is establishing unavoidable progress.

These applications of RFID in Russia are the usage of RFID chips for civil passports, transportation tickets, medical cards, animal marks, vehicle logistics, libraries, post offices etc. Some current projects can be classified as a prototyping of elements of the future IoT. For example developing systems for monitoring automobiles using satellites; developing store chains having goods tagged with RFID.

At present there are three independent RFID manufacturers in Russia:

1. The first one is Galileo Nanotech established in partnership with the Italian company Galileo Vacuum Systems SPA (a total project cost: 43 mln. euro.), the share of Rusnano - 21 mln. euro. The expected volume of manufacturing from this venture is expected to be more than 1 billion tags a year.
2. The second project - RST-Invent has been established in St.-Petersburg together with the Systematica Group of Companies. The budget of the project will be 15 mln euro, including investments from Rusnano in volume of 5 mln euro. It is expected

that a new manufacturing plant will be placed in St.-Petersburg. In 2015 its production capacity on labels PatchTag will be above 1.3 million pieces a year, and on labels iNano – nearby 160 million pieces. Also the state corporation creates in St.-Petersburg a batch production of devices and systems on the basis of acoustoelectric and chemisorption assembles, including gauges of pressure and deformation, assembling of radio-frequency identification (RFID), high-frequency strip filters and gas alarms. The output of the project on planned targets is expected in 2015.

3 JSC "Micron", located in Zelenograd near Moscow, is the largest manufacturer of RFID-tickets and smart-cards in Russia today. it is known under brand Sitronics and makes cards for the Moscow underground on the basis of Mifare ICs.

RFID projects related to IoT

1. "Future Store" Ltd.

Rusnano, Sitronics and X5 Retail Group signed a partnership agreement for a "Future Store" project in the middle of June 2011. The partners will invest $13.5 mln during two years. Rusnano share will be $4 mln. The store will be launched in 2014-2015. The project will take into account features of radio frequency identification, such as the effect of radio waves transmission through products containing liquids and metal surfaces or materials. The problem raises the possibility of losing key benefits of RFID technology in comparison to a bar code, such as the ability of group reading (identification of all buyer's goods in the cart) and the ability to read the product without the need for line of sight (when one covers the packaging of another item). There are also difficulties with tags attached to the packages. The group expect the technology of chipless tags, which is currently being actively developed will provide the solution in the coming years. Kovio recently received $15 million to develop new technology. Using these tags, it will be possible to attach them to the package by a special printer, and it can be done on a normal production line without the use of expensive equipment

Photos show President Dmitry Medvedev when he was buying goods with RFID tag using the robotic cashier (RFID readers inside corps). President Medvedev said that this was a very promising development but it may have difficulties in the beginning because people trusted live cashiesr more than the robotic ones.

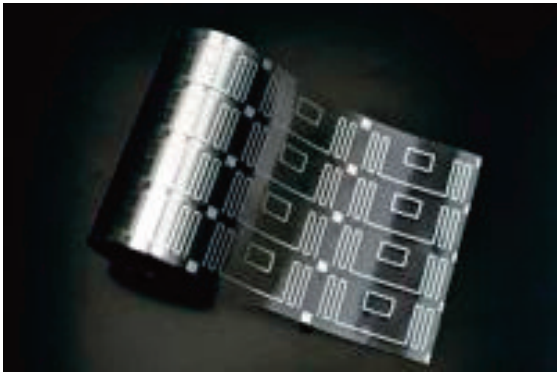
2. Rusnano's project launches manufacturing of new generation RFID tags

RUSNANO's project company "PCT-Invent" has launched its RFID tags (Radio Frequency Identification). At the first stage, the company launched a family of labels, tags, iNano, which includes BiblioTag, LogTag and DrugTag. DrugTag is ideal for labeling of drugs in glass containers.

The BiblioTag is intended to delivery the tagging into library collections and archives. This label, as well as LogTag, can also be used for tagging of items in logistics and supply chain management. Because of the original designs of antennas with high gain, these tags can read and write information over long distances. By the end of this year, "PCT-Invent" plans to ship 10 million RFID tags of iNano,'s family and by the end of 2013 to double manufacturing capacity. The main applications of new tags of the project company will remain warehouse and transportation logistics, retail, tagging of libraries and archival collections, supply chain management.

The Russian origin of the chips has also significantly simplified their use in the public sector, including law enforcement agencies. According to specialists of the company, the development, launch and production of domestic new-generation chips will enable "PCT-Invent" within the next 3-5 years to take a significant share of the domestic market because of their

high performance and lower cost to the domestic market. The total project budget is 15 mln euros, including investment by RUSNANO in the amount of 190 million rubles. In addition to the iNano's family of RFID tags, the company also produces a versatile passive PatchTag RFID tags, which are among the leaders in the range of registration.



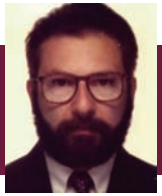
3. R&D Projects for universal UWB RFID tags using different types of modulation.

In our opinion, the existing RFID tags (UHF RFID Gen1, Gen2) cannot be applied to implement the IoT idea because of the physical limitations and weak power efficiency. So we have work under development for RFID techniques using the advanced communication technologies. The new RFID tags should have the following features:

- Very low error probability
- Multi frequencies performance
- Excellent noise resistance
- Extra low cost
- Low power consumption.

To meet these requirements Research Institute Sitronics Labs has launched a research project entitled “Development of new advanced RFID technology” where OFDM and dynamically chaotic signals approaches to RFID design are examined.

GSerebryakov@sitronics.com



SOUTH AMERICA

Brazil

By Jose Amazonas

Introduction

Since June 2010, when the CASAGRAS2 project was launched, important changes have occurred in the Brazilian scenario. Many of these changes have been driven by CASAGRAS2 with a number of awareness raising activities around Brazil and beyond.

In this report we have included reports from a number of Brazilian institutions. We invited researchers from Argentina, Colombia, Chile, Peru, Venezuela, Panama and Mexico. We were only successful with two contributions from Argentina. This is perhaps indicative that whilst IoT is becoming more known in Brazil it is not as widely known or adopted in these other countries.

Architecture approaches and models

Most of the applications in Brazil cannot be classified as typical IoT applications. They are applications that use RFID for AIDC but don't access the Internet to produce any action on the object or the environment. More properly they should be called IoT-latent applications. The Brazilian market is completely dominated by GS1 and its architecture is the most used. There is a clear need to introduce the Brazilian market to alternatives by means of workshops, courses and dissemination activities.

Naming and addressing schemes

Naming and addressing schemes are those defined by GS1. For military applications it has been realised that GS1 naming schemes are insufficient because there is a need to comply with NATO specifications.

As we are dealing with IoT-latent and islands of applications there is no need to employ search and discovery mechanisms.

Governance issues and models

The University of São Paulo (USP) has launched the Innovation Olympic Games and Prof. Maristela Basso has proposed the development of the project Modelo De Reulamentação Jurídica e Gestão da internet das coisas (IoT) - Model for IoT Juridic Regulation and Governance.

The document states in English

It is exactly at this point that Juridical and Social Sciences may provide their contribution. Our intent is to offer a product that allows for the integration of the technological advance with minimal ethical patterns of social coexistence and, in addition to respect a citizen's guarantees and fundamental rights, in a concentrated or diffused way.

We may say that, in this case, Brazil is taking the lead because such a project is very practical leaving behind empty discussions and moving towards the development of a real framework of governance.

It is important to emphasize that CASAGRAS2 has been the driving engine of the project that says:

Also for this reason we have associated to the CASAGRAS2 work that, in Brazil, is coordinated by Prof. José Amazonas and Escola Politécnica of USP, providing juridical consultancy and advice.

Inter-operability issues

The company Perception is a partner in the Probe-IT FP7 project. One of the tasks assigned to this company is to prepare an IoT interoperability event in Brazil in the beginning of 2013. It is also worth noting that HP has a RFID laboratory that is used in certification processes and CPqD-Telebras has a RFID conformance test laboratory.

Privacy and security issues

This is a topic that provokes great interest and concern in Brazil. A conference on Data Privacy and Security was organized in October 2011 by the CGI (Comitê Gestor da Internet - Internet Steering Committee) to deal

with the theme. The Science and Technology Commission of OAB-SP (Organização dos Advogados do Brasil - Lawyers Organization of Brazil) is establishing a study group to lead the discussions. It is expected that this group will be coordinated by CASAGRAS2.

Application scenarios and pilots

The 2nd Brazilian Conference on RFID and IoT was held in October 2011 attracting around 200 participants. Most recent developments were presented (see www.congressorfid.com.br). All applications are IoT-latent and no real IoT application has been developed so far. Those presented included:

1. control of clothes for the fashion industry;
2. control of the Aeronautic uniforms sold at their own stores;
3. parachutes life cycle control;
4. insertion of intelligence in the medical procedures;
5. national system of vehicle identification;
6. insertion of intelligence in industrial fixers that are used in oil extraction platforms;
7. intelligent Abadá as a tool for marketing, access control and means of micro-payments. Abadá is the garment used by people during the carnival in Salvador-Bahia.
8. trace and tracking in forests;
9. inventory control in hospitals;
10. control of juridical documents;
11. RFID identification and management of children in schools;
12. automatic identification and control of athletes in outdoor competitions

Standardisation/pre-regulatory research

It is recognized as an important topic but the participation in regulatory bodies is seen as very expensive. So the companies adopt a position of long distance watchers. I am not aware of any standardisation and pre-regulatory research being done in Brazil besides the GS1 activities.

IoT enabling technologies

CEITEC, the state owned semiconductor company in Brazil, has developed a first RFID chip that will go into commercial production in the coming months.

Cognitive technologies for IoT

There is a new project about IoT based energy efficiency for public buildings that is being submitted for funding that will use cognitive technologies.

Brazilian Competitiveness in IoT Forum

On April 9th, 2012 the Brazilian Competitiveness in IoT Forum was launched. It includes participants from different segments: private companies, academia, funding agencies and government. Main objectives:

1. identification of barriers that prevent a faster adoption of the IoT technology in Brazil;
2. definition of concrete measures that should be taken to leverage the development of IoT applications and services;
3. IoT dissemination and education.
4. The main platform of the forum is its website: www.iotbrasil.com.br.

Contributions from other institutions

Mr. Paulo Jarbas Junior has more than 10 years experience in RFID-related applications development and deployment. Presently he is an independent consultant and owner of the company "Relacionamento Professional".

In general the Internet of Things is the extension of the Internet to the physical world in which it becomes possible to interact between objects and autonomous communication. There is great interest due to the potential that this concept can be applied in building new business models. It is revolution technological that represents the future of computing and communications, whose development depends on the technical innovation of wireless sensors and nanotechnology. Advances related to miniaturization and nanotechnology mean that small objects will have the

ability to interact and connect. Our country awakens to issues related to developments in science and technology initiatives especially in nanotechnology field.

The benefits of integrated information between industrial products and objects are possible from sensors that detect physical changes. These transform static objects to dynamic, combining the intelligence environment and stimulating innovations products and new services. RFID technology is one of the most promising in this regard. In the Brazilian market, these systems are being used in several projects. The main market segments that are using RFID technology in Brazil, with our solutions are:

- **Industry -** focus on productivity solutions,
- **Logistics -** focus on track, trace and mobility,
- **Professional Services -** focus on quality assurance to solution provider customer services,
- **Entertainment -** focus on innovation and integrated consumer experiences,
- **Consumer goods -** traditional use of RFID technology in the supply chain,

There are initiatives highlighted in the health, education and security, combining other technologies to special projects with high added value.

The main challenges are related to infrastructure, security, applications and services, particularly in relation to communications autonomous systems where the current Internet resources are inadequate.

The social impact of the use of mobile devices connected to networks, integrated systems management suggest new challenges related to issues addressed by the semantic web from the responsible use of resources and knowledge about the Internet of Things. Reflections on ethics and sustainability can give legitimacy and bring the concepts being developed by IoT to reality.

Electrical Engineering Department of the Catholic University – PUCRS – Porto Alegre –Brazil. The research group is coordinated by Dr. Rubem Dutra Ribeiro Fagundes. This research group is a reference in Brazil for the development of e-health pervasive computing applications.

MOSAIC (Modular Event-based System for Pervasive Computing in HealthCare Environments).

Focus - MOSAIC is an R&D project whose goal is the development of a modular event-based system for pervasive computing in healthcare environments. The project is a fusion of Information and Communication Technology (ICT) research areas, working from middleware systems and software frameworks (to process complex event data in RFID applications) to autonomous models and platforms (HW/SW) for data integration and device management in pervasive and heterogeneous environments. This technological fusion is based on two computational model approaches that determine different levels of abstraction in the structure of the system architecture.

Challenges - The emergence of new computing niches and market trends (IoT, WoT and Next Generation Internet) and advances in the maturity of related technologies and business processes in pervasive environments are issues that influence the motivation of this project.

The challenges are addressed to the following functional requirements:

- Mitigate existing gaps in the specification standards of the EPCglobal for both middleware systems specifications and services specifications for data sharing between different business organizations;
- Adaptive system support for dynamic configuration of system modules (e.g. data management and integration capabilities) according to application business rules;
- Collaborative support for system scalability in terms of complex event processing and business events integration;
- Pervasive system platforms (HW/SW) able to integrate and manage healthcare devices as well as to provide pervasive networked services;
- Pervasive services for a better integration of business processes between hospitals, health stations, houses and ambulances;

  Pervasive services for different levels of data enrichment ensuring each system abstraction layer aggregates some kind of information used to trigger specific rules in the diffused logic.

Future Prospects

The research directions cover the following topics:

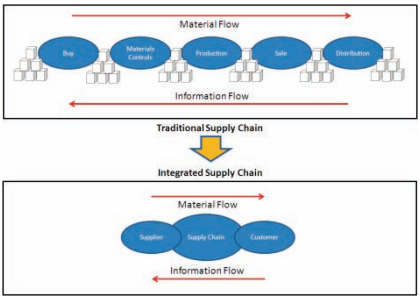
- Fusion of RFID, WSN and ubiquitous/pervasive middleware systems to handle pervasive application requirements;
- Fusion of Semantic Web for device integration (e.g. pattern of services and resources) and extensions of EPCIS standards based on SSN/WC3 and Domain Ontologies for information contextualization;
- Complex Event Processing (CEP) techniques for systems integration in event-based systems (e.g. Stream Processing Engines or Rule-based Engines);
- Internet of Things (IoT) and Web of Things (WoT) approaches aiming at devices interconnectivity (IPv4/IPv6) through real-time and lightweight embedded approaches (e.g. RESTful principles, smart gateways, server push and notification technologies, WS-* and Web standards;
- Use of embedded systems virtualization techniques to improve both complex functionality in real-time and resource constrained devices, privacy and security as well as heterogeneity of connectivity.

Flextronics Institute of Technology and HP do Brasil - The Flextronics Institute of Technology and HP do Brasil have a very close relationship. They run the RFID Center of Excellence (COE). The contribution has been sent by Samuel Bloch da Silva in the format of a case study about Integrated HP Supply Chain Model in the Internet of Things.

Present research describes a model for the process of replenishment of HP Ink Cartridge integrated with internet of things

Future supply chains will need an element to serve as a connection between the physical parts of this process, and virtual entities to improve agility in supply chains. In other words, the structure of supply chains in general must evolve in order to improve the participation of each stakeholder. Stevens already expected in 1989 that a transition from traditional to integrated supply chains is necessary (Figure 1).

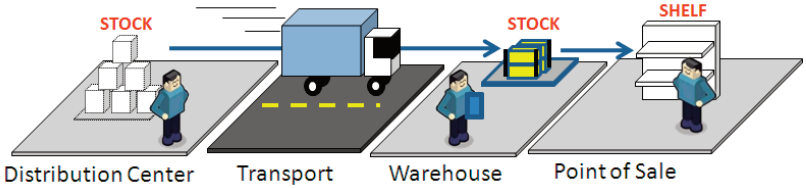
As shown in Figure 1, Stevens suggests a vision where improved information sharing eliminates unnecessary intermediate stocks. This present case study proposes a model to improve the level of integration in a supply chain scenario for HP Ink Cartridge, where the products are identified by RFID technology and information sharing through internet.



1.1 Fig. 1. Traditional vs. Integrated Supply Chains (adapted from [1]

1 Statement of the Problem

Based on the design of traditional supply chains suggested by Stevens in Figure 1, we created a generic model to characterize the current HP supply chain process (Figure 2):



1.2 Fig. 2. - Traditional Replenishment Process in the HP Supply Chain

The model shown in Figure 2, characterizes the problem to be analysed, especially in regard to costs of the low efficacy presented by traditional models.

Christopher [2] also suggests that supply chains of the future will need to be "orchestrated" in a network that creates value to end customers. This means that systems and processes need to be developed to consider the perception of consumers for products. In the same way Uckelmann et al [3] believes "the automatic identification of things and improved data handling capabilities allow individual product identification where we have previously been limited to types of products or batch identification". On the other hand, we'll need different human interfaces to release the full potential in the forefront to exploit the business opportunities. In this case, Ink Cartridges will be worked over the "internet of things" to run the replenishment process over the HP supply chain . This will mean that thousands of points

of sale will be able to automatically send replenishment orders. In this case ink cartridges will bridge the gap between information technology and objects thus information transparency.

2 Proposed Solution

The goal is to propose a model for automatic replenishment of HP Ink Cartridge at the point of sale (Supply Agent), shown in the Figure 3:

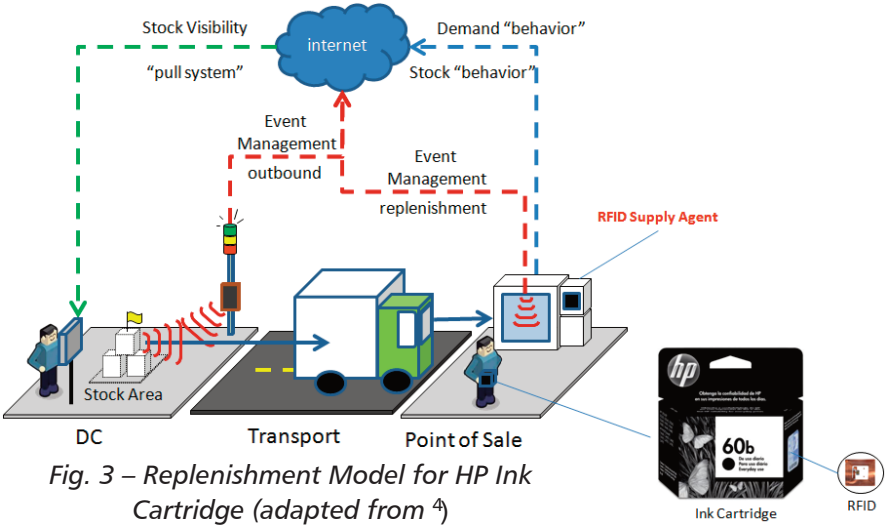


Fig. 3 – Replenishment Model for HP Ink Cartridge (adapted from [4])

In this model, RFID technology on the ink cartridge can confer behavior to increase interconnectedness of electronic devices using a common information infrastructure. In addition, the proposed solution provides feedback to the high-level systems about adjustments necessary by the realities of more detailed operations. This new model is the inspiration for uncovering new ways to improve the operations on this manufacturer.

References

1. Stevens, G. C.: Integrating the Supply Chain. Int J Phys Distrib, 19(8), 3--8 (1989)

2. CHRISTOPHER, M. Logística e Gerenciamento da Cadeia de Suprimentos – Criando Redes que Agregam Valor. Ed Cengace Learning, 2009.

3. UCKELMANN,D. , HARRISON, M. , MICHAHELLES, F. . Architecting the Internet of Things. Springer. 2011

4. SILVA, S. B.; SILVA, I. B. ; VILLAR, R. S. G. . Desenvolvimento de um Modelo Teórico de Ressuprimento baseado em Agentes de Suprimentos, RFID e Lean Manufacturing Estudo de Caso: Cartuchos de Tintas HP. X Simpósio Brasileiro de Automação Inteligente. São João del Rey. MG. 2011

joserobertoamazonas@gmail.com

SOUTH AMERICA

Argentina

Universidad Nacional de La Plata (UNLP)

The Universidad Nacional de La Plata has experience in ad-hoc and wireless sensor networks and is working in several IoT-related activities. The information has been provided by Prof. Javier Díaz. The contribution was received in Spanish and has been translated into English

Eduardo Sosa's PhD thesis in Informatic Sciences at the Informatic School of the Universidad Nacional de Plata entitled "Contribution to the establishment of a global network of interconnected wireless sensors" is presented. It has been supervised by Stefan Luebeck and co-supervised by Javier Díaz. It was presented in June 2011 and got a grade 10/10.

RELATED PROJECTS

The project "Towards a global network of interconnected sensors. An Argentine-German experimental test", within the realm of the Scientific-Technologic Cooperation Program between the Ministry of Science, Technology and Productive Innovation of Republic of Argentina (MINCYT) and the Bundesministerium für Bildung und Forschung (BMBF) of Germany.

Plans are underway to organize an IoT event in the university this year and to build a sensor testbed to enable experimentation and integration with existing testbeds in Europe.

As far as RFID technology developments are concerned we are evaluating alternatives to provide technological consulting services requested by the government of the Buenos Aires province.

In respect of the integration of mobile systems, GPS, SMS, Internet, with sensors (in the future) and information systems we are starting to develop an information system for the city of La Plata.

Finally we are joining a project of SOLAR energy generation, and its integration with the electrical energy distribution network. We are evaluating how it could be possible to integrate it with the information and monitoring system.

Universidad Tecnológica Nacional (UTN), Argentina. The research group at UTN since 2004 focus on data networks and embedded systems. The information has been provided by Prof. Gustavo Mercado, the Research Coordinator.

The gridTICs (Grupo de I&D en Tecnologías de la Información y las Comunicaciones - Information and Communications Technologies R&D Group) is a group approved by the UTN (Universidad Tecnológica Nacional). Since 2004, our topics of interest are Data Networks, Embedded Systems and Software Quality. We are seven researchers and teachers, five researchers, four postgraduate students and several fellows' students. The group is located in the FRM (Facultad Regional Mendoza - Mendoza Regional School) of the UTN, in Mendoza Argentina.

RESEARCH AND DEVELOPMENT PROJECTS

LIVRES Analysis and evaluation of relevant features of wireless sensor networks applied to the management and sensing of precision agriculture

SIPIA Net: Wireless Sensor Network for Agronomical Research Involved Institutions: gridTICS UTN FRM

Optimization of irrigation systems using wireless sensor networks

Involved Institutions: INTA Mendoza – gridTICS UTN FRM

Integration of photovoltaic generation in the distribution system of electricity within the city of Mendoza. Involved Institutions: Departments of Electronics and Electromechanical Engineering UTN-FRM, CLIOPE and GridTics

Doctoral work in progress:

- "Design of machine learning techniques applied to environmental characterization of the Andean Basin" Involved Institutions: IANIGLA Conicet Mendoza - GridTICS – UTN FRM National University of Technology
- "Analysis and design of algorithms in low power networks applied to extreme conditions in the Patagonian Andes Mountain"

  Involved Institutions: IANIGLA Conicet Mendoza - GridTICS–UTN FRM

NORTH AMERICA
U.S.A

By Steve Halliday

The Internet of Things is gathering momentum all over the world, and the United States of America is no different. Unlike other countries, there has been no government intervention with the availability of funds or incentives to get companies involved in the technologies that are involved. This has not prevented the increased involvement in the IoT, especially by the larger companies. As an example of the companies and their efforts in the IoT we can look at:

Cisco

Cisco is known by many people as the connectivity company that provides their computer networking capabilities. This insight into the networking of computers seems to have led Cisco to see the IoT as a natural progression. Their blog at http://blogs.cisco.com/tag/iot/ talks about some of the issues that they see in the connected world. The white paper on how the next evolution of the Internet is changing everything (http://www.cisco.com /web/about/ac79/iot/index.html) talks about the need for a "network of networks" and the evolution of the use of the internet into something more than just an email and research. They suggest that the IoT is the first real evolution of the internet. The Cisco view of the IoT is at http://blogs.cisco.com/news/the-internet-of-things-infographic/ .The blog entry at http://blogs.cisco.com/sp/moving-beyond-the-internet-of-things-in-2012/ shows the areas of involvement that Cisco has.

IBM

The computer giant has been involved with the IoT longer than most. They have an openly stated goal to produce a completely new world-wide web, one comprised of the messages that digitally empowered devices would send to one another. The video shown at **http://www.youtube.com /watch?v=sfEbMV295Kk** details the IBM thoughts on the IoT and the growth of the IoT. Many are familiar with the IBM Smarter Planet catch phrase and the Smart Home and Smart Grid projects that IBM are involved with. In January 2010 IBM CEO Sam Palmisano gave a speech in London where he stated that IBM had already developed 1,200 "smarter solutions" **(http://www.ibm.com/smarterplanet/us/en/events/sustainable_developmen/12jan2010/).**

HP Another computer giant Hewlett Packard is investigating sensor networks and how they can be brought together in networks to enable the IoT. The CeNSE (Central Nervous System for the Earth) project has been a key factor in understanding how we can look at the world in different ways – explained here (http://h20621.www2.hp.com/video-gallery/us/en/corporate/environmental-sustainability/1283818680001/ cense-sustainable-brands-keynote/ video/ ?jumpid=reg_r1002_usen). HP have partnered with Shell to look at the applications of sensors to the petroleum industry.

Google The internet search giant operated PowerMeter, an online tool that allows users to view and manage their electricity usage (http://www.google.com /powermeter/about/). Although this was closed down in late 2011, the results from the work showed the importance of access to energy data. Today Google X is the location of many Google projects that are based around the IoT (http://www.washingtonpost.com /business/technology/what-is-google-x/2011/11/14/gIQAfR06KN_ story.html).

IPSO Alliance Based in Colorado Springs CO, USA the Alliance's mission is to establish the Internet Protocol as the network for the connection of Smart Objects by providing coordinated marketing efforts available to the general public (http://www.ipso-alliance.org/). Currently with over 50 members from around the world, this organization is looking for ways to promote IoT.

USNAP Alliance Another US based organization, the USNAP Alliance (Universal Smart Network Access Port), is looking at ways to create connectivity standards for the Home Area Networking to link with smart meters (http://www.usnap.org). With 40 members (including Google and GE), this organization has created a specification which supports many communication technologies.The above list is just a brief snapshot of the work underway in the USA regarding the IoT. While the US may not have received the governmental grants and press coverage that other countries have seen, the impetus is no slower and work is progressing towards the ultimate connected goal.

steve@hightechaid.com

Overview of current IoT work and toward the Future IoT

By Ryo Imura, PhD, Hitachi Systems, Ltd.

The origin of "IoT" proposed by Kevin Ashton could be traced to the concept of "Computers Everywhere" (by Ken Sakamura) and also "Ubiquitous cComputing" (by Mark Weiser), and it has introduced a drastic change from the Electronic Society to a Ubiquitous Society where the communication revolution would be extended to object-to-object. IoT performs an essential part of Smart Systems and can realize an Innovation of traceability products to keep tracking and tracing the data such as "when", "where" and "what". Giving a digital identity to the objects by using an electronic coding such as "ucode" could be one of the keys for the Ubiquitous IoT Network.

Furthermore IoT has a huge impact upon the daily lives of people and will be expected to bring about many applications in various service & business domains such as Energy, Transportation, Industries, Building, Home & Consumer, Retail SCM, Healthcare and Security/Safety etc.

The most essential point of IoT deployment will be how smart and how beneficial such systems would be for the People and Society. So we should make a great effort to show how IoT Smart Systems can be beneficial for both people and society through the focused pilot projects.

Based on such background, several ventures and Business Divisions have been established in the HITACHI group for the realization of a Ubiquitous IoT society from as early as 2001. The typical example is our Security & Traceability Division, where the major targets seek to accomplish secure identification & authentication systems by using Radio Frequency Identification (RFID) and Biometric technology to demonstrate Food Traceability, Document Management and Secure Entrance Control in the hospital.

Currently these activities have been expanded to accommodate the basic business concept of "uVALUE" in our IT system company, Hitachi, Ltd., which creates a new value for the customers in the next generation network

system and also contributes to the variety of secure ubiquitous access to bridge the real world and ICT systems. The Hitachi group has taken part in many national projects on IoT and the Ubiquitous Initiative from the earliest stage. Those early activities also lead to new business strategies in our Smart City and the major Social Innovation Business.

Another key point of IoT deployment would be International co-operation with several partners such as the EU CASAGRAS 2 Project

1. to exchange ideas and learn about different research approaches for achieving a public acceptance of new technology,
2. to exchange the best practice and share the results of each project
3. to expand the practical application and create the various services with sharing know-how & experience.

Through the focused projects and also the international co-operation, the most important common elements such as agreeing a basic architecture for IoT and global standardization will be capable of developing and accelerating the creation of a Sustainable Society, and we believe an "Internet of Everything" could be realized in the relatively near future.

Vice President and Executive Officer, Hitachi Systems, Ltd.

ryo.imura.wo@hitachi-systems.com

IoT - Propelling the Networked Society

By Jan Höller & Jari Arkko
Ericsson

The Networked Society

Ericsson is known for having a vision of 50B connected devices. This builds on the proposition that anything that can benefit from being connected will be connected, and this is the foundation for the Networked Society. Today 50B seems perhaps even a conservative prediction.

The Networked Society embraces all stakeholders: people, businesses and society in general. The different stakeholders have different interests and drivers for adopting ICT solutions. For people, it is more about lifestyle, fun and "wants" rather than "needs". Enterprises are exposed to an ever increasing competitive business environment requiring cost reduction, branding and differentiation. From a society perspective, saving energy, sustainability, efficiency and safety are important drivers.

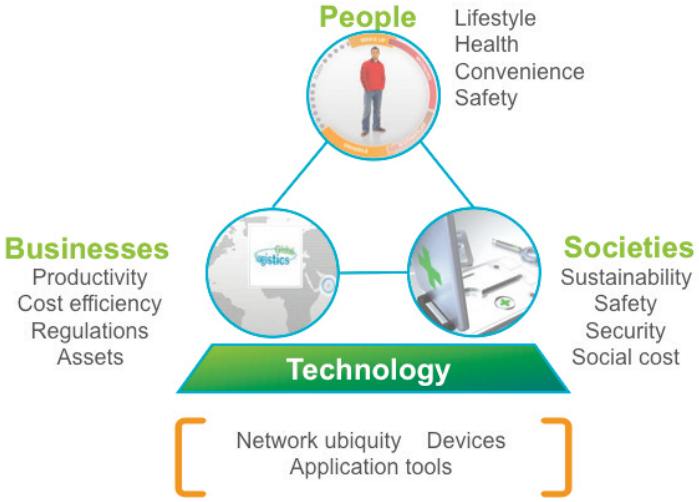


Figure: Drivers and foundation for the Networked Society

The underlying fundamental enabler that makes this happen is the technology evolution. The key enabling technologies are ubiquitous connectivity, smart devices, and the ability to integrate smart objects in different applications. We are now at the meeting point in time where viable technologies are available at the same time as the concrete needs from the different stakeholders have emerged.

Pushing the Limits of M2M and the Intranet of Things

The networked society builds on personal communications as well as communication embedded in real world objects or things, i.e. both M2M and the Internet of Things, the latter representing the bulk of future deployed devices. The things we are interested in are very diverse and range from industrial machines to vehicles, appliances, lights, and buildings. The things are not limited to tangible objects; smart places and environmental observations are very important for many applications.

The application space is very wide. Improvements in traffic safety and traffic management is one. Transforming the electricity grid to a smart grid, driven by new requirements like energy efficiency, microgeneration, electrical vehicles, and consumer energy awareness is another. Agriculture, water management and environmental monitoring are other less technology intensive usage areas.

These applications are already being deployed today, but the focus is on single applications and most of the time characterized by "one device - one application". In some cases, even special networks are being built for single applications. We do not believe this will lead to sustainable business in the end.

How can we benefit from the ongoing development, yet allow a richer, more open architecture to emerge? Can we reuse what we are deploying? In order to do this we have to open up or even break the current application silos.

The Internet of Things

Instead of deploying devices with a single purpose or application in mind, we should allow devices to serve multiple applications, and applications to employ multiple devices. We should also open up and reduce application

development costs and time to market by moving away from proprietary and legacy technologies and solutions.

The proposition is to move to a horizontal system with a focus on reuse of common enablers, and a true transformation to using the benefits of IP and Web technologies all the way, even in the tiniest device. Connectivity, access to data, data representation, and processing and storage elements are important common capabilities in such a system.

This will allow a truly open market to develop and deploy the different solution components, allow commodity components to be used, and enable easier interconnection with existing applications and Internet services.

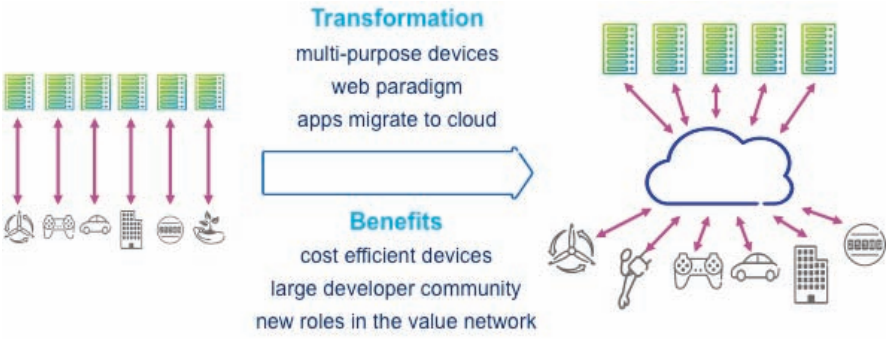


Figure: Moving from silos to an Internet of Things
Solutions for the Internet of Things

Needless to say, devices are instrumental for the Internet of Things. We are already witnessing the deployment of a range of different devices. However, this development is only at its beginning, and to get to a true mass market, several technical and commercial challenges have to be solved. Costs for developing and manufacturing the devices needs to be further reduced. The availability and compatibility of the devices to different environments needs to improve. The ease at which the devices can be deployed has to improve.

These challenges relate in part to ongoing technology development (such as advances in microelectronics and sensors), agreements on standards, reaching economy of scale, and business ecosystems to produce the right equipment at the right price. But one key issue is that the market is currently quite fragmented. Each industry vertical has developed its own technical solutions without much regard to reuse and commonality. In particular, for many industries (such as building automation), the current solutions inherit

much from past legacy networks whereas off-the-shelf Internet technologies would in many cases have provided a much more flexible and inexpensive platform. In addition, even in a single industry sector the number of alternative solutions is large. For instance, in building control and automation, there is KNX, LonWorks, X.10, BACnet and ZigBee to name a few.

What is needed

> What is needed is an architecture that is based on IP, a common set of application tools, and a reasonable set of link layer solutions. We belive that we should start by putting IP into even the smallest devices. Today, IP can run in very constrained devices and also in very constrained environments.[1] The industry is already on this track as demonstrated by momentum in product releases, standards, and industry alliances such as the IPSO Alliance.

From a commercial standpoint, it is also important to build on link layer communications that support multiple applications. Deployment of new IoT devices on existing networking infrastructures is a natural requirement.

Furthermore, we should turn to widely accepted development tools. Today, development is often done with proprietary tools. Going mainstream means that we can make use of the thousands of developers out there. To this end, open APIs are also important, and the prospect of AppStores for IoT devices is attractive.

A key concept is that of embedded web services. Embedded web services is the means to get the valuable data in and out of the devices, using a well established technology that is widely used by many developers. It will also ease the integration to existing Internet services and Enterprise systems. Variants of the Web Services model suitable for the tiniest devices have already been defined. For instance, Constrained Application Part (CoAP)[2,5] employs the REST paradigm but employs a more lightweight solution than HTTP.

It is also necessary to make simple profiles of the sensor data and there are efforts in this direction from both the research community and in standardization. CoRE link formats [3] combined with SenML [4] is one example. Examples of more heavy profiles that are dedicated include ZigBee Smart Energy Profile 2.0 [6], which basically is a vertical application profile

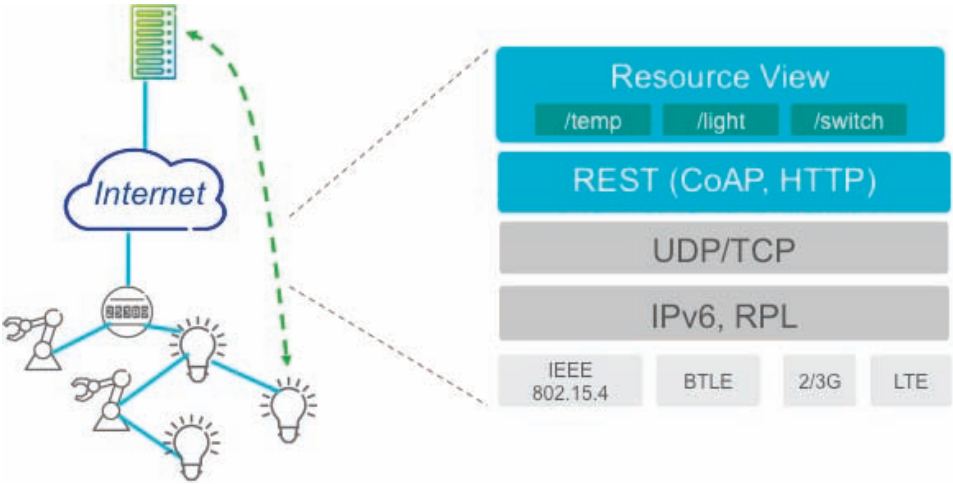


Figure: The Embedded IP Toolbox.

that does not differentiate between the data and the application in which it is intended to be used.

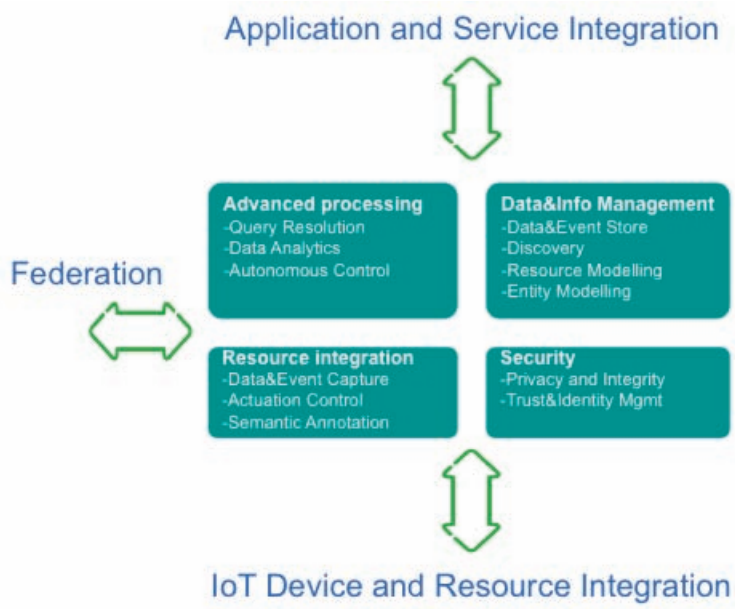
Appropriate cloud-based application enablement services is required to ease integration of IoT resources in applications. These include managed connectivity services, IoT device management and IoT resource management. IoT resource management includes discovery and directory services, data capture and integration as well as IoT data and event processing like storage and stream processing. It is important that applications can expose their information to others, discover what other resources exist, and control how their own information is distributed further and federated.

Figure: Capabilities of application integration of IoT resources

Moving towards an Ecosystem for the IoT

Our vision of the Networked Society is not just about technology. It is equally important to create an ecosystem of device vendors, application innovators, network operators, infrastructure vendors, cloud service providers, and others to create a feasible business model that does not require application builders to excel in every area.

Ericsson takes a holistic view on the Internet of Things by driving the vision, the mentioned technology evolution as well as engaging and driving the



necessary ecosystem formation. We also provide key enabling solutions to make the Internet of Things happen, like managed connectivity services for IoT devices via our Device Connection Platform and turn-key systems integration activities towards different industry sector applications. The Ericsson approach is to ensure that all the necessary parts exist for the stakeholders and user to benefit from the Internet of Things.

References

1. "Interconnecting Smart Objects with IP", A. Dunkels and JP Vasseur, Morgan Kaufmann/Elsevier 2010, ISBN 978-0-12-375165-2

2. "Constrained Application Protocol (CoAP)" , Z. Shelby, K. Hartke, C. Bormann, B. Frank. Internet Draft draft-ietf-core-coap (Work In Progress), IETF, March 2012.

3. "CoRE Link Format", Z. Shelby. Internet Draft draft-ietf-core-link-format (Work In Progress), IETF, January 2012.

4. "Media Types for Sensor Markup Language (SENML)", C. Jennings, Z. Shelby, and J. Arkko. Internet Draft draft-jennings-senml (Work In Progress), IETF; January 2012.

5. "Constrained RESTful Environments (CoRE) WG", http://tools.ietf.org/wg/core.

6. "ZigBee Smart Energy Profile Specification", Version 2.0, ZigBee Alliance, to be published

Jan Höller, Ericsson, jan.holler@ericsson.com
Jari Arkko, Ericsson, jari.arkko@ericsson.com

Remote Control and Monitoring with IoT in Korea

By Byeong-Sook Bae

KT, the leading Telecommunication and Internet company in Korea, defines a smart farm as a cultivation system that can save the cost of production and enforce the quantity and quality of crops by turning data into knowledge and elaborating 'remote control and monitoring' with IoT.

KT has been looking at opportunities for convergence of business among various industries. The convergence between IT and agriculture is one of them. Background to the strategy is as follows:

- Korea has been seriously influenced by climate change that could amplify the range of weather fluctuation. As a result, the price of crops becomes unstable. Since the average difference of air temperature between winter and summer in Korea is about 29℃min to 37℃max, Korean farmers should pay more energy cost. Therefore a year-around plant production system which is independent of weather or climate change is required.
- Although causes differ, most nations are faced with employment problems. In Korea, the baby boomer generation - babies born between 1955 to 1964 - has created severe employment problems. Population ageing and urban-rural differences in Korea have given rise to the desolation of the rural community. Despite efforts to solve these issues, the government has not found a good solution. KT thought that the smart farm could provide an opportunity to solve these issues.
- Although facility-based horticulture such as the 'Plant Factory' has many good properties, it also has some weak points. In nature plants generate more O_2 than CO_2, but in the artificial farming system, more CO_2 is generated than O_2. Since the Plant

Factory has many facilities such as cooler, boiler, lighter, fan and pump, they consume much energy. Therefore, the energy efficient farming system offers a promising business opportunity.

Figure 1 – A layout of our solution
Figure 1 – B Control on Smart Devices

KT, developed a remote control and monitoring solution for the smart farm in 2011. The solution can monitor and control plant factory on mobile app as well as the web. Figure 1-A shows the layout of the solution. Figure 1-B shows a promotional material prepared for the world IT show held in Seoul, Korea, in May 2011. The main features include:

- Monitoring and Control for growth environment: Temperature (air, water), Humidity, CO2, nutriment(pH, EC), Light Intensity, door on/off state, rainfall
- Spreading growth beds in a row in the greenhouse, and piling them up in small houses during the cold nights. With a smaller surface area, the solution can reduce heating/cooling energy to 1/10 compared with the normal plastic film greenhouse.
- CCTV monitoring
- Control and monitoring by web over PC and app on smart devices

The solution has two distinct benefits. Firstly, most of computer-added cultivation solutions can control and monitor the environment automatically, but those are locally operated. On the contrary, the KT

solution remotely controls and monitors the environmental condition of plants. Furthermore, it has been designed to collect sensing data from many factories across Korea at the same time. In order to have that property, KT standardized the protocol and data format between server and gateway. This led them to derive the optimum growing conditions from DB very quickly.

Secondly, our solution is scalable and extendable. In order to have scalability and extendibility, they adopted Lonworks (ANSI/CEA-709.1) which is a networking platform specifically created to address the needs of control applications. Lonworks protocol is one of several data link/physical layers of the BACnet ASHRAE/ANSI standard for building automation. KT have a plan to upgrade the solution as in figure 2. In that scheme, the smart farm will be controlled by real time information including price, customer order and cost effectiveness.

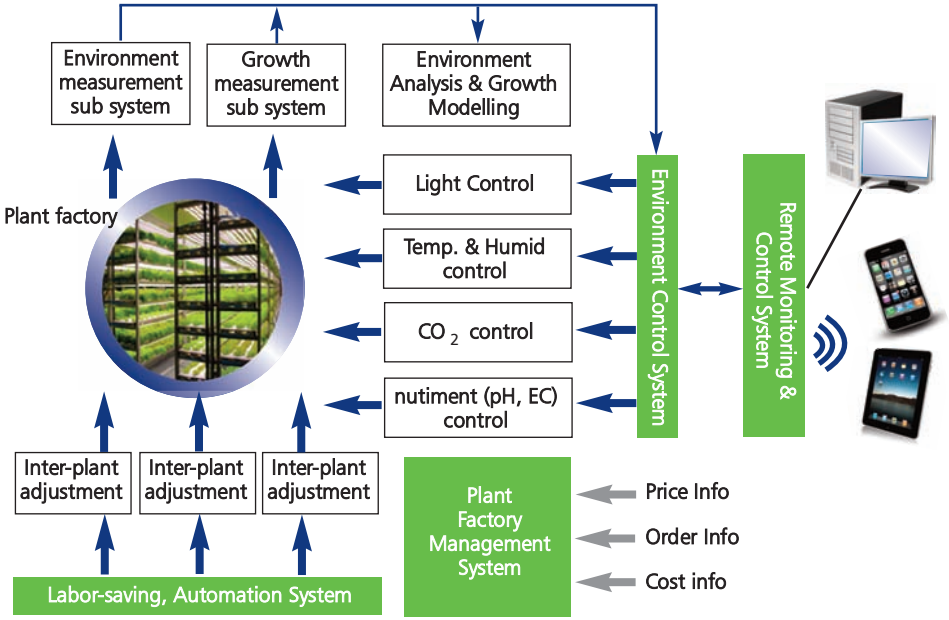


Figure 2 – the schematic diagram of the smart farm operated by management

Byeong-Sook BAE (bs.bae@kt.com, kt)

SKT M2M Activity in Korea

By Sangho CHOI

History

As the most innovative mobile service provider in Korea, SK Telecom is creating the future of mobile and delivering cutting-edge, converged wireless technologies for the global market. The company is a pioneer in the mobile industry, having been the first to launch and commercialize CDMA among other mobile services, and is now leading the way in 4G and beyond. In Korea, SK Telecom is the leading wireless communications operator, serving more than 26 million subscribers, which is over 50% of the local mobile market.

Focus Market and status

SKT started M2M Service on the CDMA network in 2006. Currently, SKT is positioning itself as a total M2M service provider. The business scope includes consulting, project management, network/platform provider and collaborative ecosystem enabler. The main categories of SKT's M2M business are utility, vehicle/fleet, and asset management, LBS/healthcare, environmental monitoring, finance service and so on. In 2011, the total number of M2M terminals being served by SKT network were more than 650,000. Among these, the leading application is the payment service which has about 200,000 subscriber lines. The second is a tracking service, with about 170,000 lines. The total revenue of M2M service in 2011 is 83 billion KRW. It is expected that the revenue will grow to 520 billion KRW by 2015, with more than four million M2M terminals on site.

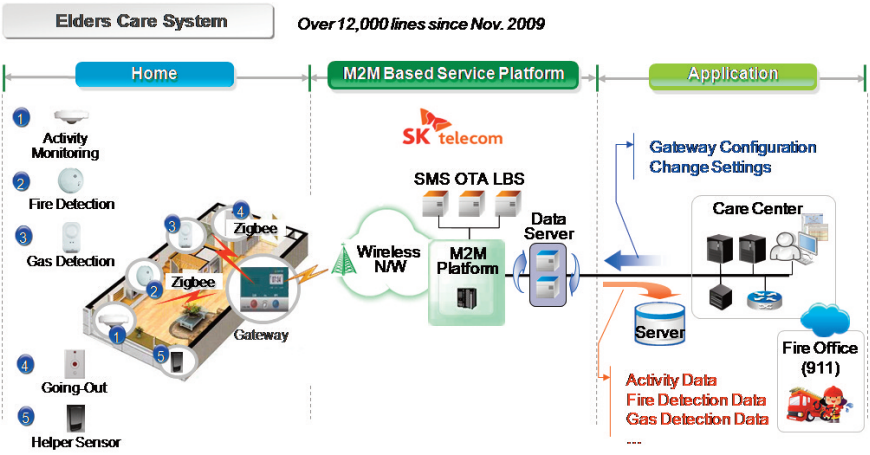
M2M Biz Category	Utility Mgmt	Vehicle/Fleet Mgmt	Assest Mgmt	LBS/ Healthcare	Environment SoC	Finance
	Electricity, Gas, Water, Enerygy, AMR	Bus, Taxi, Enterprise Vehicles	Equipment, Machine, Building, Store Security	Healthcare, Safety, Welfare	Traffic Mgmt., Fire Protection, Smart Grid	Mobile Payment, ATM

M2M Platform

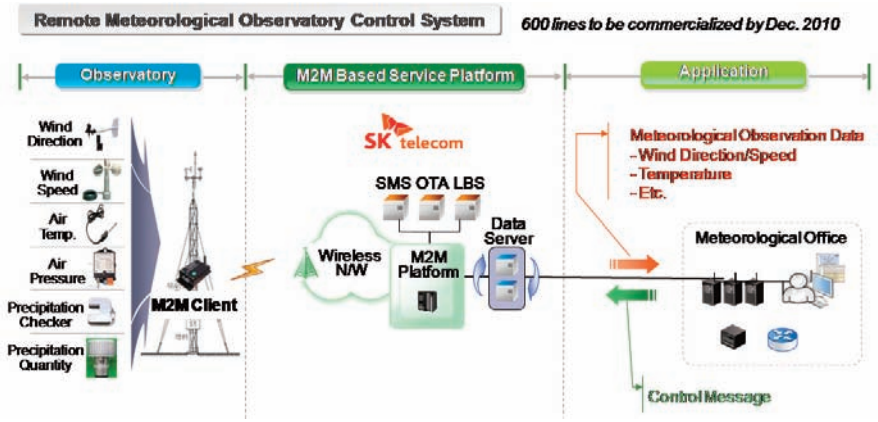
In 2009, SKT launched the first M2M Platform for a managed M2M service. It provides many functions which are not available without the platform, such as QoS control, reliable triggering, location and data store/forward. The applications carried on the M2M Platform are meteorological observations, senior citizen care services, location tracking services and so forth. But, only a few of the M2M services are being served with the support of M2M platform.

Recently, SKT has implemented a new Open M2M Platform based on ETSI M2M Specification Release 1. Using this platform, any M2M service developer can easily attach their application server to the SKT M2M Platform through ETSI mIa interface. The M2M Server Platform is connected to SKT's infrastructure which makes remote upgrade and device management easier. The purpose of the open M2M platform is to boost the M2M ecosystem in Korea by collaborating with device manufacturers, application developers and service providers.

SKT also implemented an M2M WEB portal, on which M2M Service Providers can monitor and control M2M terminals. Developers can test and validate their application on this WEB portal, checking whether APIs are interworking well. By utilizing SKT's M2M platform, it is expected to save development costs by 30%. The new platform is planned to open in mid- 2012.



One of the typical M2M services is an elder-care service. A Zigbee gateway collects data (i.e. activity, fire and gas detection) from sensors and automatic reports are sent to welfare offices for regular checkups and to assist senior citizens on-time. The M2M platform plays the role for delivering collected data to the care center with high security and reliability.



In the remote meteorological observatory service, sensors measure meteorological data such as wind speed, temperature etc. Those collected data are sent to remote meteorological centers through the M2M platform and used in weather forecasts

M-pid Project for Open M2M Platform

By Yong-Jin KIM

M2M (Machine-to-machine) communications and IoT(Internet of Things) are creating a new blue ocean in the ICT market and quickly penetrating into our daily lives. M2M/IoT is essential for the convergence of ICT and other vertical markets. In order to boost the M2M market and promote M2M service applications, a standardized M2M service platform is urgently required. It is the most important technical issue for the establishment of a sound M2M eco-system and is mandatory for an easy, fast and cost-effective development of several M2M applications.

However, the development of one commonly used standardized M2M service platform is very challenging work because M2M/IoT has an enormous number of vertical markets and each vertical market has its own distinctive requirements.

In order to make it possible several SDOs have started standardization activities and ETSI is the first runner for the standardization of M2M service platforms. In accordance with this trend, Modacom has launched a two-year M2M platform development project named M-pid with 600 million US dollar investment. M-pid is a portmanteau of M2M and Cupid and it means the lover of M2M!

The main purpose of the project is to develop a standardized middleware platform especially for M2M terminal devices in order to provide application developers with a Software Development Kit (SDK) having open APIs for fast and cost-effective development of M2M applications. The other purpose of the project is to provide M2M device developers with a Reference Design Kit(RDK) and M2M communication modules for easy trial and developments of M2M device hardware and communication functions. Furthermore, it includes the development of an M2M service platform for M2M servers and setup of M2M service test-bed so as to verify its outputs and to test a feasibility of new M2M services and applications. The design and development of the M2M platform has been done alongside international and local standardization activities.

Specification of the work scope

The main work scope of the project includes the followings:

- M2M Middleware platform for M2M devices, as a form of SDK
- RDK for M2M device hardware development
- Standardized M2M communication module especially for WiMax and LTE
- Advanced M2M technologies especially for low power consumption, QoS, and M2M gateway
- M2M server platform
- Test-bed for trial of new M2M services and applications
- Finding New M2M service models

Participating organizations

In order to fulfill the project successfully, four organizations which have appropriate technologies and rich experiences for M2M device, server, gateway, and standardization are actively involved. Modacom, as the leading company of the project has been in charge of M2M device technologies including SDK, RDK, and communication modules for M2M device developers. It also established the M2M test-bed. KT, as the biggest network and IT service provider in Korea has been involved for the development of the M2M service platform. PicosNet and Ajou University have joined for the M2M gateway and standardization. In addition, Korea's major mobile network/service providers such as SKT and LG U+ have joined an advisory committee to review of the direction and design of the project. The specification of the work and the role of each participating organizations for the project is shown in Figure 1.

Outputs of the project

As outputs of the project, an SDK which includes an M2M middleware platform and an RDK, 4G mobile communication modules, M2M gateway and M2M service platforms were produced. Also, an M2M service test-bed to verify the project results and to test the feasibility of new services and applications is another ouput. The development of new M2M services and applications and their trials for e-Health, automotive, and video surveillance are other results of the project.

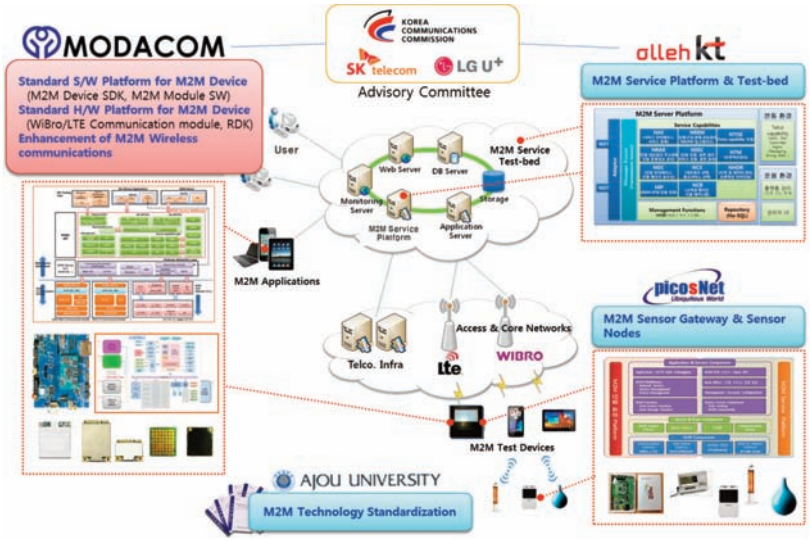


Figure 1 Project work scope and the role of participating organizations

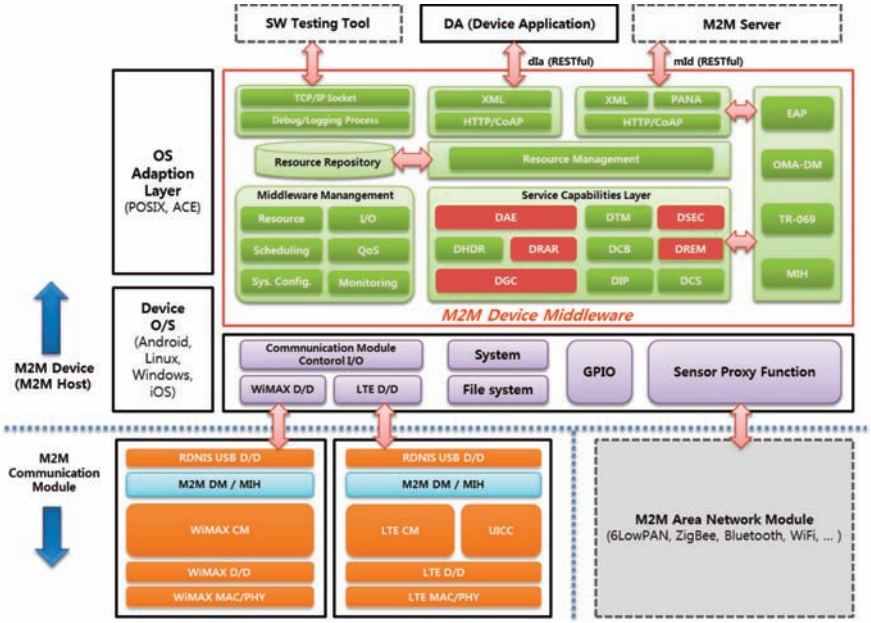


Figure 2. Architecture view of M2M Device platform

SDK for M2M Device Middleware

M2M middleware for device was developed based on ETSI M2M standards, in which M2M service capabilities were modularized. It can be executed in the form of mobile phone's application. It is communication technology-agnostic and it is operational on several types of the operating system including Android, Linux, Windows, and iOS. Figure 2 shows the overall view of functional architecture of the M2M Device middleware. The SDK also includes debugging tools, documents and examples of applications.

Communication modules for M2M Device

M2M communication modules developed in this project support 4G mobile communications including WiMAX and LTE. The form factors are connected B2B(Board-to-board) type and PCI express mini card type. Local standardization has been done in parallel and the standardization scope includes mechanical, electrical specifications of the modules. WiMAX module supports WiMAX-16e and WiMAX-16m and LTE module support TDD-LTE, FDD-LTE functionalities.

Mini PCI Express Card type (Full/Half)

B2B type (Front/Back)

<LTE M2M modules>

Mini PCI Express Card type (Full/Half)

B2B type (Front/Back)

<WiMAX M2M modules>

RDK for M2M Device

RDK for M2M devices supports test environments in which the M2M device vendor can develop the M2M device hardware, communication module, service middleware and applications, It also provides wireless communication interfaces such as 6LoWPAN, ZigBee, Bluetooth, WiFi in order to be connected to M2M area networks in which various sensor nodes or terminal devices exist. Figure 3 shows an image of RDK and its functional block diagram.

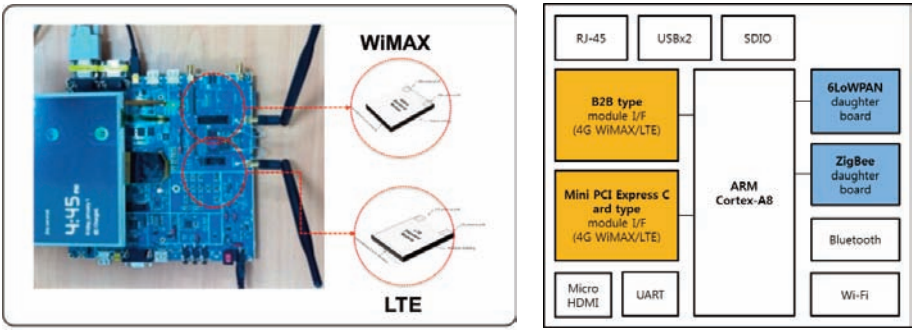


Figure 3. RDK for M2M Device and its functional block diagram

Standardization efforts for M2M platform

Modacom has been actively involved in International and local standardizations bodies. International standardization activities are mainly concentrating on ETSI TC-M2M for M2M middleware platform specification and ETSI ISG-SMT for M2M module standardization. It also has been participating in oneM2M activities from its initiation. In particular Modacom leads sensor network standardization in JTC 1 as the convener for JTC 1/WG 7(Working Group for sensor networks) and M2M domestic standardizations activities through participation in TTA and theM2M Forum in Korea.

Applications of Outputs and Future plan

The outcomes of this project such as SDK, RDK for M2M devices and M2M service test-bed are expected to be released to all M2M eco-system players including M2M service/network providers, M2M application developers, M2M platform vendors and M2M device vendors so that they make use of these outcomes to make their works easier. In order to verify the interoperability of the M2M platform globally and to demonstrate the M2M service models developed during the project, Modacom has a plan to participate in ETSI Plug Test for M2M on October 2012. Modacom has also provided the outputs to the M2M Support Center(MSC) in Korea, where many domestic M2M industrial bodies use the outputs for testing their products.

Modacom has already demonstrated the M2M service model named as "DIY-M2M, or Do-It-Yourself M2M" with KT in the Mobile World Congress(MWC) 2012 held in Barcelona and it also plans to participate in MWC 2013 with an updated model next year. Modacom plans to continuously update its outcomes and support M2M-related vendors for customizing their products and solutions



IoT – Going horizontal to win in verticals!

By Harish Viswanathan, Mary Lenney, Gunter Woysch
Alcatel-Lucent

The Internet of Things is a promising long term future market that service providers can exploit. By deploying horizontal platforms that support vertical market solutions to be created by third-party application providers and their own teams or even by the service providers themselves. Service providers can define and possibly enlarge their prospective position in the IoT value chain.

Although a fundamentally different approach is needed, service providers are in the best position to take advantage of the future Internet of Things opportunity by leveraging their network assets and expertise.

Introduction

The vision of the Internet of Things is currently being developed into a broad set of interrelated research projects by the European Commission.

The Internet of Things has to be founded on a well defined architecture with precise interfaces between all its levels in order to guarantee interoperability between devices, services and applications to be used by world-wide distributed operators.

The Internet of Things will partly make use of the existing infrastructure already developed for M2M communications and for globally standardized communication networks. We will discuss several aspects of the future of the Internet of Things from a telecommunication company's point of view.

The ever-expanding "Internet of Things"

With the number of connected devices to grow to many billions in the near future, service providers are intending to take an active role in the Internet of Things as in machine-to-machine (M2M) communications.

The Internet of Things and M2M communications refer to the idea that things – especially everyday objects – are readable, recognizable, locatable, addressable and controllable through the Internet. The Internet of Things is expected to add autonomous objects and cooperating systems of autonomous objects for new kinds of intelligent services to the current offers.

The growth of Internet of Things communications will be pushed by

- Near-universal wireless network availability
- Reduced communication costs
- IP networks that simplify solution development
- Industry regulations that demand automated remote monitoring.

In the future this market will extend to applications connecting the interactions of (intelligent) devices with social networking and crowd intelligence approaches, while addressing concerns such as privacy, security and even ethical constraints.

Capitalizing on billions of connections

In the past service providers were limited to selling wholesale bandwidth to value-added resellers and mobile virtual network operators (MVNOs).

Now, with the forecasted growth in connected devices and the revenue potential associated with that growth, service providers are looking to capitalize even on the future Internet of Things traffic.

Service providers are

- Investing into new business groups, centres of excellence, joint ventures and developer programs,
- Expanding existing business-to-business (B2B) service groups,
- Creating in-house service platforms now at least for M2M and most probably later for Internet of Things communications too.

Service providers have a role to play in device communications. They can increase their relevance by using their expertise in device management, billing, provisioning, data storage, security and other related services. Providing additional services will allow them to attract more enterprise customers with long-term M2M and later IoT contracts and will help them to enhance their revenue opportunities through increased loyalty.

Service providers may offer applications and services directly to end users, but most often they will deliver them indirectly through third-party or enterprise application providers. These are being challenged to establish themselves in these expanding markets.

Service provider challenges

A complex and fragmented value chain

The Internet of Things value chain is expected to be complex and fragmented into various niche applications, devices, modules, vertical markets and services. It will include product, system and content providers and solution integrators. Because no single company can provide all components of a complete solution, it is not clear who will play what role. Partnership can help.

Network requirements

Network challenges result from increasing network traffic, caused by an extremely high number of short messages with high signalling overhead:

Availability: Connectivity will be required in locations not yet considered in current networks.

Reliability: If networks are critical parts of the business, they must be as reliable as any other critical equipment.

Scaleability: Service providers must manage the significant additional traffic load of the Internet of Things and ensure that each application's (voice, video, data, IoT) communication requirements and service level agreements are met.

Flexibility: With the varied needs of different applications, enterprises will demand flexible pricing schemes that match their network utilization needs.

Security: Lack of security could derail Internet of Things applications. Devices provide access to a network with applicationsand data; all of them including the communication have to be secured.

Response time: Service providers need the ability to define flexible priorities for services with different response times, ranging from real-time responses to uncritical long delays.

Business model dilemmas

Finding the right business model is important, as the opening Internet of Things market will be comprised of multiple vertical markets, such as smart cities, buildings, transport, energy, living and smart health.

Service providers must understand how to address different markets, their unique ecosystems and specific requirements.

For example:

- Should they create separate organizations and network infrastructures for each vertical market?
- Can they create meaningful horizontal platforms satisfying multiple vertical markets?
- To what extent should they try to provide specific vertical market services themselves versus relying on third-party providers?

Given the expected market complexity and service providers' unique needs, there is no simple answer of one-solution-fits-all approach to these dilemmas.

IoT application provider challenges

Internet of Things application providers also face some hurdles before deploying such services:

Device and application certification are required before deployment to ensure that networks are not disrupted by these deployments. Device distribution, installation, provisioning and activation are all logistical challenges.

Device management technology must be used to remotely and automatically configure, diagnose, deactivate and upgrade firmware in field programmable devices.

Communication management The application software must be able to securely communicate and scale to support a large number of devices.

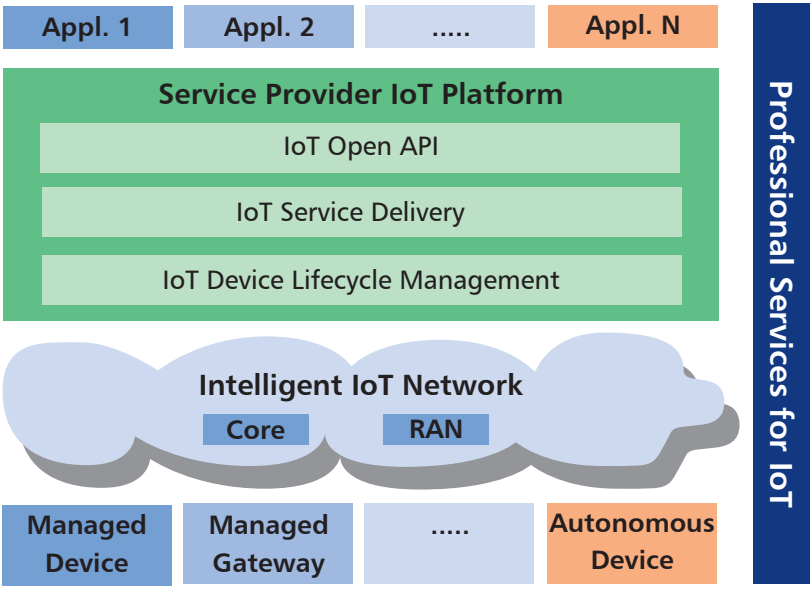
Billing and customer care Internet of Things application providers must deploy billing and customer care solutions for their customers.

Addressing IoT market challenges

Service providers will be able to leverage their infrastructure assets for Internet of Things solutions in three key areas:

- Network
- Application enablement
- Customer experience.

Addressing the broad scope of different solution requirements from this horizontal perspective allows flexible targeted solution development.



Vertical Market Solutions

(Smart Cities, Buildings, Transport, Energy, Living, Health)

Application-specific quality of service (QoS)

Future intelligent networks will provide basic transport for all applications and ensures delivery with the appropriate QoS. Network elements within these future networks can also prioritize packet forwarding to ensure QoS for certain flows.

High reliability

Deploying geo-redundant data centers and cloud infrastructures will help service providers to guarantee high reliability. Network monitoring tools will measure key network performance indicators to prevent or correct network malfunctions in order to meet Service Level Agreements. Distributed overload protection mechanisms can prevent flawed applications from abusing the network.

Simplified development and operations

Service providers can selectively and securely expose a number of enablers through easy-to-use application programming interfaces (API) to the developer communities, both in large enterprises and in small application providers.

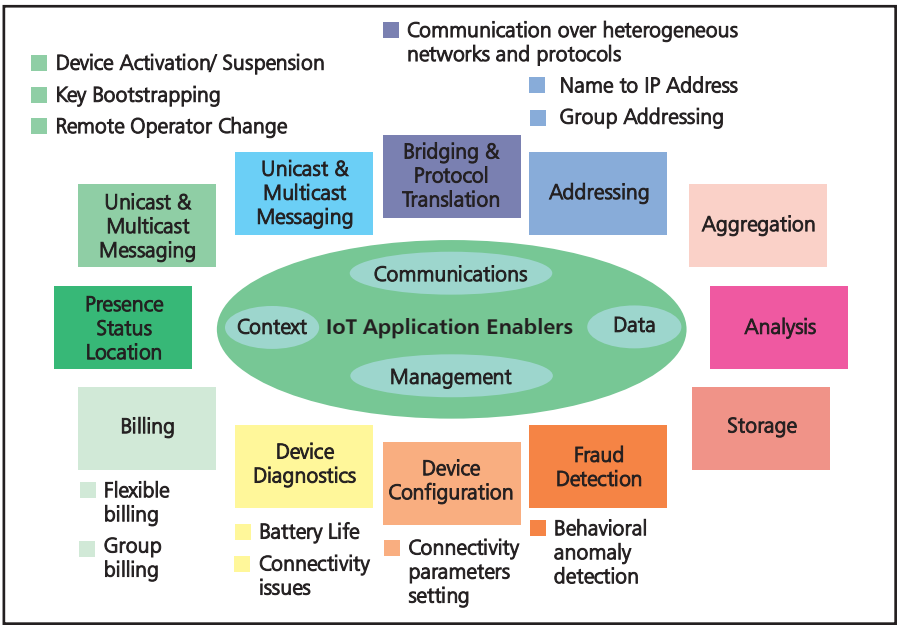


Fig. 2: Service providers can offer Internet of Things enablers

Providing these functionalities will create the service delivery and application enablement platform. Network protection will be covered by enforcing policies for network usage.

Device management

Service providers can also offer device management services for the enterprise devices deployed in their networks via appropriate application program interfaces.

Network diagnostic tools will give customers visibility into the operational behaviour of their devices.

Summary

The future Internet of Things will develop into a huge opportunity for infrastructure and service providers and for application developers.

Its size and complexity will pose significant challenges on all system levels to academia and industry.

Smart and autonomous systems will lead to new and sometimes disruptive user experiences in an intelligently connected world.

Appropriate business models will be needed for complex and fragmented value chains, taking care of Internet of Things market challenges.

Harish Viswanathan,
Alcatel-Lucent, Bell Labs Chief Technology Office, Murray Hill, NJ, USA

Mary Lenney,
Alcatel-Lucent USA, Corporate Marketing, Murray Hill, NJ, USA

Gunter Woysch,
Alcatel-Lucent Deutschland AG, Bell Labs Germany, Stuttgart, Germany

IoT applications of strategic interest

Presser, M. (AI), Krco, S. (EYU)

Initial report from IOT-I (The Internet of Things Initiative)

Introduction

The range and diversity of IoT applications is huge, permeating through practically all aspects of every day life. This report presents the results of the IoT-i's initial efforts to systematically organise IoT scenarios designed, proposed and analyzed by several research projects (FP6 and FP7) and then to collect feedback from a variety of communities about the scenarios.

In particular, we were interested to find out which scenarios people considered the most important from the societal and business aspect as well as how mature the scenarios were (from the market and technology points of view).

The scenarios were collected from eight FP6 and FP7 projects by directly contacting representatives of the projects and using contact networks of the IoT-i partners. These scenarios were then analyzed, grouped and aggregated to make the analysis and evaluation more efficient.

IoT Survey Introduction

The aim of the survey was to analyse a large set of application scenarios addressing different application sectors that use IoT technology at their core. Application scenarios were defined as a user centric story illustrating the technology itself, software or user interface using IoT technology or a user action that is impacted by IoT technology.

The analysis then focussed on discerning the impact of the application scenario on society and its business value. In total 150 application scenarios were collected from the following projects:

- ICT SmartSantander
- ICT SENSEI
- IST e-SENSE

- ICT EXALTED
- ICT FLORENCE
- ICT PROSENSE
- ICT LOLA
- IST MIMOSA

All 150 scenarios were analysed in terms of categories and similarities. A total of 14 categories were agreed upon, containing from two to eight application scenarios each:

- Transport (7 application scenarios)
- Smart Home (3)
- Smart City (5)
- Smart Factory (3)
- Supply Chain (3)
- Emergency (5)
- Health Care (7)
- Lifestyle (6)
- Retail (3)
- Agriculture (2)
- Culture and Tourism (4)
- User Interaction (3)
- Environment (4)
- Energy (2)

The analysis resulted in 57 application scenarios from the original total of 150.

Applications of Strategic Interest

In this chapter we feature the top five scenarios for Business and Societal Impact. It is interesting to note that there are three scenarios that are common to both lists, two from Health Care and one from Emergency.

We also provide a snapshot of those scenarios that are perceived to be most mature from a market and a technology perspective. In general, the survey responses indicate an optimistic view of the maturity of many IoT- based services and technologies with several expected to appear in a 2-3 year timescale.

The perceived maturity of the Top 5 Business and Societal Impact indicates that all of these scenarios are expected to be realisable within 4-5 years.

Top 5 Business Impact

1. Continuous Care (Health Care)
2. Remote Factory Management (Smart Factory)
3. Smart Product Management (Retail)
4. Smart Events (Emergency)
5. Aging population – Alzheimer's disease (Health Care)

Top 5 Societal Impact

1. Smart Events (Emergency)
2. Continuous Care (Health Care)
3. Aging population – Alzheimer's disease (Health Care)
4. Mine Sensor Chat (Smart Factory)
5. Sustainable Urban Planning (Environment)

Top 5 Market maturity (shortest time to market)

1. Product Interaction (User Interactions)
2. Mine Sensor Chat (Smart Factory)
3. Smart Tags (User Interactions)
4. Mobile Fitness Application (Life Style)
5. Remote Factory Management (Smart Factory)

Top 5 Technology maturity (nearest achievable development)

1. Smart Tags (User Interactions)
2. Product Interaction (User Interactions)
3. Smart Pallet Loading (Supply Chain)
4. Cultural Information (Smart City)
5. Mine Sensor Chat (Smart Factory)

You can find details of all 57 application scenarios at:
www.iot-i.eu/public

Top Application Scenarios: Business Impact

Continuous Care: Health Care

In continuous care the concept enables patients with chronic diseases or elderly people with health impairments to stay in their own home despite their health constraint, to reduce cumbersome visits to the doctor and to avoid premature relocation to a nursing home. David's mother Charlotte comes to visit the family and complains about her many consultations at the doctor's surgery just for routine checkups for her low blood pressure and impairments due to age. She feels that she is spending a great amount of time waiting at the doctors and loses her freedom. She knows that she is getting older and her state of health is worsening, but she wants to keep her independence and freedom as long as possible. David shows her the application that he is currently using for the recovery from his heart attack and tells her that he is feeling very comfortable with it. Back in her home-town Charlotte asks her doctor about a similar application and he/she agrees that such a system will be suitable for Charlotte, too. A special device for her home will help her to monitor her blood-pressure, blood-sugar, etc and also in case she falls will transmit an alert. She feels relieved and can now spend more time with her friends doing activities she enjoys.

- Business Impact rank 1
- Societal impact rank 2
- Market Maturity 2-3 years
- Technology Maturity 1-2 years
- Adapted from FP6 e-SENSE and FP6 MIMOSA

Remote Factory Management: Smart Factory

Wireless communication networks are a cost efficient way for remotely controlling industrial facilities and infrastructures: Pressure sensors are located along gas/oil pipelines. Abrupt change of pressure provokes automatic closing of lines. Sensors are placed on each section, depending on the architecture and risk assessment.

- Business Impact rank 2
- Societal impact rank 30
- Market Maturity 2-3 years
- Technology Maturity 1-2 years
- Adapted from LOLA

Smart Product Management: Retail

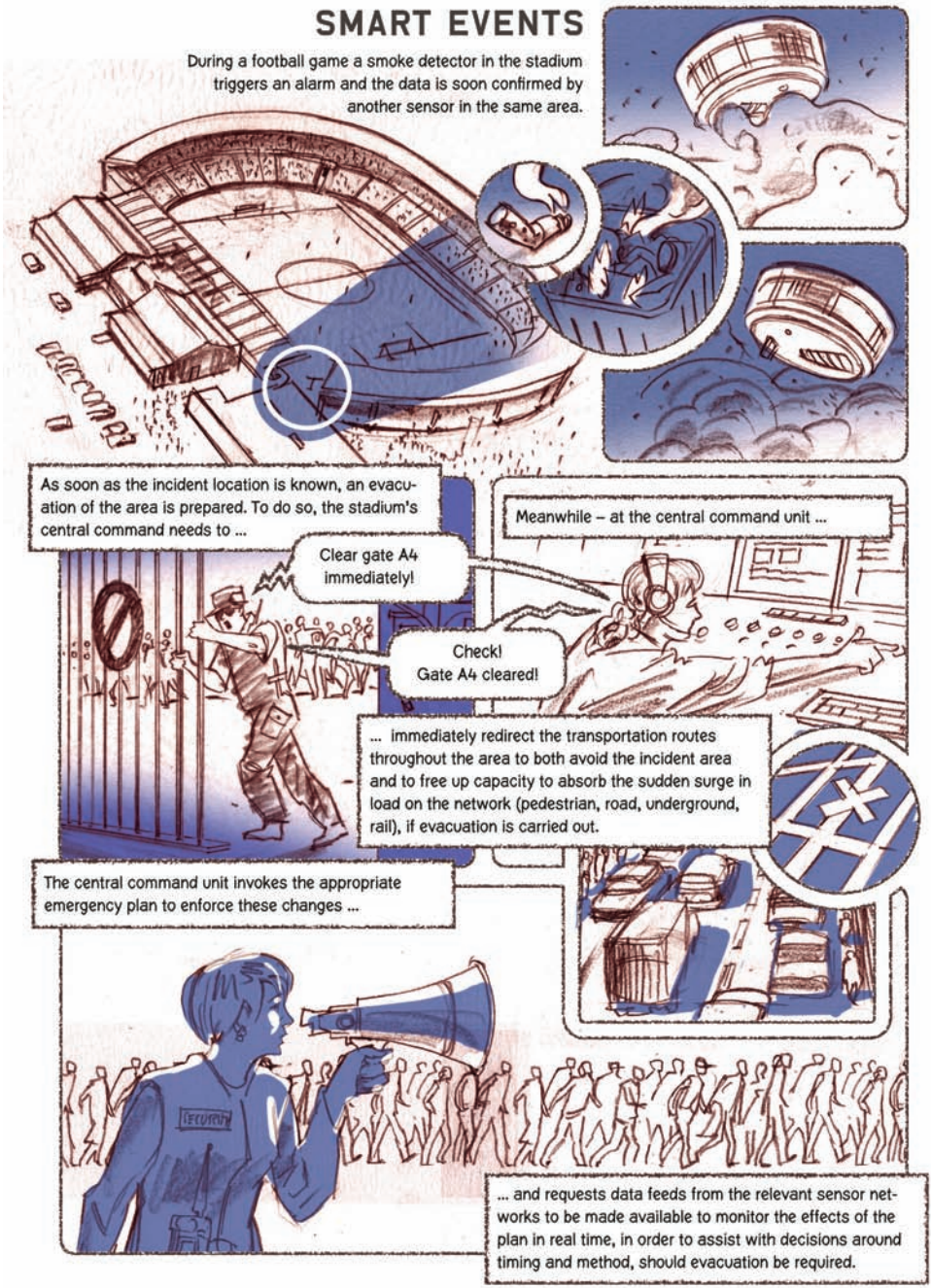
Tom is working in a supermarket. He is in charge of the management of a beverages department. Thanks to RFID and sensors he is able to monitor information about the products: type\variety, state, condition of the storage, expire date, quantity\stock in the line, the changes in the products' location, time of moves, location, position... and the consumers: profile, time spent in the area or in front of a product, products they are interested in, etc. He infers: the flow of the goods in the section, the efficiency of his marketing strategy in the department, and he learns about the behaviour\satisfaction of the consumers according to the supply. In real time, he observes the way the products impact the consumers' behaviour.

- Business Impact rank 3
- Societal impact rank 41
- Market Maturity 4-5 years
- Technology Maturity 2-3 years
- Adapted from FP6 e-SENSE

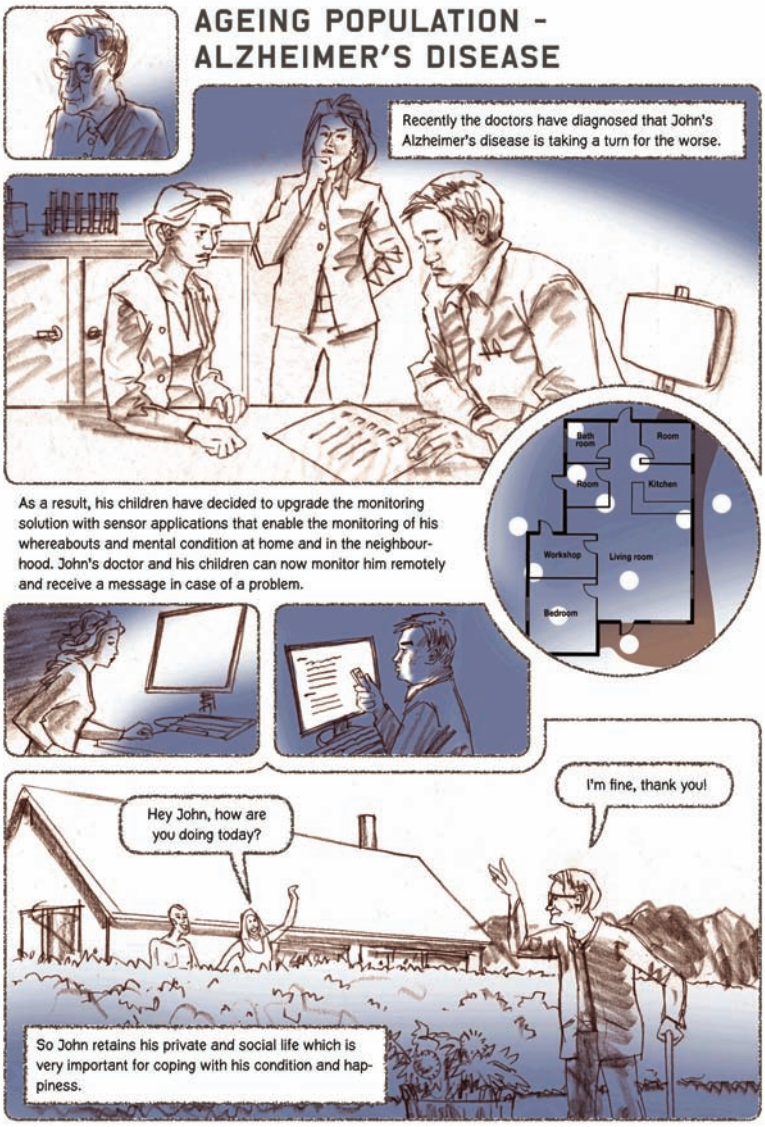
Smart Events: Emergency

During the Olympic Games, a smoke sensor within the stadium is triggered, and the data is soon confirmed by another sensor in the same area. As soon as the incident location is known, an evacuation of the area is prepared. To do so, the games' central command needs to immediately modify the transportation routes throughout the area to both avoid the incident area and to free up capacity to absorb the sudden surge in load on the network (pedestrian, road, underground, rail), if the evacuation is carried out. The central command centre invokes the appropriate emergency plan to enforce these changes (evacuation of major venues are pre-planned), and requests data feeds from the relevant sensor networks to be made available to monitor the effects of the plan in real time, in order to assist with decisions around timing and method, should evacuation be required.

- Business Impact rank 4
- Societal impact rank 1
- Market Maturity 2-3 years
- Technology Maturity 2-3 years
- Adapted from FP7 SENSEI



Illustrations by Mikael



Illustrations by Mikael

- Business Impact rank 5
- Societal impact rank 3
- Market Maturity 4 years
- Technology Maturity 2-3 years
- Adapted from FP7 SENSEI

Top Application Scenarios: Societal Impact

The top 3 scenarios for Societal Impact: Smart Events (Emergency), Continuous Care (Health Care) and Aging population – Alzheimer's disease (Health Care)) is described opposite.

Mine Sensor Chat: Smart Factory

Mine Sensor Chat (MSC), is a simple application but with a lot of benefits for miners' health and safety. The system prevents dangerous accidents in the mine areas and provides more security for the miners in their working environment. Sensor nodes detect dangerous substances in the mines (CO as the most hazardous), in order to secure miners' activity. Miners carry sensor nodes as additional part of their equipment.

- Business Impact rank 23
- Societal impact rank 4
- Market Maturity 1-2 years
- Technology Maturity 1-2 years
- Adapted from FP7 PROSENSE

Sustainable Urban Planning: Environment

Sensors are placed all over the city. A city official from the urban planning department is able to log on to the system and see historical data regarding different substances in the air and meteorological parameters, including noise levels, in all areas of the city. This information helps the city planner to make decisions such as where to plan new residential areas, more green areas (parks), industrial zones, etc. If the city planner notices elevated level of harmful substances in certain districts, a notification can be sent to the city's Inspection Department to check the source of the pollution.

- Business Impact rank 25
- Societal impact rank 5
- Market Maturity 5 years
- Technology Maturity 2-3 years
- Source Adapted from FP7 SmartSantander

Illustrations

To progress the scenario communication, a set of illustrations has been developed. We are grateful to Mikael for permission to reproduce some of his illustrations.

Illustrations by Mikael


Japan-Europe Cooperation on ucode technologies

By Ken Sakamura and Gérald Santucci

Cooperation in science and technology between Japan and Europe has developed steadily in the wake of the Science and Technology Cooperation Agreement between the Government of Japan and the European Union, signed on 30 November 2009. Two coordinated calls have already been organised, respectively on superconductivity materials and photovoltaics, and a new one is expected to be launched in the field of ICT.

We believe that the Internet of Things (IoT) will rapidly emerge as a powerful candidate for Japan-Europe cooperation in ICT.

More than one year has elapsed since the world witnessed the dreadful devastation caused by the Big Earthquake and Tsunami on 11 March 2011, the largest natural disaster to strike Japan in over 1,000 years. All Europeans felt compassion and solidarity towards the Japanese people during these challenging months, and many were moved by the courage shown by the Japanese people during and after the earthquake. The Earthquake and Tsunami have not changed the Japanese vision of the future Ubiquitous Computing and Internet of Things applications. In the coming months experts will increasingly come to the view that these applications are needed more today than ever before.

After visiting the annual TRONSHOW in Tokyo on a number of occasions, one of the authors, Gérald Santucci from EC's Directorate-General Information Society and Media, saw that this was a place where visitors could get a glimpse of Ubiquitous Computing environments in which computers are embedded in various objects and locations, and networked; a place where Ubiquitous Computing and Internet of Things are explained from the different yet complimentary perspectives of technology solutions, application development, standardisation, and international deployment.

At TRONSHOW2011, he proposed to work out a detailed and applicable cooperation strategy, involving a partnership between the Yokosuka Research Park's Ubiquitous Networking Laboratory (YRP UNL) and the European IoT community.

One year later, on 14th December 2011, during the TRONSHOW 2012, YRP UNL and a non-profit European multi-stakeholder interest group named 'the European Internet of Things Alliance' (EIoTA) signed a Memorandum of Understanding establishing close cooperation in the field of Ubiquitous Computing and the Internet of Things. TRONSHOW2012 was, in this respect, a defining moment for Japan and for Europe - a point in time when decisions moved from concepts to reality.

Prof. Sakamura (left) greets European partners to the MOU signing ceremony in Tokyo

EC's Directorate-General Information Society and Media foresees that in the coming months, further European organisations, in particular from industry, will join this IoT Alliance, thus extending the opportunities for sharing ideas and talents and for working cooperatively in research, innovation and take-up projects.

To get there, several meetings have taken place between members of the fledgling EIoTA, Professor Ken Sakamura (professor at the University of Tokyo and director of UNL), and UNL. These followed the first 'IoT Week' in Barcelona, Spain, in June 2011, in Lille (at the 'International RFID Congress'), in Barcelona (at the EPoSS Annual Forum), in Helsinki (at the ARTEMIS and ITEA2 Co-summit) in October, and finally in London (with CASAGRAS2 leaders in November).

The European IoT Alliance aims "to initiate, support and organise activities that promote the beneficial use and further development of ucode, T-Engine and similar IoT-related technologies within the European Union and abroad".

Let us elaborate on the two key words, "ucode" and "T-Engine".

ucode

ucode is part of the uID architecture that sits behind many advanced IoT applications developed and deployed in Japan today. ucode is the name given to a code system developed and promoted by the uID center, an NPO (non-profit organization), headquartered in Tokyo and chaired by one of the authors (Ken Sakamura). The uID center manages the allocation of ucode to application builders and users. **URL: http://www.uidcenter.org/**

ucode is used during the process of acquisition of context-awareness, i.e., the information about the surrounding environment. Basic information of context-awareness includes what objects are around the computer systems, or where the computer systems are located in the first place. ucode can be assigned to objects and places to help the computer systems to attain context-awareness efficiently.

The features of ucode and uID architecture can be summarized as follows.

- ucode is a 128 bits number;
- It is a unique identifier that can be associated with objects (real, virtual) and places;
- Its unique assignment is managed by the uID center,
- Tag-agnostic: ucode can be stored in any data carrier device for which a publicized specification for its R/W (reader/writer) interface exist (uID center lists so called certified ucode tags so that users can choose from them if they are not sure.);
- It is not semantic code, i.e., no special field for classification such as company code is pre-defined;
- All the relevant information associated with an object or a place to which a code is assigned is stored in so called information servers;
- The process to retrieve the associated information from the ucode is called "resolution process"

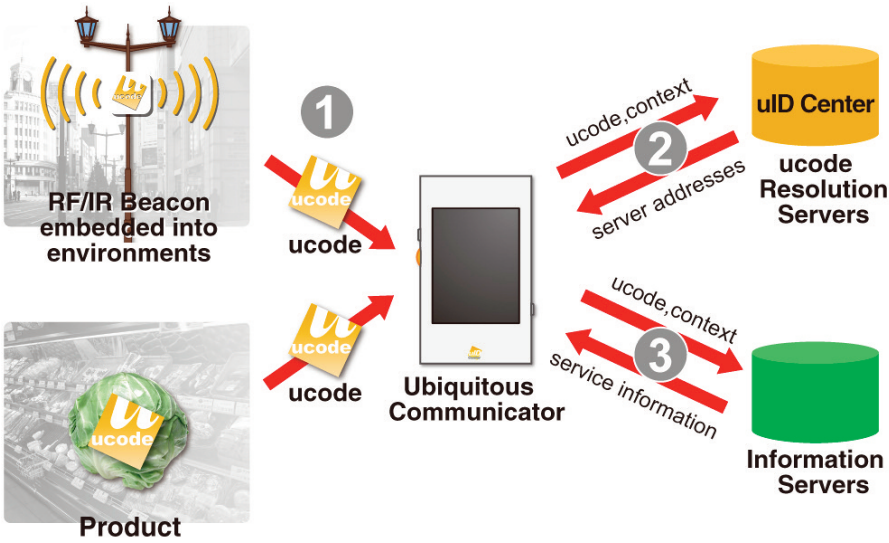


Figure 1: uID Architecture

ucode is read from a tag and data associated with an object or a place can be retrieved from an information server after "resolution" process.

Unlike many other code systems proposed in the last 10 years or so, ucode is not tied to a particular tag (i.e., data carrier device). Inexpensive QRcodes can be used as well as NFC tags, other RFID tags, optical codes, and there are even devices that can embed ucode in light beams, or sound emanating from a sound source.

Many prototypes of advanced IoT applications have been developed using uID architecture as its major component. Major categories are applications for objects and applications for places.

Applications for objects include:

- **Food traceability systems**
- **Drug traceability systems, and others**

Figure 2: An Example of a Food Traceability System

A shopper can easily learn who prepared the food package, when, and where

Food traceability attracted attention following the BSE scare back at the turn of the century. Ever since, the interest in food traceability has been strong all over the world. The release of radio-active material from the Fukushima nuclear power station in 2011 after the big earthquake has heightened the interest in food traceability to the next level in Japan.

Applications for places are so called location-based information services. Such services can be used for

- **Sight-seeing guidance;**
- **Promotion of local shopping streets;**
- **Helping the aged and the physically-challenged to walk around the town, and other purposes.**

These services are offered during normal times. However, during and after a disaster such as a big earthquake, the same infrastructure can be used to disseminate relief information such as where to find shelters, the operational status of transportation systems, etc.

ucode has been stored in QRcodes, NFC tags, infrared beam markers, radio beacon markers and placed along the street of Ginza, a famous shopping street in Tokyo. People can obtain sight-seeing guides there, and the physically-challenged can obtain route guidance to non-barrier toilets, etc.

Figure 3: Tags used in Ginza Street

NFC tags can offer tourist information during normal times, relief and information following a disaster. Active tags embedded in the street helps guide the visually-challenged.

YRP UNL has pioneered many such applications and is actively working with government, industry and academia to move ahead with new research and development activity on IoT applications and on fundamental technologies to make context-awareness possible.

T-Engine

Now back to the other keyword, "T-Engine". YRP UNL and many of its partners are members of T-Engine Forum (TEF - also the name of the hardware), another NPO under which uID center operates. T-Engine Forum is instrumental in bringing the R&D results of T-Kernel, a real-time OS kernel, and uID architecture to the masses by involving the commercial sector in the application development utilizing the technologies.

T-Kernel is an important software component operating in parallel to T-Engine and considered a key engineering element from Japan in EIoTA's initial objective. While T-Engine is the name of the hardware component of embedded systems which TEF has promoted, TEF has also been promoting T-Kernel, a small and efficient real-time operating system kernel that is suitable for building a smart node in a sensor network that plays an important role in the IoT.

T-Kernel runs on many types of CPUs as well as on the original T-Engine board. TEF has published the specification of T-Kernel (now version 2.0) and its source code for free from its web site: **www.t-engine.org**

Anyone can build an embedded computer system using T-Kernel without paying royalties. T-Kernel is an attractive platform to build an intelligent node in the IoT environment. From a Japan-Europe perspective, it has to be noted that the T-Engine/T-Kernel technology has been a subject of specific co-operation under projects of the ARTEMIS Joint Technology Initiative (JTI). For instance, the SOFIA project has developed an environment enabling information sharing across devices, platforms and applications on top of T-Kernel technology.

Open Architecture

For the future technological infrastructure, an open architecture with easily available specification is very important. An accessible sample implementation is also important. TEF provides T-Kernel for the future developers of IoT applications free of charge.

It is hoped that many European researchers and developers will take advantage of T-Kernel through the technology transfer via EIoTA.

Global and Future Applications of IoT

The applications of the IoT are still being developed in many new fields. For example the IoT can be used for eco-friendly environments, contributing to the slow-down of global warming.

TRON Smart House, an advanced example of the IoT application, is equipped with solar panels, solar cell walls, and a power station that helps the residents keep tabs on the usage of electricity by visualizing the usage. PAPI, a TRON Smart House, could obtain electricity from the hybrid car in case of power grid blackout.

Figure 4: TRON Smart House, PAPI

Built in 2004, this house uses many sensors, actuators and computers. During the total black out of the electric grid, it can obtain electricity from Toyota's hybrid car,

Today, the application of IoT goes beyond a single smart house to the larger target: urban landscape. A major Japanese focus is on the application of IoT on Smart Grid and Smart Metering. Such applications at society level will help us conserve energy at the town or wider level as well as at the house level in the long run. And such smart control of the power-grid involving the active participation of individual smart houses and small businesses may be a decisive "killer" application to avoid the total blackout of a large area after the supply of electricity is cut short due to a disaster like a big earthquake. Many districts in Tokyo and elsewhere suffered from such wide-area rolling or planned blackouts immediately after the big earthquake in 2011, and people's expectations for this type of application are high.

The usage of ICT in coping with disasters has gained much attraction after the big earthquake in 2011 in Japan. There had been research activities in this direction even before the earthquake, but the application needs are felt very strongly today. So the researchers are working with government offices to see how ICT can help the needs of regional government offices. Use of satellites for communication when the ground-based communication is cut, or using ID tags for recording the whereabouts of disaster victims, are two important applications.

Global Application Framework

Back to uID architecture. It should be stressed that the basic uID architecture is meant to be universal, so it can be used across national borders, not to speak of industry or organizational boundaries.

ucode has a built-in distribution allocation management. This means the allocation of ucode can be done locally at national level and at a lower -level efficiently. But once the objects flow across national borders, the information about these objects can be found using the resolution process from a remote server that may sit on the other side of the earth.

ucode allocation management is done in a distributed hierarchical manner to facilitate such distributed allocation.

> Finland's VTT has already installed and is running both the top level and second level uID servers. Top level servers are meant for countries, cities, etc. whereas second level servers (companies, organisations) handle (or resolve) directly the ucode queries.

All queries are eventually resolved by the server hierarchy. The current implementation is only for experimental purposes. Both servers, running on PCs, are accessible outside VTT and can be used for small pilots and experiments. VTT has the ability to grant ucode spaces and all the management capabilities for linking ucodes with information and services. The initial setup was assisted by a Japanese researcher who visited VTT for one month; such visits are expected to continue and gain more importance in the context of the UNL-EIoTA MoU. The objective of VTT is to integrate uID ecosystem with smart spaces and environments through their own semantic interoperability techniques.

Building on VTT's experience, EIoTA will seek to establish some research teams or lablets (certainly in Finland, but also in Italy, Germany, France, Spain, etc.) concentrating on the development, application and exploitation of IoT technologies, an EIoTA Communication Office, with the responsibility of relations to industry and business, public authorities, and Japanese partners, and a few Business Showcases to promote awareness of the possibilities of IoT applications in various domains. During 2012, EIoTA will finalise its business plan (research lab, show room, liaison office, new venture) and define the first locations in Europe. It will also clarify its organisation in terms of legal status, human resources, funding, responsibilities and rights, management structure, and contract issues.

For its part throughout the discussions between UNL and EIoTA, the European Commission stressed three points:

1 **Openness.** The European Internet of Things Alliance is not a sort of 'European tribe' willing to cooperate with the YRP Ubiquitous Networking Laboratory to fight against other organisations here and there. On the contrary, it is an initiative that aims at fostering dialogue and cooperation among all countries and organisations on the timing, conditions, and circumstances for the deployment of Ubiquitous Computing and Internet of Things.

Universities, research centres and companies in Europe are willing to improve or enhance the T-Engine Forum solutions in order to design and build innovative applications that are well adapted to local needs. This begins with an approach of openness, transparency, mutual respect, acceptance, trust, and accountability that welcomes potential partners from all countries as well as other technical solutions insofar as the same general objectives are shared.

2 **Interoperability.** The Ubiquitous ID Center, which operates within T-Engine Forum, has recently taken some initiatives to establish the ucode within the standardisation community on a more formal basis. In particular, the UID Center is seeking formal registration under ISO for a set of RFID data constructs and having the ucode as a unique item identifier in ISO. These initiatives deserve to be hailed as important developments to ensure interoperability among established systems, but yet the risk exists that the ucode fails to meet the fundamental requirements of the unique item identifier. In this context, Japan-Europe collaboration under the Memorandum of Understanding offers a glimmer of hope to resolve this situation in an efficient and effective way.

3 **Connectivity and scalability.** The evolution of Ubiquitous Computing and the Internet of Things can be a powerful vector for having a Future Internet that is worthy of society's trust. We must acknowledge the practical constraints such as the speed of light, or limitations on computation, memory, and bandwidth resources. We must also acknowledge the design requirements for goals like efficiency, security, privacy, reliability, performance, ease of management, and so on. Nevertheless, we should wonder whether it is possible to achieve scalability without relying on hierarchical addressing, route traffic directly on the name of a service rather than the address of an object, or have notions of identity that cannot be forged. The Memorandum of Understanding can promote collaborative research and experiments that provide helpful insight into these matters.

Conclusion

TRON Project, a computer architecture project for embedded systems led by one of the authors (Ken Sakamura) has been on-going since 1984. In it, the vision of Ubiquitous Computing, which is today's IoT in essence, was described from the start. Thanks to advances in microelectronics, RFID and other advanced ICT, ubiquitous computer networks today make the applications of IoT using ucode possible. But this is only a start. Feedback now needs to be collected to build more interesting applications in the future.

IoT applications that use ucode can be built for many application fields:

- **Tourism**
- **Commercial promotion**
- **Support for physically-challenged people**
- **Helping victims in times of natural disasters, etc.**

Applications have already been prototyped and put into use in several countries including Japan and Finland.

The approach taken by uID architecture is open to everybody so it can create synergy with other similar technologies and hence better address the growing global and societal challenges.

Cooperation between EIoTA and Japan's UNL is a model of global alliance that has the potential to bring ICT to every organisation and every individual for improved efficiency and better quality of life.

It is hoped we are demonstrating the right direction for the future adoption of IoT with this global alliance between EU and Japan, and with future partners from other regions.

Readers' participation will be welcome!


National Value Creation Networks

By Ovidiu Vermesan & Peter Friess

Pan European Cross Fertilisation and Integration of IoT Programmes and Initiatives Through National Value Creation Networks

In the area of the Internet of Things (IoT), Europe is addressing the competitiveness in the context of globalisation. The technological specialisations built up over decades are rapidly transforming. In the area of IoT the IERC (IoT European Research Cluster) is focusing on increasing the network of projects, companies, organizations, people and knowledge at the European level as a way of making projects more innovative and competitive. The strategic relationships in the European IoT cluster involve national and international linkages that support knowledge investments.

Innovation in the area of IoT is the successful exploitation of new ideas generated. It is considered the key factor for fostering the use of IoT technology in new applications resulting in economic growth and supporting industry competitiveness in the global market, by bringing new knowledge into business, developing new applications, high value-added products and services. IERC see open innovation as a mechanism to support the positioning of existing European research and development assets in the face of rapid IoT technological and market change. The cluster is actively involved in the process of knowledge creation, knowledge diffusion, and knowledge sharing.

Evolutions in the global environment and evolutions in national, science and technology and industrial/enterprise policy are converging on the objective of supporting these linkages at a national level. One of the vehicles proposed by the IoT Cluster in order to achieve a real pan European coordination and cooperation is to support a national cluster liaison in every

Figure 1 Internet of Things - Connectivity

European country with "national value creation networks/clusters, innovation/research incubators"- concentrations of projects and supporting actors financed by the national public authorities.

> The creation of national clusters enables the projects and the organisations involved to become more flexible to grasp business opportunities, to react quickly, and to engage in partnerships with complementary strengths and capabilities.

This process will be very important in regard to innovation considering that strong international competition and rapid technological development in the area of IoT will require companies to produce new products, new applications, new services, develop new processes and access new markets.

Cooperation is one of the first priorities for action in Europe to prepare for the new knowledge-based economy where IoT technology and applications will play a significant role. This is needed based on the nature of global competition and on an estimate of the types of jobs that will be demanded by the market in the future.

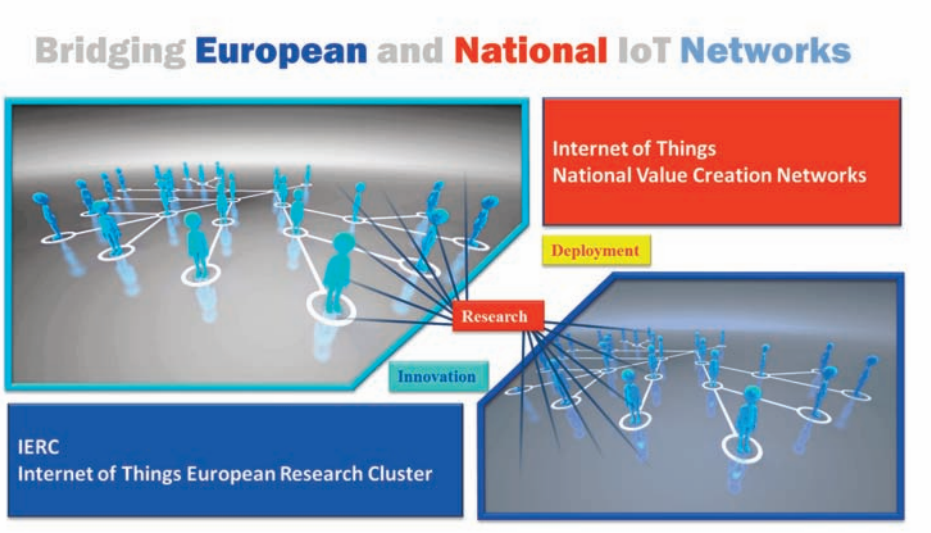


Figure 2 Bridging European and national research programmes on IoT

In the context of global competition the Member States in Europe are forced to organize the brainpower to capture the growth in the area of IoT by closer cooperation.

Participation in these new IoT networks enables the European projects and organisations to concentrate on core capabilities, and provide access to resources including specific know-how, technology, financial means, products, applications, services, markets etc., in other projects and organisations.

IERC strategy includes the provision of a policy framework for interactive learning between projects that involve industry, public bodies and research and education organisations. The development phases of the IERC are described in the table overleaf.

This new approach is visible across a number of different policy fields implemented by the IoT Cluster. One of them is the creation of common activity chains (ACs) to favour close cooperation between the IoT Cluster projects and to form an arena for exchange of ideas and open dialog on important research challenges.

IERC Development Process Stages	Goals	Needs	Implementation
Idea started with the need to cluster the activities related to IoT technology. The result is the establishment of this stakeholder community based on common technological interests, trust and confidence	Create the basis for cooperation, build a strong community, develop the common vision, strategic research agenda and sustain trust and confidence	Technological leadership, cooperation among projects, liaisons with global community, confidence building, willing to challenge the current situation, delegate the responsibility of common activities to individual projects and companies. Identify relational and communicational skills. Cluster building requires patience, commitment, resilience and in-depth knowledge of the projects.	Projects identity building, a cluster foundation and strategy.
Creating and formalising strategic linkages with other programs and organisations at the European and global level.	Build institutional bridges, institutionalise collective routines	Excellent regional knowledge and vision. Integrity, managerial and analytical skills. Brokerage, mediation, conflict resolution and communication skills.	Setting up activity chains, and national value creation networks. Obtain a clear understanding of the European and global IoT activities and the stakeholders involved by involving the projects in common activities mapping national and international activities and knowledge sharing.
Vision, strategy development and creation of common activity chains	Determine strategy, produce strategic research agendas and roadmaps for IoT technology and applications, action plans, continuous evaluation (fine tuned visions).	Market and national knowledge, awareness and vision. Consensus building among projects including the use of external expertise to support the process.	Develop the annual strategic research agenda, publish the Cluster book with focus on European and Global IoT research and development trends.
Implementation	Improve IERC dynamics by promoting the IoT enabling technologies and applications, stimulate clustering among projects at European and national level, secure common resources and participation of common events, and invest in a Cluster Web site and web space.	Select activity chains responsible with relational and analytical skills able to secure resources and organise common events while having technical skills in the area of IoT and related enabling technologies.	Organise relevant IERC meetings, common activity chain workshops, create an annual IoT week, develop R&D activities and stimulate joint projects. Set up national IoT value creation networks/clusters, innovation/research
Evaluation and sustainability	Continuous policy improvement with EU support; provide resources to the cluster, set up procedures to rapidly adapt to changing contexts, and needs.	Strategic leadership, ability to see the global view and significant change processes and re-assess integrity.	Consensus based and open discussions with the projects involved.

The activity chains are defined as work streams that group together partners or specific participants from partners around well-defined technical activities that will result in at least one output or delivery that will be used in addressing the IERC objectives

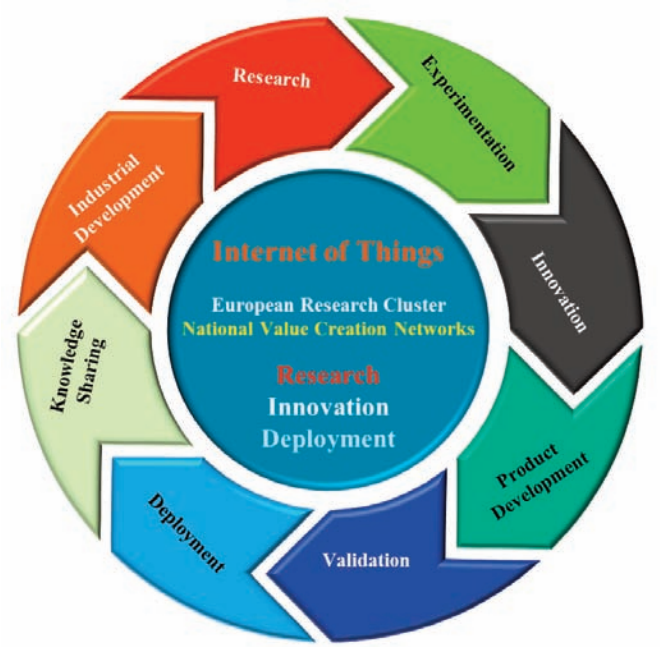


Figure 3 Internet of Things: Research-Innovation-Deployment

The creation of national IoT value creation networks/clusters, innovation/research incubators linked with the IERC allows a better coordination of knowledge-producing projects in the area of IoT at the national level with inter-linkages among different countries and cooperation at the European level through the integration with the IERC.

This liaison concept helps strengthen and replicate the success factors that are or will be achieved by specific projects in the area of IoT and will be an instrument that can help promote exchange of ideas, solutions, results and validation of these among different projects at national and European level. In the new global environment with increased competition and scarce financial resources this approach is a convenient and pragmatic organising principle at the European and national level by which to focus resources and build cooperation, partnerships and avoid duplication of effort.

IoT is considered in the global context and in order to compete globally, Europe has to use the enormous potential existing in the synergies among national science and technology programmes, and the European programmes, by favouring a multi-sector approach towards policies that push for co-operative, multi-projects and often integration of national-based and European activities in order to achieve the ultimate goal of improving competitiveness and innovation capacity in the area of IoT.

This approach provides a more transparent, inclusive and competitive framework for efforts to strengthen European IoT research efforts and Entrepreneurship and Innovation Programmes and allows easier involvement of SMEs who are participants in the national programmes.

Instruments for Pan-European Coordination of IoT Activities

The instruments used to create and integrate the national projects into a common European framework cover five distinct areas:

- Engagement of national public funding authorities and the national actors actively involved in the area of IoT,
- Creation of national value creation networks/clusters, innovation/research incubators (concentrations of projects and supporting actors financed by the national public authorities) in different European countries,
- Integration and liaison of the national activities with the IERC
- Common/collective exchange of ideas through the IERC activity chains including the European strategic research agenda for IoT
- Creation of larger-scale collaborative research and innovation initiatives in specific selected areas that require a certain critical mass in order to be successful.

The knowledge is created through innovative processes, and research/innovation is a critical input into those processes and through an increased pan-European coordination in the area of IoT allows the promotion and preservation of future national and European corporate competitiveness.

The IERC promotes in this way the integration of technological, structural, national systems of innovation under one framework where the active participants in the system are European and national companies,

universities, academic research institutions, private and public-sector educational facilities involved in projects addressing the IoT technology.

It builds on the ideas put forward by the Cluster Strategic Research Agenda and extensive discussions among the Cluster projects on overall priorities for Horizon 2020 – the Framework Programme for Research and Innovation and shows how the framework programme could support the research and innovation objectives of the Europe 2020 strategy and the Framework Programme for Research and Innovation and connects/coordinates the new framework programme with national initiatives.

Internet of Things Research and Innovation Implementation

IoT research and innovation activities should be interlinked and integrated across Horizon 2020 Framework Programme for Research and Innovation. These innovation activities must address important IoT advancements such as infrastructure development, standardisation, education programmes and measures to support important industrial sectors or innovation-conducive environments such as smart cities or regions.

Figure 4 Integration and liaison of the national activities with the European initiatives

The integration and coordination between the European programmes and national initiatives in the area of IoT offers the needed innovation-oriented, industry-driven approach as an integral part of the Horizon 2020 Framework Programme for Research and Innovation where the involvement of SMEs as drivers of innovation is ensured.

This facilitates dissemination of the IoT knowledge and technology transfer including applications that address social and societal challenges.

Internet of Things Research and Innovation Expected Results

The common framework and integration concept for IoT activities at national and European level generates programmes for innovative actions with a view to developing international networks and providing support for national programmes on knowledge and technological innovation.

The common framework and integration concept for IoT activities at national and European level is expected to:

Diversify and strengthen IoT research and innovation at the European level in partnership with national programmes by improving the innovation systems.

Improve IERC capability for drawing up and cooperating with national innovation strategies.

Build and sustain new partnerships with member states.

Improve the quality of IERC partners' programmes.

Assist EU, and national policies with new examples of good practices.

Develop a new framework for SMEs and IoT technology cluster.

Creation of new transnational links among enterprises working in the area of IoT.

Exchange of good IoT applications and technology developments practices for business networks.

Transfer of IoT technology between scientific institutions and SMEs.

New measures through venture capital for financial support for start-ups and spin-offs for new IoT developments.

Testing of innovative IoT pilot measures.

The common framework and integration concept for IoT activities at national and European level is considered to be a source of innovation and creativity since this is facilitating the development of common visions and thus contributing to achievement of common goals in the area of IoT technology, applications and services by enhancing the competitiveness of participating projects and companies/organisations through the rapid diffusion of knowledge and expertise.

In the actual economical context, common framework and integration concept for IoT activities at the national and the European level represents an efficient instrument that acts as a bridge in promoting inter-national and pan-European collaboration and in networking research, industry and services for innovation in the area of IoT.

www.internet-of-things-research.eu

"The future has already arrived.
It's just not evenly distributed yet."
William Gibson

CASAGRAS2
an EU Framework 7 Project

IERC
European Research Cluster on the Internet of Things