Vision and Challenges for Realizing the Internet of Things

ARTICLE · APRIL 2010

DOI: 10.2759/26127

Harald Sundmaeker
Institut für angewandte Systemte…

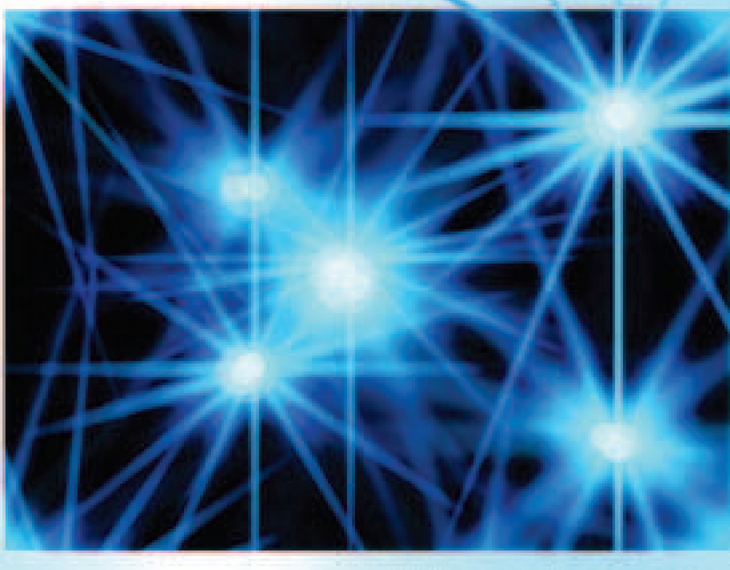
Patrick Guillemin
European Telecommunications St…

CERP-IoT

Cluster of
European Research Projects
on the Internet of Things

Vision and Challenges for Realising the Internet of Things

March 2010



Edited by
Harald Sundmaeker
Patrick Guillemin
Peter Friess
Sylvie Woelfflé

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

Antoine de Saint-Exupéry

European Commission
Information Society and Media

Editors and **Contributors**

Book Editors

Harald Sundmaeker, CuteLoop Coordinator
ATB, Bremen, Germany
Sundmaeker@atb-bremen.de

Patrick Guillemin, CERP-IoT Coordinator,
ETSI, Sophia-Antipolis, France
Patrick.Guillemin@etsi.org

Peter Friess, CERP-IoT EC Coordinator,
European Commission, Brussels Belgium
Peter.Friess@ec.europa.eu

Sylvie Woelfflé
European Commission, Brussels Belgium
Sylvie.Woelffle@ec.europa.eu

Foreword

Gérald Santucci, Head of Unit
DG INFSO Unit D.4; European Commission

SRA Core Authors and Editor Team:

Ovidiu Vermesan, NO,
SINTEF, EPoSS

Mark Harrison, UK,
University of Cambridge, Auto-ID Lab,
BRIDGE, EPCglobal Data Discovery JRG

Harald Vogt, DE,
SAP, SToP

Kostas Kalaboukas, GR,
SingularLogic, EURIDICE

Maurizio Tomasella, UK,
University of Cambridge, Auto-ID Lab,
SMART, BRIDGE

Karel Wouters, BE,
K.U.Leuven, PrimeLife

Sergio Gusmeroli, IT,
TXT e-Solutions SpA, iSURF, COIN

Stephan Haller, CH,
SAP, CoBIS

IoT Related Articles

Several teams stemming from IoT related research projects and initiatives were summarising their perspectives and experiences. The authors and their affiliation are listed within the separate sections of Chapter 4.

The editors would also like to thank the review team for their support and contributions.

Project Profiles

As popular as IoT became recently, as wide are the research fields distributed. The members of the Cluster of European Research Projects on the Internet of Things (CERP-IoT) are outlining their objectives and research work. The individual project partners and contact points are mentioned as reference for future collaboration.

For further information:

Information Desk
European Commission - Information Society and Media DG
Office: BU25 02/59 B-1049 Brussels
Email: infso-desk@ec.europa.eu
http://europa.eu/information_society

Foreword

Vision and Challenges for Realising the Internet of Things

It goes without saying that we are very content to publish this Clusterbook and to leave it today to your hands. The Cluster of European Research projects on the Internet of Things – CERP-IoT – comprises around 30 major research initiatives, platforms and networks working in the field of identification technologies such as Radio Frequency Identification and in what could become tomorrow an Internet-connected and inter-connected world of objects. The book in front of you reports to you about the research and innovation issues at stake and demonstrates approaches and examples of possible solutions.

If you take a closer look you will realise that the Cluster reflects exactly the ongoing developments towards a future Internet of Things – growing use of Identification technologies, massive deployment of simple and smart devices, increasing connection between objects and systems. Of course, many developments are less directly derived from the core research area but contribute significantly in creating the "big picture" and the paradigm change.

We are also conscious to maintain Europe's strong position in these fields and the result being achieved, but at the same time to understand the challenges ahead as a global endeavour with our international partners. As it regards international co-operation, the cluster is committed to increasing the number of common activities with the existing international partners and to looking for various stakeholders in other countries.

However, we are just at the beginning and, following the prognostics which predict 50 to 100 billion devices to be connected by 2020, the true research work starts now. The European Commission is decided to implement its Internet of Things policy for supporting an economic revival and providing better life to its citizens, and it has just selected from the last call for proposals several new Internet of Things research projects as part of the 7th Framework Programme on European Research.

We wish you now a pleasant and enjoyable reading and would ask you to stay connected with us for the future. Special thanks are expressed to Harald Sundmaeker and his team who did a remarkable effort in assembling this Clusterbook.

Brussels, March 2010

Peter Friess Gérald Santuci

Europe Direct is a service to help you find answers to your questions about the European Union

Freephone number (*)**:**

00 800 6 7 8 9 10 11

(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

More information on the European Union is available on the Internet (http://europa.eu).

Cataloguing data can be found at the end of this publication.

Luxembourg: Publications Office of the European Union, 2010

ISBN 978-92-79-15088-3
doi:10.2759/26127

Printed in Belgium

PRINTED ON WHITE CHLORINE-FREE PAPER

Table of **contents**

Chapter 1 The Internet of Things

1.1 The Internet of Things: Between the Revolution of the Internet and the Metamorphosis of Objects

Gérald Santucci

Head of Unit "Enterprise Networking and RFID"
European Commission Directorate General Information Society and Media

"The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so."

Kevin Ashton, 2009

"And men got dreaming. Shouldn't there be a network that made all my devices collaborate at all times, converse spontaneously among themselves and with the rest of the world, and all together make up a kind of single virtual computer – the sum of their respective intelligence, knowledge and know how?"

Rafi Haladjian, 2005

"Society is now created for technological, rather than for human, requirements. And that's where tragedy begins."

C. Virgil Gheorghiu, The Twenty-Fifth Hour, 1950

"Because of the crisis, doomsday is postponed"

La Gueule Ouverte, May 1968

After the World Wide Web (the 1990's) and the mobile Internet (the 2000's), we are now heading to the third and potentially most "disruptive"[1] phase of the Internet revolution – the "Internet of Things". The Internet of Things links the objects of the real world with the virtual world, thus enabling anytime, anyplace connectivity for anything and not only for anyone. It refers to a world where physical objects and beings, as well as virtual data and environments, all interact with each other in the same space and time.

[1] The term "disruptive technology" was coined by Clayton M. Christensen and introduced in his 1995 article Disruptive Technologies: Catching the Wave, which he co-wrote with Joseph L. Bower. Ref. Harvard Business Review, January-February 1995.

1 Origin of the concept of "Internet of Things"

1.1 MIT Auto-ID Center

The phrase "Internet of Things" was coined some 10 years ago by the founders of the original MIT Auto-ID Center, with special mention to Kevin Ashton in 1999[2] and David L. Brock in 2001[3]. The term "Auto-ID" refers to any broad class of identification technologies used in industry to automate, reduce errors, and increase efficiency. These technologies include bar codes, smart cards, sensors, voice recognition, and biometrics. But since 2003 the Auto-ID technology on the main stage has been Radio Frequency Identification (RFID).

The climax of the Auto-ID Center reputation occurred in September 2003, when the EPC (Electronic Product Code) Executive Symposium taking place in Chicago (Illinois, USA) marked the official launch of the EPC Network – an open technology infrastructure allowing computers to automatically identify man-made objects and track them as they flow from the plant to distribution centre to store shelves. The Symposium, supported then by more than 90 major companies from around the world – representing food, consumer goods, retail, transportation and pharmaceuticals industries, among others – highlighted RFID deemed to become a key enabling technology for economic growth in the next fifty years. Considering the Symposium in historic terms, Kevin Ashton foretold a shift from computer information processing to computer sensing.

A few weeks after the Symposium, in October 2003, the MIT Auto-ID Center was rechristened as Cambridge Auto-ID Lab when it was closed and split into a research arm – the Auto-ID Labs – and a commercial arm – EPCglobal, a joint venture between UCC and EAN.

The goal of the Auto-ID Labs is to develop a network connecting computers to objects – not just the hardware (RFID tags and readers) or the software to run the network, but actually everything that is needed to create an Internet of Things, including affordable hardware, network software and protocols, and languages for describing objects in ways computers can understand. It is important to note that the Auto-ID Labs is not seeking to create another global network but rather to develop the elements built on top of the Internet[4] that would enable tracking items and sharing information over the Internet.

1.2 When Internet of Things leaves the lab to come in broad daylight

Among the first papers of general interest on the Internet of Things, those mentioned below marked the beginning of a new era for commerce and industry. The Internet of Things is considered then as the mere extension of Radio Frequency Identification where "*RFID is kind of the amoeba of the wireless computing world*" (Kevin Ashton). But the phrase "Internet of Things" points out a vision of the machines of the future: in the nineteenth century, machines learned to do; in the twentieth century, they learned to think; and in the twenty-first century, they are learning *to perceive* – they actually sense and respond.

- "The Internet of Things", by Sean Dodson, The Guardian, 9 October 2003.[5]
- "Toward a Global Internet of Things", by Steve Meloan, Sun Microsystems, 11 November 2003.[6] It heralded that "With the official release of the Electronic Product Code Network, we are about to see the Internet of Things paradigm enter the big time – the world of mainstream commerce". Sun Microsystems argued of course that with its notion that "The Network is the Computer", it was uniquely positioned to play a leading role in the Auto-ID revolution, especially with respect to security, scalability and cross-platform compatibility.
- "A Machine-to-Machine Internet of Things", Business Week, 26 April 2004.

---

2 "*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*", Kevin Ashton, RFID Journal, 22 June 2009.

3 David L. Brock, MIT Auto-ID Center, MIT-AUTOID-WH-002, "The Electronic Product Code", January 2001.

4 More specifically the Electronic Product Code (which gives each item a unique number), the Object Name Service (which points a computer to an address on the Internet where information about a product is stored), the XML-based Physical Markup Language (which enables computers to gather information and act on it), and the software technology called Savant (which allows to manage and move information in a way that doesn't overload existing corporate and public networks).

5 http://www.guardian.co.uk/technology/2003/oct/09/shopping.newmedia

6 http://java.sun.com/developer/technicalArticles/Ecommerce/rfid/. This article heralded that "*With the official release of the Electronic Product Code Network, we are about to see the Internet of Things paradigm enter the big time – the world of mainstream commerce*". Sun Microsystems argued that with its notion that "The Network is the Computer", it was uniquely positioned to play a leading role in the Auto-ID revolution, especially with respect to security, scalability and cross-platform compatibility.

- "The Internet of Things", by Neil Gershenfeld, Raffi Krikorian and Danny Cohen, Scientific American Magazine, October 2004 – "The principles that gave rise to the Internet are now leading to a new kind of network of everyday devices."
- "The Internet of Things: Start-ups jump into next big thing: tiny networked chips", by Robert Weisman, The Boston Globe, 25 October 2004.[7]

1.3 International Telecommunications Union (ITU)

The concept of "Internet of Things" came into limelight in 2005 when the International Telecommunications Union published the first report on the subject[8]. At that time, Lara Srivastava, ITU's Strategy and Policy Unit, said: "*It's safe to say that technology today is more pervasive than we would ever have imagined possible 10 years ago. Similarly, 10 years from now things will continue in this general direction. That's what these new technologies are telling us.*"

The ITU report adopts a comprehensive and holistic approach by suggesting that the Internet of Things will connect the world's objects in both a sensory and intelligent manner through combining technological developments in item identification ("tagging things"), sensors and wireless sensor networks ("feeling things"), embedded systems ("thinking things") and nanotechnology ("shrinking things"). By addressing ICT and nanotechnology together, this report touches on the concept of "convergent technologies" brought up by the U.S. National Science Foundation (NSF) in its 2002 report for achieving "a tremendous improvement in human abilities, societal outcomes, the nation's productivity, and the quality of life"[9] . At the same time, the ITU report identifies the most important challenges that need to be tackled for fully exploiting the potential of the Internet of Things – standardisation and harmonisation, privacy, and socio-ethical issues.

2 Development of the Internet of Things

Today, there are roughly 1.5 billion Internet-enabled PCs and over 1 billion Internet-enabled cell phones. The present "Internet of PCs" will move towards an "Internet of Things" in which 50 to 100 billion devices will be connected to the Internet by 2020. Some projections indicate that in the same year, the number of mobile machine sessions will be 30 times higher than the number of mobile person sessions. If we consider not only machine-to-machine communications but communications among all kinds of objects, then the potential number of objects to be connected to the Internet arises to 100,000 billion[10]! In such a new paradigm, networked objects are so many that they blur the line between bits and atoms. Several authors have created new concepts to apprehend the Internet of Things paradigm. For example, Julian Bleecker speaks of *blogjects* to describe objects that blog[11], Bruce Sterling speaks of *spimes* to portray location-aware, environment-aware, self-logging, self-documenting, uniquely identified objects that provide a lot of data about themselves and their environment, Adam Greenfield speaks of the "informational shadows" of networked objects, Rafi Haladjian speaks of the Pervasive Network connecting any type of machine, permanently and seamlessly, both indoors and outdoors, at high speed and at an imperceptible cost, but not with just anyone/anything.

All specialists agree that the challenges of the Internet of Things will be manifold and far-reaching. We will try here to identify some of these challenges by considering the perspectives of Research, Industry, and Central and Local Government. Obviously, many initiatives involve Research, Industry and Government at the same time like, for instance, the three-year project, announced in February 2010, involving the U.S. National Science Foundation (NSF) and Microsoft[12].

---

7 http://www.boston.com/business/technology/articles/2004/10/25/the_internet_of_things/
8 "The Internet of Things", ITU, November 2005.
9 NSF/DOC-sponsored Report, "Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science", June 2002.
10 Source: Rafi Haladjian, inventor of the communicating rabbit Nabaztag, 25 May 2009.
11 Perhaps we could speak as well of *twitterjects* if we consider that networked objects all around the world will be able to share and discover almost instantly what's happening in their environments.
12 The goal of this project is to give American scientific researchers the Cloud Computing power to cope with exploding amounts of research data.

2.1 Research perspective

Today the Auto-ID Labs form an independent network of seven academic research labs on four different continents[13] that develop new technology such as RFID and Wireless Sensor Networks (WSNs) for revolutionising global commerce and providing previously unrealisable consumer benefits.

Three of the laboratories – University of St. Gallen, ETH Zurich and MIT – organised in Zurich in 2008 the first Internet of Things Conference[14] that brought leading researchers and practitioners from both academia and industry together to facilitate sharing of applications, research results, and knowledge. The next conference will be organised at the end of 2010 in Tokyo around the theme "IoT for a Green Planet"[15] – it will explore the technical requirements and business challenges to address today's societal challenges with IoT technology: Health monitoring systems to support the aging society, distributed awareness to help predict natural disasters and react more appropriately, track and trace to help reduce traffic congestion, product lifetime information to improve recyclability, transparency of transportation to reduce carbon footprint, and more insights into various kinds of processes to improve optimisation. It is noteworthy that this conference will take place at about the same time as the 27th TRON Project Symposium on the Ubiquitous Computing Society, which is organised every year by Professor Ken Sakamura[16].

Another research perspective for the Internet of Things is given by Hewlett-Packard which has launched a ten-year mission, a Central Nervous System for the Earth, to embed up to a trillion pushpin-size sensors around the globe. By combining electronics and nanotechnology expertise, Hewlett-Packard researchers have developed "smart dust" sensors with accelerometers that are up to 1,000 times more sensitive than the commercial motion detectors used in Nintendo Wii video game controllers and some smart phones. Potential applications include buildings that manage their own energy use, bridges that sense motion and metal fatigue, cars that track traffic patterns and report potholes, and fruit and vegetable shipments that tell grocers when they ripen and begin to spoil.

In China, research in the field of Internet of Things is viewed as essential to foster economic growth and catch up with the developed countries. Since 2006, several research institutes have been involved in a far-reaching project, including Shanghai Institute of Microsystem and Information Technology (SIMIT), Chinese Academy of Sciences (CAS), Nanjing University of Aeronautics and Astronautics, North-western Polytechnical University of China, with strong support from Chinese government. Researchers in Electrical & Electronic Experiment Demonstration Centre of Nanjing University of Aeronautics and Astronautics have already developed a wireless sensor network platform of their own intellectual property, which includes ad hoc network wireless sensor node, data storage and data remote access terminal.

A promising initiative for pushing forward the limits of imagination, creativity and audacity with respect to the Internet of Things is "Council" – a loose group of professionals, animated by Rob van Kranenburg, Media theorist, which includes artists, designers, coders, thinkers and tinkerers. The members of this open consultancy/think-tank "*have been through the full range of emotions and conceptual breakdown that comes with grasping the territory, the full logistical, business, social and philosophical implications of the Internet of Things.*"[17]

2.2 Industry perspective

The first industrial realisation of the Internet of Things, in the sense of RFID tags embedded in objects, was actually the Presto network in 1998[18]. Despite this forerunning initiative, during ten years, the Internet of Things was more a topic for research, especially in the Auto-ID Labs, than for industry.

---

13 The goal of this project is to give American scientific researchers the Cloud Computing power to cope with exploding amounts of research data.

14 http://www.iot2008.org/

15 http://www.iot2010.org/

16 Ken Sakamura is a Japanese Professor in information science at the University of Tokyo, Japan. He is the "father" of TRON, the real-time operating system architecture which is a dominant and essential part of most embedded systems in Japan today. He is also Director of the YRP Ubiquitous Networking Laboratory (UNL) and the Chair of Japan's T-Engine Forum and µID Centre. See http://www.tronshow.org/index-e.html

17 http://www.theinternetofthings.eu/

18 Henry Holtzman, now Chief Knowledge Officer of the MIT Media Lab, did a project back in 1997 involving RFID tags put onto Pokemon figures. Along with MIT Lab's professors Andrew Lippman and Michael Hawley, Holtzman created in 1998 a commercial company, Presto Technologies, to output Internet of Things products. See Wired article of February 2000 at http://www.wired.com/wired/archive/8.02/mustread.html?pg=14

When in January 2005 Wal-Mart and the U.S. Department of Defence demanded that their major contractors and suppliers mark their shipments with RFID tags for inventory control, Kevin Ashton said: "*It is an incredible milestone in the development of the technology. We need to understand that January 2005 is more the end of the beginning than anything else. When RFID really gets to go to the ball. It has kind of been a Cinderella technology in the basement of the computer revolution for the last ten years.*" The explosion of the RFID market in 2005 marked the dawn of the thinking about the Internet of Things...

Then, in 2008, an open group of companies launched the IPSO Alliance to promote the use of Internet Protocol (IP) in networks of "smart objects"[19]. The IPSO alliance now boasts 53 member companies, including Bosch, Cisco, Ericsson, Intel, SAP, Sun Microsystems, Texas Instruments, and – since December 2009 – Google and Fujitsu. Several large companies have already invested in Internet of Things applications such as, among others, ATOS Origin, AT&T, Cisco, Deutsche Telekom, Ericsson, Fujitsu, Google, Hitachi, IBM, Intel, Motorola, Oracle, Qualcomm, SAP, Siemens, Telefonica, Texas Instruments, Thales, VeriSign and Verizon.

Furthermore, as the Internet is running out of addresses, in the near future it will be moving to a new protocol, IPv6. The current system, IPv4, has roughly four billion addresses. The new address space can support 21^{28} (about 3.4×10^{38}) addresses, which means, to take a commonly used analogy, that it provides enough addresses for every grain of sand on every beach in the world! While it is unlikely that we will be assigning IP addresses to grains of sand, the idea of assigning them to each of the more or less 5,000 daily objects that surround us, is quite appealing. With the right technology in each object (e.g., an RFID tag) and the right network in the surroundings, it will become easy to locate and catalogue items in a few seconds and to reap the benefits of the vast array of new information that communications among them will provide. IPv6 is undoubtedly one of the steps to making the Internet of Things a reality. The IPv6 Forum[20], which is based in Europe, is working towards deploying IPv6 in line with the European Commission Communication of 27 May 2008[21].

In Europe, SAP has been an early promoter of the Internet of Things along with the Internet of Services. Noting that the Internet of Things combines the power of ubiquitous networking connectivity with modern sensor technologies, SAP highlighted the merging of the digital world with the physical world (i.e. information concerning the identity, location and condition of physical objects can be made available through the Internet anytime and anywhere), the capability of objects to communicate with each other and hence become active participants in global business processes, thus leading to tremendous efficiency gains in many industries.

But over the last few years, beyond sporadic announcements and initiatives from industry, the Internet of Things has been ramping up[22]. Some specific Internet of Things products have indeed gained visibility; few examples are given below:

- Violet's Nabaztag[23] (2005), a cute bunny that can deliver anything from ambient information through lights and sounds to verbal information,
- ZeroG Wireless (2006), a new paradigm of wireless connectivity through low-cost, small-size Wi-Fi chips embedded into any system including consumer electronics, smart energy devices, home and building controls, portable medical sensors, and sensor networks), and T2TIT (a software solution that enables secure and privacy-friendly communication between objects,
- Arduino (2008), an open-source electronics prototyping platform intended for artists, designers, hobbyists, and any "tinkerer" interested in creating interactive objects or environments,
- Alcatel-Lucent's Touchatag (2008), a contactless application service for consumers, application developers and businesses, which by using Radio Frequency Identification

[19] Smart objects are defined by the IPSO Alliance as being small computers with a sensor or actuator and a communication device, embedded in objects such as thermometers, car engines, light switches, and industry machinery. They enable a wide range of applications in areas like home automation, building automation, factory monitoring, smart cities, health management systems, smart grid and energy management, and transportation.

[20] http://www.ipv6forum.com/index.php

[21] COM(2008) 313 final.

[22] Top 10 Internet of Things Products of 2009 http://www.readwriteweb.com/archives/top_10_internet_of_things_products_of_2009.php

[23] Nabaztag, a multipurpose, Internet-connected mini-robot that talks, hears, smells objects, blinks and moves, was invented by Rafi Haladjian and Olivier Mével, and manufactured by their company, named Violet. On October 20, 2009, following a long period of technical difficulties, ultimately leading to Violet's bankruptcy, Mindscape purchased Violet.

(RFID), Near Field Communication (NFC) and 2D barcode technology provides users with one-touch, fast and easy access to, among other things, information, registration, ticketing and payment,

- Arrayent's Internet-Connect System (2009), a turnkey communication system that enables companies to connect their products to smartphones and computers via the Internet,
- Usman Haque's Pachube (2009), a service that lets the user tag and share real-time sensor data from objects, devices, buildings and environments around the world,
- Haier's Internet of Things refrigerator[24] (2010), the world's first refrigerator that can store food but also be connected to a network, for food management, and be connected with the supermarket for enhancing consumer experience.

What these first Internet of Things applications point out to is a "metamorphosis of objects" from *artefacts* (objects that are simple, hand manufactured one by one at local scale, and activated by muscular energy) to *machines* (objects that are complex, gauged, composed of several parts, and whose electric power source is neither human nor animal) to *products* (objects that are mass manufactured) and finally to gizmos (objects that are unstable, modifiable by the user, programmable, and short-lived)[25].

The emergence of the Internet of Things is likely to provoke industry disruptions and transformations as the latter often originate from major technological breakthroughs. However, what we observe at this early stage of Internet of Things deployment is that established industry incumbents and new entrants co-exist in the embryonic marketplace. Focusing on competence enhancement, the former do not seem to have great difficulty crossing the chasm created by the Internet of Things disruption (e.g., Cisco's *Intelligent Urbanization Initiative*, IBM's *Smart Planet*) while new entrants, favouring competence destroying innovations, rise rapidly to visibility and significant presence on the market by holding market niches (e.g., Arduino, Arrayent, Pachube, Violet from 2003 until 2009). This shows that changes in the emerging Internet of Things industry are likely to come more from the introduction of new business models (i.e. the organising principles and templates around which a business is built) than from the seniority and size features of the companies.

2.3 Government perspective

Several countries have recognised the importance of the Internet of Things for future economic growth and sustainability. From 2006 onwards the European Commission launched public consultations and stimulated widely open discussions on RFID and the Internet of Things, especially regarding critical policy issues such as governance, privacy, and resilience/security. These initiatives reached their climax in 2008 when the French Presidency of the European Union organised a Ministerial Meeting in Nice to address the Internet of Things within the broader context of the Future Internet. During the same period, the U.S. Government commissioned a series of studies that emphasized the strategic importance of Internet of Things for U.S. relative wealth and economic power. In 2009, Chinese Premier Wen Jiabao himself announced China's intention to push national industry to make a breakthrough in wireless sensor networking, seen as a key technology in the Internet of Things[26].

At the Final Conference of the EU-funded CASAGRAS1 coordination and support action[27], which took place in London on 6-7 October 2009, the project leaders noted that their work had proved without doubt that

"*There is the need and will for international co-operation. China, Japan, Korea and the USA are on board. Europe has taken the lead and now needs to drive the initiative as a truly global partnership. It has also been shown that governments, industry and business lacked awareness of the Internet of Things and of what it offered. Awareness and education pro-*

---

24 Haier is a Chinese company founded in 1984 (adopted current name in 1992), headquartered in Qingdao. It is the world's top refrigerator producer.

25 Source: from Bruce Sterling, Shaping Things, 2005.

26 When Chinese Premier Wen Jiabao heralded the Internet of Things as a national imperative for China, it received surprisingly little play in the western world, but in Asia it was widely advertised since it was acknowledged as an important moment signalling that not only government leaders there realise that wireless sensor networks are critical to China's future as a manufacturing power, but the Internet of Things will pervade many other industries where China is, or hopes to become, a global leader.

27 CASAGRAS was coordinated by AIM UK and included the following non-European partners: YRP Ubiquitous Networking Laboratory (Japan), Supply Chain Innovation Centre (Hong Kong), Electronics and Telecommunication Institute (Korea), and Q.E.D. Systems (USA).

grammes are key requirements in creating a better understanding of the potential and benefits, and these programmes should be especially directed at the SME community."

2.3.1 The European Union

The concept of Internet of Things was adopted by the European Union in the Commission Communication on RFID, published in March 2007[28]. But it had been beforehand debated at a workshop organised in Brussels by the European Commission's Information Society and Media Directorate-General (DG INFSO) on 6 and 7 March 2006[29].

The Council conclusions of November 2008 on Future Networks and the Internet:

- recognised that "that the Internet of Things is poised to develop and to give rise to important possibilities for developing new services but that it also represents risks in terms of the protection of individual privacy",
- welcomed the Commission's intention to "adopt a communication in 2009 on the Internet of Things, presenting architecture and governance issues and identifying a series of concrete actions to initiate", and
- invited Member States and the Commission to "*deepen, with respect to the Internet of Things, the reflection on the development of decentralised architectures and promoting a shared and decentralised network governance*" and "*contribute to ensuring the confidentiality, security, privacy and ethical management of the data that will be exchanged on the Internet of Things, for example by promoting where appropriate the possibility of deactivating RFID chips or any other way which provides empowerment and user control.*"

2.3.2 The United States

In April 2008, the U.S. National Intelligence Council published a report on "Disruptive Civil Technologies – Six Technologies with Potential Impacts on U.S. Interests out to 2025". These technologies are: Biogerontechnology; Energy Storage Materials; Biofuels and Bio-Based Chemicals; Clean Coal Technologies; Service Robotics; *The Internet of Things*.

The NIC report was prepared by SRI Consulting Business Intelligence[30]. As regards the Internet of Things, it stressed that

> "By 2025 Internet nodes may reside in everyday things – food packages, furniture, paper documents, and more. Today's developments point to future opportunities and risks that will arise when people can remotely control, locate, and monitor even the most mundane devices and articles. Popular demand combined with technology advances could drive widespread diffusion of an Internet of Things (IoT) that could, like the present Internet, contribute invaluably to economic development and military capability."

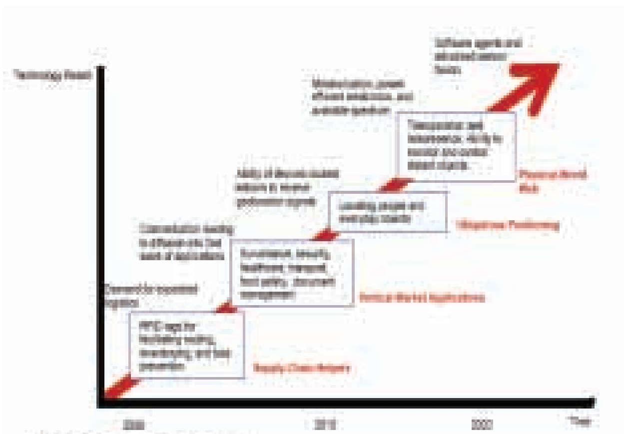


Figure 1.1-1: Source: SRI Consulting Business Intelligence

[28] COM(2007) 96 final of 15 March 2007.
[29] ftp://ftp.cordis.europa.eu/pub/ist/docs/ka4/au_conf670306_buckley_en.pdf
[30] Appendix on Internet of Things can be consulted at http://www.dni.gov/nic/PDF_GIF_confreports/disruptivetech/appendix_F.pdf

According to SRI Consulting Business Intelligence, the technologies of the Internet of Things are the following:

Enabling Building Blocks *These technologies directly contribute to the development of the IoT*	**Synergistic Technologies** *These technologies may add value to the IoT*
▪ Machine-to-machine interfaces and protocols of electronic communication ▪ Microcontrollers ▪ Wireless communication ▪ RFID technology ▪ Energy harvesting technologies ▪ Sensors ▪ Actuators ▪ Location technology ▪ Software	▪ Geo-tagging/geo-caching ▪ Biometrics ▪ Machine vision ▪ Robotics ▪ Augmented reality ▪ Mirror worlds ▪ Telepresence and adjustable autonomy ▪ Life recorders and personal black boxes ▪ Tangible user interfaces ▪ Clean technologies

A few months later was published the fourth instalment in the National Intelligence Council-led effort to identify key drivers and developments deemed likely to shape world events a decade or more in the future[31]. This report highlighted once again the importance of the Internet of Things, also named Ubiquitous Computing, i.e. the widespread tagging and networking of mundane objects such as food packages, furniture, room sensors, and paper documents:

"*Such items will be located and identified, monitored, and remotely controlled through enabling technologies – including RFID, sensor networks, tiny embedded servers, and energy harvesters – connected via the next-generation Internet using abundant, low cost and high-power computing (...) These technologies could radically accelerate a range of enhanced efficiencies, leading to integration of closed societies into the information age and security monitoring of almost all places. Supply chains would be streamlined with savings in costs and efficiencies that would reduce dependence upon human labour.*"

The U.S. Department of Defense (DoD), which operates the largest and most complex supply chain in the world, awarded in January 2009 a contract for 429 million dollars in DASH7 infrastructure. This represents a major development in terms of global adoption of an ultra low-power wireless sensor networking technology based on a single global standard.

2.3.3 China

In the second half of 2009, a number of significant public speeches were delivered about Internet of Things in China. On 7 August, Chinese Premier Wen Jiabao made a speech in the city of Wuxi calling for the rapid development of Internet of Things technologies. On that occasion, he provided the following interesting equation: *Internet + Internet of Things = Wisdom of the Earth*. This equation suggests that the Internet and the Internet of Things can be used to help humans understand the consequences of individual actions, and the relationship between those actions and physical laws ("wisdom of the Earth"). For example, we can choose to let a million vehicles idle on the highway, but in doing so we cannot escape the social consequences in terms of the environment and health.

互联网+物联网=智慧地球

Wen Jiabo followed up with another speech on 3 November at the Great Hall of the People in Beijing, in which he called for breakthroughs in wireless sensor networks and the Internet of Things.

It is expected that in 2010 China will push forward with major policy initiatives to speed up the development of its national industry. At the same time, Chinese provinces, municipalities and industrial parks will release supporting policies. In December 2009, Zhou Hongren, executive vice chairman of the Advisory Committee for State Informatization (ACSI), advised that Guangdong Province use the Internet Protocol version 6 (IPv6) first around China, be-

31 National Intelligence Council, "Global Trends: A Transformed World", NIC 2008-003, November 2008.

cause the IPv4 resources will be used up by 2012, which will somehow block the growth of the Internet of things in China[32].

2.3.4 Japan

Japan's involvement in the general field of ICT has been spelled out in the New IT Reform Strategy (January 2006) and Priority Program 2008 (August 2008) at the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (IT Strategic Headquarters). The goal is "*to realise ubiquitous and universal network society where everyone can enjoy the benefits of IT*."

The Ministry of Internal Affairs and Communications (MIC) promotes R&D and standardisation of ICT for enhancing Japan's international competitiveness. The Ministry of Education, Culture, Sports, Science and Technology (MEXT) promotes research in important fields such as life science, information technology, nanotechnology and materials, and the utilisation of quantum beam. In the field of ICT, one of the main goals is a safe ubiquitous network society, such as next-generation electronic tags. In January 2010, MEXT has released a White Paper on Science and Technology 2009.[33] The Ministry of Economy, Trade and Industry (METI) started in 2008 the Green IT Project aiming at a balance between environment and economy.

In February 2009, Japan's METI and European Commission's DG INFSO concluded a Memorandum of Cooperation on RFID, wireless sensor networks and the Internet of Things. Besides a joint commitment to developing a regular dialogue, the two entities will cooperate on social acceptance (accessibility, consumer convenience, privacy, etc), networked RFID and future Internet of Things, health and environmental impact, and harmonisation issues (code system, definition of messages, development of open global standards and/or harmonisation of regional standards, interoperability between different systems).

Table 1.1-1: Main R&D priorities for MIC, MEXT and METI.
(Source: from the White Paper on Science and Technology 2009)

	MIC	MEXT	METI
Networking	All-packet type, highly functional network; increase in Internet traffic; information-communication infrastructure; all-optical networks with ultra-high speed and extremely low power consumption; sharing of multiple wireless systems with the same frequency; wireless systems in unused frequency bands; beyond the next-generation network.		
Ubiquitous networking	RFID tags and sensors (2004-2007); Ubiquitous Platform Technology R&D (since 2008); digitalisation of home appliances; broadband networks.		
Device/ display		Innovative spin device; large-capacity, high-speed storage to realise high-function and ultra low-power consumption computing.	Miniaturisation technologies for a 45-nanometer or smaller technology node; next-generation memory with a non-volatile function; chip technology to reduce power consumption in information household appliances; 3D integration technology in a

[32] By September 2008, there had been 66,290 allocated IPv6 addresses worldwide, including 14,729 for the U.S., followed by Germany, Japan, France, Australia, and South Korea. While Brazil had then 128 IPv6 addresses, the figure was only 54 in China, which is insufficient to meet the demand of advanced applications and restrains the steady and sustainable growth of the Internet industry.

[33] http://www.mext.go.jp/english/wp/1288376.htm

	MIC	MEXT	METI
			semiconductor device (since 2008); Green IT (router to control power consumption, etc).
Security and software	Prevention of information leaks; technologies for detecting, mitigating and preventing BGP prefix hijacking.	Visualisation techniques for software construction status; software for system integration and cooperation to realise e-Science.	Bot trapping/analysing system; prevention of damage caused by new types of threats to information security; management techniques for developing a secure IT environment for people; voice recognition for consumer convenience.
Human interface and content	Super-ultra-high-density image broadcasting; future 3D imaging techniques; network voice translation (one of the Pioneering Projects for Accelerating Social Return); believability of information among various types of information available on networks.	Super-high-performance database platform software enabling the management and utilisation of huge amounts of data; software enabling the seamless use of various computers distributed throughout Japan.	Accurate search and analysis of required information from among large amounts of data and infrastructure for futuristic business (Information Grand Voyage Project).
Robotics	Robots with versatile sensors and devices that can provide services like life support and welfare/caretaking support.		Industrial robots, service robots, and special environmental work robots; intelligence technologies for the rapidly changing environment of production and the living environment; standardised methods to connect and control various components of robots and to make reusable parts (modules).

2.4 Smart City perspective

The initiatives of IBM (*Smarter Planet*: "instrument the world's systems, interconnect them, make them intelligent") and Cisco (*Intelligent Urbanization*: "using the network as a utility for integrated city management"), already mentioned, but also General Electric (*Ecomagination*: "solve today's environmental challenges and benefit customers and society at large") and other multinational companies, are typical examples of the contribution of the Internet of Things to the development of Smart Cities.

By 2050, 70% of people on Earth will live in cities, which suggests that more than states, regions or perhaps even nations, cities are increasingly for businesses the central measure for success or failure. New Songdo City in Korea is still today the most famous smart city project so far, covering all aspects from infrastructure to architecture, transportation, utilities, density, open space and parks, in short everything that defines the substance of an urban area. There has been also the Ubiquitous Network Project of Tokyo University Professor Ken Sakamura, which started in 2007 with a field test in Tokyo's Ginza shopping district where more than 1,200 chips, 270 infrared spotlights, and 16 Wi-Fi stations were placed on lampposts, flower beds, stores, and underground subway tunnels.

Many other smart city projects have emerged over the last few years in different parts of the world. They concern the rise of "new cities" – e.g., King Abdullah Economic City (KAEC) in Saudi Arabia, (MASDAR) in Abu Dhabi, Gujarat International Finance Tec-City (GIFT) in India, the Infocomm Development Authority (iDA) of Singapore – or the modernization of existing cities – e.g., Amsterdam CITYNET in The Netherlands, Borlänge City in Sweden, San Francisco TechConnect in California, U.S., Yangzhou in China's Jiangsu province, Santander in Spain. Using Internet of Things technology that offers wireless communication and real-time data such as temperature, pressure, vibrations, and energy measurements between the devices which surround us, endless applications are being developed aiming at positioning cities as attractive global investment nodes for advanced manufacturing and service industries.

The development of Smart Cities is often – not always – carried out through a partnership between the local public authorities and the private sector (e.g., Cisco-KAEC, GE-City of Yangzhou, IBM-Stockholm). The European Commission, building upon its 10-year old IADS experience[34], intends to support initiatives regarding Smart Cities through the "Future Internet Public Private Partnership" (FP7, 2011-2012 Work Programme) and the ICT Policy Support Programme (CIP, 2010 Work Programme).

3 IoT research and technological development in Europe

The debate about Internet of Things in Europe rose at a time when the structure of the 7th Research Framework Programme (FP7) was already established. It is obvious that the holistic approach adopted by the "Networked Enterprise and Radio Frequency Identification (RFID)" unit (DG INFSO/D4) in its initiatives, especially the Communication of June 2009 and its follow-up, deemed to draw attention in policy makers, academics and industry and to yield considerable and lasting benefits for the European economy and society, does not fit well the FP7 structure with its few "Challenges" and associated "Objectives". During the implementation of the first two ICT-FP7 Work Programmes (2007-2008 and 2009-2010), the networking and communications aspects of IoT fell clearly within the remit of Challenge 1 (*Pervasive and Trustworthy Network and Service Infrastructures*) whereas the hardware aspects (nanotechnologies, sensor technologies, solutions bridging nano and micro systems, etc.) matched better the contents of Challenge 3 (*Components, Systems, Engineering*) and the applications aspects could be found relevant to the contents of Challenge 5 (*Towards sustainable and personalised healthcare*), Challenge 6 (*ICT for Mobility, Environmental Sustainability and Energy Efficiency*), and Challenge 7 (*ICT for Independent Living, Inclusion and Governance*).

This discrepancy between a vision (Internet of Things), the related technologies (RFID, sensors, wireless sensor networks, nanotechnologies, etc.), and the available policy instruments (FP7) will unfortunately not disappear rapidly. It would not be advisable indeed to modify the structure of FP7 for accommodating just one particular vision. But it can be regretted that the FP5 idea of "cross-programme actions" was abandoned in the next Research Framework Programmes, and hence the possibility of clustering the projects from different "Challenges" with respect to their adherence to the IoT vision should be explored. The recommendations put forward by a number of relevant industry groups, especially the IST Advisory Group (see 3.1 below), go in the same direction.

Meanwhile, in 2008, DG INFSO/D4 had taken the initiative of defining the contents of a specific call for proposals (Call 5 of the 2009-2010 Work Programme) for addressing Internet of Things in a dedicated and holistic way. The response to this call, which was received at the end of 2009, was high and the overall quality of the proposals very good or good.

3.1 Setting the scene

The IST Advisory Group (ISTAG)[35], which was set up in 1998 to advise the Commission on the overall strategy to be followed in carrying out the ICT thematic priority under the European Framework Programme for Research, stated in a 2009 report[36] that "*the development of a Future Internet with its three components (Internet of services, network architectures and technologies, Internet of things) [was] a key development for the ICT sector*". Referring to the Internet of things as "*an explosive increase in the number of devices attached to the Internet, including many machines, sensors and intelligent devices*", this report recommended "*to support research and development in the area of self-organizing embedded systems and autonomic diagnosis to provide the infrastructure for new applications in the coming Internet-of-Things*".

[34] In 1997, under the 4th Research Framework Programme (FP4), the European Commission selected 12 Integrated Applications for Digital Sites (IADS) projects founded on strong private-public sector partnerships and funded primarily by industry and research bodies. 52 million euro of EU funds were then attributed to the 12 projects, i.e. an average EU contribution of 4.4 million euro and a total cost per project amounting to an average of 11 million euro. Participants in these IADS projects included 43 digital cities and towns and 21 digital regions.

[35] From 1999 onwards, ISTAG popularized the phrase "Ambient Intelligence" – initially a technology vision for the timeframe 2010-2020 – that had been coined by Eli Zelkha and Brian Epstein, from Philips, in 1998.

[36] ISTAG, "Revising Europe's ICT Strategy", February 2009.

According to ISTAG, technical research challenges to turn the vision of Internet of Things into reality have to be addressed at multiple layers[37]:

- Edge technologies, such as sensors and actuators, passive/active identification tags, embedded systems, which are attached to real-world objects and make them smart enough to participate in Internet of Things scenarios.
- Networking technologies, such as fixed, mobile wired and wireless networks allowing the highly available bidirectional communication on different levels (between real-world objects, applications and services offering functionality).
- Middleware systems putting real-world data into the context of various Internet applications.
- Platform services that run in the background to support a superior management of all involved technical components in an integrated way ensuring scalability, high availability, and safety/security.

In its 2009 report, ISTAG goes further, arguing that based on Europe's experience in several fields – Embedded Systems, Wireless Autonomous Transducer Systems, Robotics, Components, and Nano-Electronics/Systems – the Internet of Things could be linked to an Internet of Services provided that "technology for context-aware, reliable, embedded, energy efficient and secure distributed networks of cooperating sensors end actuators, as well as the energy provision for this technology" is made available. Such technology would require a 'total system" solution (from systems theory of massive distributed networks through embedded software platforms to the development of "more than Moore" nano-system design) as well as new models of interaction ("beyond the desktop metaphor").

3.2 Call 5 of the ICT theme in the 7th Research Framework Programme

Call 5 of the ICT theme managed by DG Information Society and Media under the 7th Research Framework Programme (FP7) was the first time the Internet of Things community was invited to submit proposals for collaborative research in the field. It was a test of the ability and willingness of Europe's ICT community to deal cooperatively with the Internet of Things challenges. The description of the work proposed in the Call text was the following:

Architectures and technologies for an Internet of Things

- Architectures and technologies using open protocols, which enable novel Internet-based applications including – but not restricted to – business/enterprise scenarios. They should use information generated at the periphery of the network from the virtual and physical worlds with aggregation of those, and allow action on the physical world. Physical world event information are generated by tags, sensors, actuators and wireless devices. Related processes and applications may be object- or location-centric and cover management capabilities of various classes of events, such as real world events (sensor based), behavioural/people events, or business events. For business scenarios, traceability networks correlated with logistics and order or billing flows are of particular importance.
- Optimised technologies covering distribution of intelligence between the edge network and the more centralised business/process information system. This includes service discovery systems as well as scalable, secure, open middleware necessary to put real world data into the context of various Internet applications with event processing, separation and filtering. Of particular importance are the integration and interoperability with the mainstream business/process management platforms and tools and the necessary management of varying data ownership across the edge device/object life cycle.
- Architectural models enabling an open governance scheme of the Internet of Things, without centralised gatekeeper lock-in of critical business/process functionalities.

DG INFSO/D4 organised two information days in Brussels, respectively in February 2009 and September 2009, to raise awareness of the ICT community about the contents of the Objective 1.3 "Internet of Things and Enterprise Environments" and to facilitate consortium building among sector actors.

The call resulted in 45 R&D proposals related to the Internet of Things, including 9 Integrated Project proposals and 36 Specific Targeted Research Project proposals.

The call attracted 357 partners, including 178 (50%) from industry, 93 (26%) from academia, 69 (19%) from research organisations, and 17 (5%) from the public sector. This underlines the strong interest of industry in IoT research and the ability of all stakeholders to build balanced consortia. Interestingly, small- and medium-sized enterprises (i.e. roughly, independent com-

[37] Source: ISTAG, Working Group on Future Internet Infrastructure, Version 8, 23 January 2008.

panies with less than 250 employees) represent a significant 47% of all companies, which is a good indicator of the dynamism of the emerging IoT industry.

EU organisations represented 86% of all organisations involved in the call, the other 14% including countries like Norway, U.S., Brazil, Canada, Israel, and Japan. 53% of the total number of participating organisations came from only five EU countries, which shows a high degree of concentration. Germany had 49 organisations involved, followed by Spain (46), Italy (39), the United Kingdom (32) and France (23). Some countries surprisingly scored a relatively low participation figure (France, the Nordic EU countries...); conversely, countries like Greece, Switzerland, Ireland and Poland scored well in that respect.

The diagrams below give some indication of the leading organisations involved in IoT research in Europe.

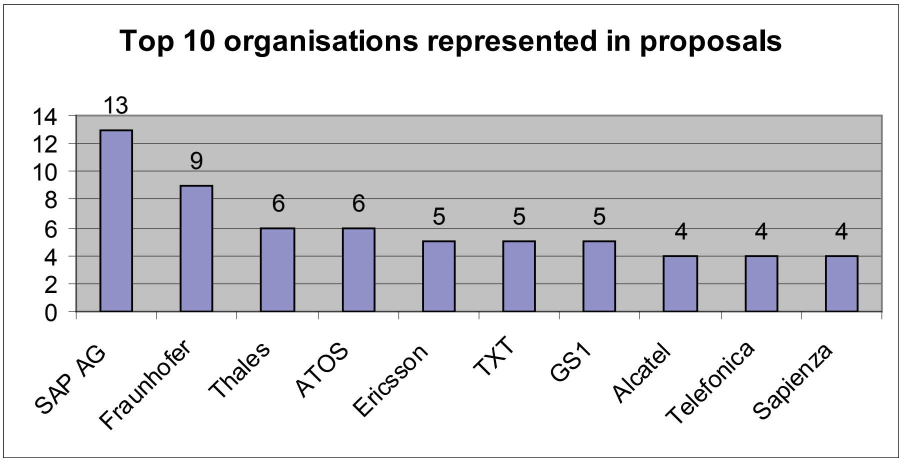


Figure 1.1-2: Top 10 organisations represented in proposals

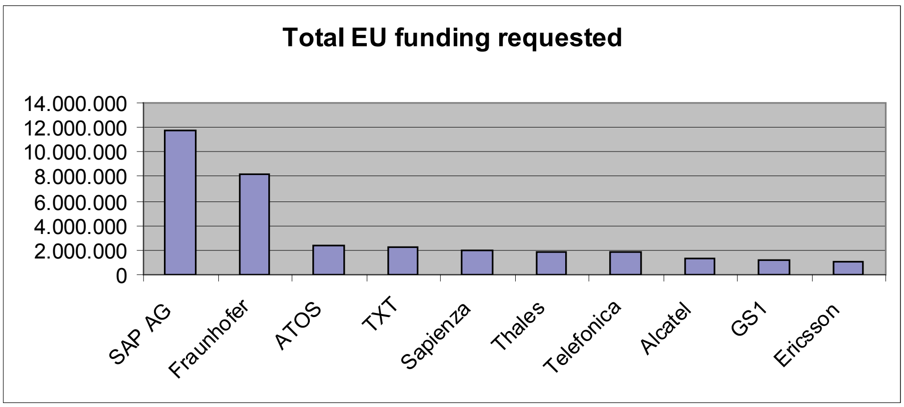


Figure 1.1-3: Total EU funding requested.

4 Conclusion

The Internet of Things is a vision that encompasses and surmounts several technologies at the confluence of Nanotechnology, Biotechnology, Information Technology and Cognitive Sciences. Over the next 10 to 15 years, the Internet of Things is likely to develop fast and shape a newer "information society" and "knowledge economy", but the direction and pace with which developments will occur are difficult to forecast.

In fact, when considering the spectrum of possibilities for the Internet of Things in the 2020-2025 timeframe, little can be said at this stage since the technology is still being refined, the industry is in a process of reconfiguration, and the market is embryonic. The main uncertainties can be grouped around two axes: the timing of developments (slow versus fast) and the depth of penetration (niches versus ubiquity)[38].

In terms of timing, the Internet of Things will grow all the more rapidly if favourable policies, technological progress and business collaboration prevail. This is actually the sort of "Golden Triangle" which the European Commission is seeking to harness through its regulatory (Directives, Recommendations), research (7th Research Framework Programme) and innovation (ICT Policy Support Programme) instruments.

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 strong market demand. Otherwise, should these demand signals not materialise, the Internet of Things would remain limited to a few niches (e.g., health care, logistics, manufacturing, health care, security, transportation).

Overall, much will depend, among other factors, on technological advances in miniaturisation and energy-efficient electronics, advances in software acting on behalf of people and actually fusing sensor information from heterogeneous sources, the size and nature of demand in the private sector (commerce, logistics, etc.) and the public sector (defence, health care, etc.), the effectiveness of initial waves of IoT in reducing costs/improving efficiencies, the ability of devices located indoors to receive geolocation signals, and the efficient use of spectrum.

The turn that the debate has taken in 2009 – a year which might be regarded later as the true beginning of the Internet of Things – with the U.S. and China joining Europe in addressing the challenges and opportunities of this vision, indicates that a growing number of analysts, not only in industry and academia but also among public decision makers, have become convinced that the Internet of Things will ignite fresh demand for a wide range of hardware and software to store, process and search the trillions of data from tags, sensors and other identification and location devices to actually create useful knowledge. *It does feel almost like the beginning of the Internet*[39]*!*

The journey to the Internet of Things will be a long one. Besides some well-known embryonic applications (Arduino, Nabaztag, Pachube, Touchatag, etc.), today objects can only exchange information within "intranets of things", i.e. environments within which processes are controlled. These objects cannot yet address any Internet of Things, which by definition should be open, uncertain and complex. One of the main challenges of the Internet of Things is therefore to transform connected objects into real actors of the Internet by developing and implementing appropriate applicative design methodologies[40]. This shift of paradigm involves major societal and ethical challenges that loom ahead and need to be tackled, certainly at European level but also at global level. The metamorphosis of objects, if left without any regulation or interference, might give rise to a genuine, extensive surveillance society. Each individual would spontaneously document his life by complementing factual information on his journeys, locations and transactions, which are today aggregated, with the micro-events of his day-to-day intimate life. Besides the technology, an open dialogue must take place on the ethics of the Internet of Things in order to mitigate the risks of a society which would be transparent for a few and opaque for all the others.

The Internet of Things fundamental challenges will be addressed in the next ICT-FP7 Work Programme (2011-2012) by inviting multi-stakeholder, multidisciplinary consortia to put forward ambitious proposals on the related technical aspects.

At the same time, DG INFSO will seek to organise and steer an open debate on the different "lines of action" described in the European Commission Communication on the Internet of Things.

[38] Source: U.S. National Intelligence Council – "Disruptive Civil Technologies: Six Technologies with Potential Impacts on U.S. Interests Out to 2025", pp39-42.

[39] Source: Katharine Frase, vice president for emerging technologies at IBM Research, quoted by The New York Times in "Smart Dust? Not Quite, but We're Getting There", 31 January 2010.

[40] See Philippe Gautier, "Internet des Objets: Objets connectés, objets communicants… ou objets acteurs", http://www.refondation.org/blog/2385/internet-des-objets-objets-connectes-objets-communicants-ou-objets-acteurs

1.2 A Poor or a Rich Internet of Things; our choice now

A look into the future and the meaning of the Internet of Things

Rob van Kranenburg

Fontys Applied Sciences, Lectoraat Ambient Intelligence/Council

The Internet of Things promises dramatic changes, yet in an age of permanent revolution the word 'revolution' itself becomes decadent, outmoded. Still it is the best word to describe disruptive innovation. It holds a promise of new and something different, alerts proven practices to the fact they too are historical, and in its most successful forms redefines the dreams and abundance of youth with the longing for stability and status quo.

1 A global revolution

In Carl Schmitt's political philosophy he makes a distinction between the *real enemy* and the *absolute enemy*. This latter enemy is the one that negates your own position, questions your very existence. The real enemy denotes our possibility to act, we can react to challenges and threats. The absolute enemy appears on thresholds to new realities that are being born out of revolutions, not out of easy transitions Heidegger foresaw the road that *Techne* (craft or art in Ancient Greece) was travelling, yet was articulating the notion of *Techne* itself. Can we see technology still as helpful in the current strategies for sustainability, energy infrastructures, and communication protocols?

In Bandung (Indonesia), artist think-tank Common Room is working with designers hoping to develop a "talking three forest" in within five years. They hope this can develop a new relationship between people and environment. Usman Haque, the founder of Pachube, one of the defining start-ups in the very young field is "quite excited by a site that Mauj (an artist think-tank in Karachi) is working with, of unofficially reclaimed mangrove area, that has much potential for analysis, speculation and actual on-site workshop action; involving both social and ecological issues, environmental as well as economic." He "would love if we could consider how some kind of citizen-oriented data collection and sense-making process could inform wider community-oriented activity."

Throughout Asia, Africa, Eastern Europe and South America, projects are being considered of pushing trials for the inclusion of RFID in banknotes in order to fight corruption and tax evasion that greatly hamper the growth of genuine public space, public institutions and generic infrastructures of energy, transport, IT infrastructure and lifelong education. Maybe it is very simply because things can only get better in a lot of places in the world. Given the current economic situation in Europe, we may have to say that things will probably get worse, not better in the terms in which we have been defining 'better'. Yet the European Union cannot lead if it cannot engender and muster a wave of positive interest and a genuine longing for more or better connectivity.

2 A mental revolution

Artists have always exploited the conditions for technological change, applications and services, from the pencil onwards. In the move towards ubiquitous computing - from the Internet to the 'Internet of Things' - the poetic process of making meaning and creating experiences is no longer only productive at the level of design, but it lies at the heart of the IT architecture of the system, its standards and protocols. In a pervasive computing environment, distributed security – which is the key to digital systems that are focused on control – will halt innovation, emerging uses and services, and launch and learn scenarios. Resonance, not interaction, is the design principle in environments where connectivity is everywhere yet not always accessible to individual users.

The Internet of Things (IoT) is a new actualization of subject-object relationships. Me and my surroundings, objects, clothes, mobility, whatever, will have an added component, a digital potentiality that is potentially outside of 'my' control. Every generation builds its own add-ons to the notions of reality, to what it believes are the foundations of the real. What makes this move so different?

There is a table. On the table a glass. A glass of tea, Jasmine? Jasmine tea. Hmm, good tea. I reach for the glass in a hurry, I gotta run. My hand, it feels like sweeping it off the table yet gently grasps it. I am not in a hurry at all. I can take it in my hand and admire the engravings. I can see drops of condensed water gently not quite sliding over the edge. I am not in a hurry. I pour you a glass. I offer it to you. Here, a glass of Jasmine tea. There are a great number of ways to reach out for a glass. And now this glass is the one your grandmother gave to you on her dying bed. You put it on the table. Pour out Jasmine tea. The affordances of a lifetime, the scope of a generation, as you reach out for the cup, the gesture itself become the reality that bridges worlds.[41]

What is most likely to happen in my opinion? A child will grow up and see a glass on that table. She will put her mobile phone/device/cuddle next to the glass. She wants to find out what it is, what it means. She will for evermore and from the beginning of her time do this with and through mediating devices. And lo and behold, a movie starts playing on its cuddle, triggered by the tag embedded in the glass. The movie is scripted by the Jasmine tea providers who tell the stories they want to tell. Finally the real has become scriptable and the scriptable becomes the real.

3 A political revolution

The primary claim to data gathering, determining what data is in the first place, what the status of information is, and how knowledge is to be made operational, is no longer wed to universities and academic institutions. Neither is its output: essay, report, document - the sole format through which broadly shared notions on what is acceptable and real can be spread. Networks of professional amateurs, informed citizens and self-taught experts as well as science itself are looking for new trusted formats of transmitting data, information and knowledge. The expertise of designers and artists in designing broadly shared events, conferences, local workshops, flash mob seminars in streets and neighbourhoods, foregrounding humour, irony, passion and love, is essential.

Maybe it can be the positive solution, the logical step in the history of outsourcing memory to objects, devices and the environment, for the challenges we all face today of an ever growing individualization that might tempt citizens into breaking with the existing solidarities (among race, gender, ethnicity, age...) that are currently harnessed through the nation state. What if through the Internet of Things we can create a layer of data, open to all, through which individuals can decide for themselves what they are willing to pay for, get direct feedback from their voluntary donations, coordinate community spending that has a direct bearing to their needs through participatory budgeting, negotiate with other people in other parts of the world how to use their money?

4 A bartering revolution

There is a broad growing consensus that current monetary systems are not working for any of the stakeholders in the long run, whether it is citizens, lenders, shareholders, investors. They might all profit maximally at one particular point in the cycle but overall loss and gain seems to even out. IoT seems to favour micropayments and transparency in transaction. We can envisage a definition of IoT identity as an ever-changing mix of relations between the physical body of a person, his or her objects and a 'smart' environment: *privacies*. Monitoring mechanisms will be built into devices themselves. It is unproductive to attempt to isolate old constants in such an environment. The privacy of objects is just as relevant or irrelevant as the privacy of persons in this fluid ecology that is called 'identity'.

[41] Rob van Kranenburg, 5 February 2010, http://www.newtechacademy.eu/

5 An educational revolution

What is the role of a museum in a world of cloud computing? What is the function of making quality decisions on what to keep and what to throw away if the Facebook generation does not delete anything anymore? Not on their mobiles, not on their laptops. Serious debating all over the world is taking place on the function of our current educational systems. In a world where hardware is becoming cheap, one can imagine a learning situation that consists of rapid prototyping skills on the one hand and making scenarios through storytelling on the other.

6 A technological revolution

Research into quick and dirty applications of soft biometrics and innovative ways of gaining biofeedback in intuitive and non-invasive ways are of paramount importance. Taking into account as much of the granularity of experience as input into our systems, may lead to not only an acceptance of ambient intelligence, but an embracing of it by people who realize that this could actually help them gain more agency – individual and collective – through getting real-time feedback on real actions and real needs.

7 A spiritual revolution

In *Separating and containing people and things in Mongolia*, Rebecca Empson writes: "... the doing involved in making things visible or invisible makes relations. In this sense 'vision' becomes the tool by which relations are created."

The *komuso*, a wandering monk, plays a central part in the history of Japanese *Shakuhachi* music. From behind their wicker visors these men wearing straw hats have "viewed the flow of Japanese life from the seventeenth century to the present", as Charles P. Malm writes. The ranks of the komuso were filled with conspirators or antisocial groups such as *Ninja* and *Ronin*. In Kyoto, a group of komuso called themselves the *Fukeshu*. Malm writes: "The Buddhist shogun government, which had smashed all Christian inspired opposition after the battle of Shimabara, was very suspicious of any form of organisation that contained these samurai whose allegiance was doubtful." The *Fukeshu* secretly purchased a building that belonged to one of the larger Buddhist temples. By faking a number of papers claiming their historical origins as coming from China via a priest named Chosan, the *Fukeshu* tried to secure their position. They also produced a copy of a license from the first Edo Shogun, Ieyasu, giving them the exclusive right to solicit alms by means of *Shakuhachi* playing. When a samurai became *Ronin* he could no longer wear his double sword. So these wandering monks redesigned the *Shakuhachi*. The flute became a formidable club as well as a musical instrument. The *Fukeshu* asked for official recognition of their temple. The government demanded the official document. The *Fukeshu* claimed it was lost. The shogun granted their request on the condition that they act as spies for the government. The *Fukeshu* accepted, playing soft melodies and overhearing intimate conversations. If we read these steps backwards there always seems to be one more mask.

The final layer is nonexistent, the essence never material, the object ever empty. It is very hard to debate this. At one particular point, somebody decides to give meaning to some data, any data. This is an act of will. Any society entering an ontologically different frontier needs strong stories to actualize its promises through and with the people.

Conclusion: poor or rich; a choice to be made

We can safely assume that the above trends will take place or grow to be effective in the coming years. There are many possible futures forming a continuum with at one end a 'poor' and at the other a 'rich' potential actualization. The decision is up to us *now* and could not come at a worse time. For the trend is towards not taking risks but having safety and security and nothing-happening-that-is-not-in-my-to-do-list as a default for decision-making. The responsibility of the entire field - from policy to programming - is to show leadership in feeling comfortable in more insecure times, in trusting the inherent traits for collaboration and friendship, and in combining Europe's strong human rights and democratic tradition with the new balances required by the IoT between the "individual" and the "collective".

Chapter 2 The CERP-IoT Cluster

Cluster Description

Cluster of European Research Projects on the Internet of Things

CERP-IoT: Cluster of European Research Projects on the Internet of Things

http://www.rfid-in-action.eu/cerp-iot

The Internet is based on a layered, end to end model that allows individuals at each level of the network to innovate free of any central control. By, placing intelligence at the edge of the network rather than control in the middle of the network, the Internet has created a platform for innovation.

The advances in technology create the basis of high rate of change and progress of Internet functions and applications. In the world there are many more "things" than "people" and the integration of the Internet with the physical world will be a challenge for the future Internet technology and propagate the coming of a new paradigm shift in information processing.

Today the world of the Internet and the physical world are almost two standalone worlds with "people" being the interface between the two and the development of the future Internet of Things will make that these two worlds will get significantly intertwined.

The ultimate vision, is an "Internet of things" linking tens of thousands of sensor networks using a convergence of technologies that will let companies and individuals keep track of every physical item on earth at every moment, while addressing the privacy and security concerns.

The development of Internet of Things depends on dynamic technical innovation in number of important fields from wireless sensors to nanotechnology, software to embedded systems.

The world is increasingly merged into a global market economy, and one of the main pillars of European information and communication technology policy is stimulating technological innovation and global cooperation with the United States, Japan, China, South Korea, and other countries for enhancing competitiveness and developing technologies such as "Future Internet" and "Internet of Things" targeting the future global society.

Today, 10 per cent of all the mobile phones sold in China are smart phones, and this is growing at annual rate of 28 per cent. China is speeding up on development of "Internet of Things", making it a new engine for economic growth and an opportunity to catch up with the developed countries. China has started exploring the 'Internet of Things' (IoT) concept where objects, equipped with wireless identifying devices, are able to communicate with each other to form, a self configuring network. The areas of application would be public assets/facilities management, environmental surveillance, disaster management, and remote monitoring of health.

In order to leverage IoT successfully the global cooperation between Europe, US, India and Asia (China, Japan, Korea, etc.) is essential in order to clearly identify the technology research and development needs and work out a clear structure for different stakeholders to work together.

A number of technologies, functionalities and many functions implemented by a diverse set of systems and technologies are behind the IoT that includes aspects of electrical engineering, computer science, sensors technology, management research, and psychology.

In the context of the evolution of integrated information systems, the IoT vision will offer a new quality of integration, which is no longer limited to the information flows of the digital world but also directly links processes in the physical world as well as the associated products (e.g., objects, home appliances) and means of production (e.g., equipment, tools), which means that the scope of integration crosses the boundaries of information systems and pervades the world of physical objects and processes.

The management of processes in manufacturing, logistics, sales, and services, mainly depends on accurate information on the availability of parts, the status of machines and tools, the correct execution of workflows, customer behaviour on the production/sales floor, and other things happening in the physical world.

The objective of this book on the Internet of Things is to present the activities of the projects financed by the European Commission in order to develop the enabling technologies for IoT, while fostering the discussion in academia, research and industry on the development of a future Internet of Things.

The projects that are addressing the underling technologies for the development of IoT have a common platform offered by the activities of the Cluster of European Projects on the Internet of Things

The European Research Cluster on the Internet of Things is part of Europe's ambition to shape a future Internet of Things (IoT) for its businesses and citizens.

The research cluster (CERP-IoT) goal is to bring European research projects together to define and promote a common vision of the Internet of Things with the main objectives to:

- Facilitate networking of different IoT projects in Europe
- Coordinate research activities in IoT
- Leverage expertise, talents, and resources and maximise impact
- Establish synergies between projects and ensure international collaboration

During the last years 32 EU-funded projects and initiatives were actively involved in the Cluster activates. A table with a short description of each project is presented in annex of this section.

The projects address different technologies and a short overview of the topics covered is given below:

- STOP: anti counterfeiting and how to deal with it in an IoT
- CuteLoop: Challenges for usage of Intelligent Networked devices
- STOLPAN: NFC technology and its application scenarios in a future IoT
- SMART, TRASER: Usage of RFID in tracking and tracing - lessons learnt and outlook towards IoT
- CASAGRAS, GRIFS: Standardisation issues challenges on RFID and a future IoT
- BRIDGE: Specific solutions for RFID and outlook towards a future IoT
- ASPIRE, HYDRA: Open source Middleware and for embedded systems for SMEs with respect to RFID and outlook to a future IoT
- INDISPUTABLE KEY: Usage of RFID in the wood environment and contribution to environment protection European
- RACE networkRFID: Stimulating the take-up of RFID in Europe
- ETP EPoSS: Outlook on future IoT applications

A brief description of the results from a selected number of the projects participating in the Cluster is presented below.

CuteLoop project has identified innovative features based on the requirements analysis in food chain and craftsmen business environments. Those features were seen as enablers to decentralise the intelligence from central entities in the overall ambience to networked devices, representing decentralised things in the integrated enterprise. Therefore, was envisaged a contribution to an evolution from classical client-server architectures towards the Internet of Things. A framework was developed, combining a multi-agent system for usage on networked devices and using both a service oriented and an event driven architecture for dynamic interaction of distributed actors. Furthermore, decentralised mechanisms for ensuring security and trust were addressed as well as an infrastructure for supporting basic interaction models of the integrated enterprise.

AMI-4-SME project has elaborated three Building Blocks for realising innovative AmI as well as human centred solutions:

- RFID based sensor system, mobile readers & middleware, highly compatible for integration with SME infrastructures.
- Speech recognition system, for implementing configurable natural human interaction on mobile devices; easy to generate & maintain; using standard interfaces.
- AmI system adaptor for mobile device, service & system integration. Enabling a flexible, secure & efficient configuration, mapping & interfacing of legacy systems, AmI services as well as mobile devices.

Moreover, the AMI-4-SME Software Platform was realised to easily set-up the required runtime environment as well as software infrastructure to provide a cost and time efficient realisation of a human centric turn-key solution.

ASPIRE project elaborated three parts for realising innovative SME oriented solution:

- ASPIRE Middleware Architecture and solution introduces a new approach to RFID middleware through a two-tier filtering:
  - Conventional filtering (e.g., EPC-ALE paradigm): Open Source Tools

(Stored/Save, Edit, Delete Filters) compliant to ALE specifications
  - Filtering of business events (i.e. based on the paradigm of BEG module):
    - Combination of filtered data with business metadata according to declared/ configured processes
    - Specifications for mapping sensor reading events into business events
- Filtering of many types of sensors other than RFID, like ZigBee (IEEE 802.15) and HF sensors.
- ASPIRE Low-cost hardware and Tools
- ASPIRE Trails: The trails are being performed in the areas of Logistics, Textiles-Apparel, Cold Chain Management, Process Management and Retail to lower SME entry cost barrier and Total Cost of Ownership (TCO) for RFID technology solutions Provide efficient inventory and smart services.

Moreover, the ASPIRE Middleware Platform will be user-friendly especially focusing on SME demands

The ***BRIDGE*** project delivered innovative hardware and software products. It also issued several important contributions to standard bodies in the areas of sensors, security and Discovery services. The lessons learned from the multiple pilot implementations will be inspiring for many companies in various sectors. Finally, a considerable set of education material has been made publicly available. The BRIDGE project has contributed to the development of new solutions for all businesses, from small to large. Improving skills and expertise on RFID technology and network information sharing is leading to enhanced competitiveness of European companies and to benefits to customers and citizens.

CASCADAS goal was to provide an automatic component-based framework that can support the deployment of a novel set of services, via distributed applications, which can cope with dynamic and uncertain environments, i.e. having Self-Configuration, Self-Healing; Self-Optimization; Self-Protection (self-CHOP) capabilities. CASCADAS toolkit has been successfully used to build a prototype system to suit a potentially industrial future scenario, called Behavioural Pervasive Advertisement, which takes a crowded venue, with many public screens. The advertising screens display information independent of the context. Smart services could then gather publicly information on Users and advertise their particular interests.

CoBIs project main results can be summarized as follows:

- A middleware based on a service-oriented architecture (SOA). The middleware allows the deployment of business logic in the form of services to the edge of the network. CoBIs provided the basic SOA framework as well as the tools to monitor and manage the network.
- A new service description language called CoBIL (CoBIs Language) to describe services for wireless sensor networks, their interface, their composition and dependencies as well as technical constraints regarding their deployment.
- A set of reusable collaborative services that were applied in a set of demonstrators and application trials.
- Hardware adaptation and integration of three different sensor network platforms, namely Particles, μNodes and Sindrion, through a common abstraction layer.

Application trials were conducted to show how the technology developed can be applied to a real-world setting.

Euridice is an integrated project where the basic concept is to build an information services platform centred on the individual cargo item and on its interaction with the surrounding environment and the user. The Euridice Platform will allow addressing simultaneously the logistics, business and public policy aspects of freight transportation, by dynamically combining services at different levels of cargo interaction:

- Immediate proximity services, for direct interaction with cargo items on the field, like individual shipments or packages: RFID-based identification services, mobile user services, vehicle services, site services supporting freight interaction with fixed structures such as terminals, warehouses and intermodal facilities;
- Supply chain services for interaction with the actors responsible of shipping, carrying and handling the goods, as well as producers and consignees of the goods themselves;
- Freight corridor services managed by authorities and operators in charge of infrastructures efficient operation, security and safety control, such as land and port terminals, railways and motorways for resources allocation and traffic control, customs agencies and other entities in charge of safety and security checks on the goods.

PEARS Feasibility project study the feasibility for an improved RFID system based on Silent Tags; providing increased privacy, security, affordability, reliability and performance. On the side of technical feasibility, several solutions have emerged, either with existing technologies. Moreover, advanced simulation software created within the project demonstrated that current technology capabilities (e.g. bandwidth) suffice to support a polling-based tracking system, even in the most complex retail environments. On the side of the commercial feasibility, the added security and privacy at a lower device cost has opened the possibility of countless applications, particularly in the fashion, library and jeweller industries.

SMMART has addressed an innovative approach of logistic and maintenance services based on ubiquitous availability of “in service” product data for air, road, rail and marine transport. The results are reported on both technology and system integration:

- Technology:
  - RFID tag system operating in the harsh, metallic, cumbersome environment of engines
  - Wireless, auto adaptive sensor networks
  - RFID tag systems for track and trace in Maintenance workshops
  - End to end data security and trust system
  - Innovative, high added value software features as configuration control, trouble shooting, strategic forecasting and optimisation.
- System Integration:
  - 2 demonstrations, on truck and on helicopter engine successfully validated the end to end integration.

SToP has addressed the complex issue of understanding and combating the problem of product counterfeiting by using ambient intelligence based solutions. The project’s results can be summarised as following:

- An analysis of the structure, the mechanisms, and the extent of the illicit market and the supply- and demand-side drivers of trade with counterfeit products,
- A business case framework to assist governments and companies (especially small and medium sized enterprises) to calculate the impact of illicit trade on brand name and revenue, the required financial investments to counterfeiting, and the return on investment,
- Novel product authentication approaches based on ambient intelligence technologies, in particular RFID technology and the analysis of tracking data,
- Innovative smart tagging technologies suitable for authentication,
- The product verification infrastructure, a software prototype that supports enterprises manufacturing and delivering authentic products to customers and allows consumers and supply chain participants to check the authenticity of products with a combination of various approaches,
- Integration concepts for various industries that help organisations to seamlessly integrate solutions into their products as well as their business process landscape,
- Real-world application trials that assessed the feasibility and performance of the solutions.

The present cluster book includes a CERP-IoT Strategic Research Agenda (SRA) introducing a common IoT definition, a vision of Future Internet with 18 main IoT Application Domains. The SRA proposes a list of research fields and a roadmap on future R&D until 2010, before 2015 and beyond 2020. This roadmap forms the basis for the research priorities presented and 13 IoT enabling technologies

The CERP-IoT SRA is part of a continuous IoT community dialogue initiated by the European Commission (DG Information Society and Media) for the European and international IoT stakeholders. The SRA has been largely discussed in the projects and with relevant stakeholders in Europe and overseas. CERP-IoT is fostering of the International IoT co-operation. In 2009 and 2010, the cluster collaborated with Japan, Korea, US and China and cluster stakeholders foresee IoT collaboration with India, Russia and Latin America regions.

The projects involved in CERP-IoT http://www.rfid-in-action.eu/cerp-iot are listed in the following table.

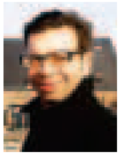
Acronym	Project Title	Coordinator
AMI-4-SME www.ami4sme.org	Ambient Intelligence Technology for Systemic Innovation in Manufacturing SMEs	Harald Sundmaeker sundmaeker@atb-bremen.de ATB, Germany
ASPIRE www.fp7-aspire.eu	Advanced Sensors and lightweight Programmable middleware for Innovative RFID Enterprise applications	Prof.Dr. Neeli R.Prasad np@es.aau.dk CTIF Aalborg, Denmark
BRIDGE www.bridge-project.eu	Building Radio frequency Identification solutions for the Global Environment	Henri Barthel henri.barthel@gs1.org GS1
CASAGRAS www.rfidglobal.eu	Coordination and Support Action (CSA) for Global RFID-related Activities and Standardisation	Ian Smith ian@aimuk.org AIM UK
CASCADAS www.cascadas-project.org	Component-ware for Autonomic Situation-aware Communications, and Dynamically Adaptable Services	Antonio Manzalini antonio.manzalini@telecomitalia.it Telecom Italia - Future Centre
CE-RFID http://www.rfid-in-action.eu/	Coordinating European Efforts for Promoting the European RFID Value Chain	Dr. Gerd Wolfram gerd.wolfram@mgi.de METRO Group, Germany
CoBIs www.cobis-online.de	Collaborative Business Items	Stephan Haller stephan.haller@sap.com SAP,Switzerland
CONFIDENCE www.confidence-eu.org	Ubiquitous Care System to Support Independent Living	Igone Velez ivelez@ceit.es CEIT, Spain
CuteLoop www.cuteloop.eu	Customer in the Loop: Using Networked Devices enabled Intelligence for Proactive Customers Integration as Drivers of Integrated Enterprise	Harald Sundmaeker sundmaeker@atb-bremen.de ATB, Germany
ETP EPoSS www.smart-systems-integration.org	European Technology Platform on Smart Systems Integration	Alessandro Bassi alessandro.bassi@Hitachi-eu.com Hitachi Europe
DACAR www.dacar.org.uk/	Data Capture and Auto Identification Reference Project	Dr. Christoph Thuemmler c.thuemmler@napier.ac.uk Chelsea and Westminster NHS Foundation Trust, London
DiYSE www.dyse.org/	DiY Smart Experiences, Creating smart experiences on the Web of Things	Marc Roelands marc.roelands@alcatel-lucent.com Bell Labs, Alcatel-Lucent, Belgium
Dynamite dynamite.vtt.fi/	Dynamic Decisions in Maintenance	Kenneth Holmberg kenneth.holmberg@vtt.fi VTT, Finland
EU-IFM www.ifm-project.eu	Interoperable Fare Management Project	John Verity compliance@itso.org.uk ITSO Limited
EURIDICE www.univiu.org/projects/euridice/	European Inter-Disciplinary Research on Intelligent Cargo for Efficient, Safe and Environment-Friendly Logistics	Paolo Paganelli paolo.paganelli@insiel.it Insiel, Italy
FIA/RWI www.rwi.future-internet.eu	Future Internet Assembly: Real World Internet	Alex Gluhak a.gluhak@surrey.ac.uk University of Surrey, UK
GRIFS www.grifs-project.eu	Global RFID Interoperability Forum for Standards	Stephane Pique stephane.pique@gs1eu.org GS1, Belgium

Acronym	Project Title	Coordinator
HYDRA www.hydramiddleware.eu	Heterogeneous physical devices in a distributed architecture	Markus Eisenhauer markus.eisenhauer@ fit.fraunhofer.de Fraunhofer FIT
IMS2020 www.ims2020.net	Intelligent Manufacturing System 2020	Dr. Dimitris Kiritsis dimitris.kiritsis@epfl.ch EPFL, Lausanne
INDISPUTABLE KEY www.indisputablekey.com	Intelligent distributed process utilization and blazing environmental key	Richard Uusijärvi richard.uusijarvi@sp.se SP, Sweden
iSURF www.isurfproject.eu	An Interoperability Service Utility for Collaborative Supply Chain Planning across Multiple Domains Supported by RFID Devices	Asuman Dogac asuman@srdc.metu.edu.tr METU, Turkey
LEAPFROG www.leapfrog-eu.org	Leadership for European Apparel Production From Research along Original Guidelines	Dieter Stellmach dieter.stellmach@ditf-denkendorf.de euratex, Belgium
PEARS Feasibility www.friendlytechnologies.eu	Privacy and Security Ensuring Affordable RFID System: Technical and Commercial Feasibility	Humberto Moran hmoran@friendlytechnologies.eu Friendly Technologies
PrimeLife www.primelife.eu	Bringing sustainable privacy and identity management to future networks and services	Dieter Sommer DSO@zurich.ibm.com IBM Zurich
PRIME	Privacy and Identity Management for Europe	Marit Hansen prime@datenschutzzentrum.de ULD,Germany
PROMISE www.promise.no	Product orientated manufacturing systems including RFID technology	Dr. Dimitris Kiritsis dimitris.kiritsis@epfl.ch EPFL, Lausanne
RACE net-workRFID www.race-networkrfid.eu	ICT PSP European RFID Thematic Network (Call2) : Raising Awareness and Competitiveness on RFID in Europe	Philippe Rohou philippe.rohou@ercim.org ERCIM, France
SMART www.smart-rfid.eu	Intelligent Integration of Supply Chain Processes and Consumer Services based on Unique Product Identification in a Networked Business Environment	Dr. Antonis Ramfos antonis.ramfos@intrasoft-intl.com Intrasoft, Belgium Dr. Katerina Pramatari k.pramatari@aueb.gr Athens University
SMMART www.smmart.eu	System for Mobile Maintenance Accessible in Real Time	Jean-Louis Boucon jean-louis.boucon@turbomeca.fr TURBOMECA, France
StoLPaN www.stolpan.com	Store Logistics and Payment with NFC	András Vilmos Vilmos@stolpan.com Motorola, Hungary
SToP www.stop-project.eu	Stop tampering of products	Harald Vogt harald.vogt@sap.com SAP, Germany
TraSer www.traser-project.eu	Identity-based Tracking and Web-Services for SMEs	Zsolt Kemeny kemeny@sztaki.hu SZTAKI,Hungary
WALTER www. walter-uwb.eu	Wireless ALliances for Testing, Experiment and Research	Franck Le Gall F.le-gall@inno-group.com Inno

CERP-IoT collaborates with the Future Internet Enterprise Systems (FInES) cluster http://cordis.europa.eu/fp7/ict/enet/ei_en.html, the European Technology Platform on Smart Sensors (ETP EPoSS) http://www.smart-systems-integration.org and the Future Internet Assembly http://rwi.future-internet.eu (FIA/RWI). In 2010 the objective are to elaborate common taxonomies and IoT reference model.

In the "Project Profiles" section of this book, the members of CERP-IoT are outlining their objectives and research work. The individual project partners and contact points are mentioned as reference for future collaboration.

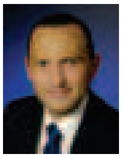
Patrick GUILLEMIN - ETSI
Patrick.Guillemin@etsi.org



Peter FRIESS - European Commission, DG Information Society and Media
Peter.Friess@ec.europa.eu

Ovidiu Vermesan - SINTEF

Ovidiu.Vermesan@sintef.no



Harald Sundmaeker - ATB Bremen

sundmaeker@atb-bremen.de

Chapter 3 Strategic Research Agenda

Executive Summary

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

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

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

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

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

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

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

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

- Safety, Security and Privacy,
- Environment Monitoring,
- People and Goods Transportation,
- Food traceability,
- Agriculture and Breeding,
- Media, entertainment and Ticketing,
- Insurance,
- Recycling.

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

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

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

SRA Coordinators:

Patrick Guillemin,
CERP-IoT Coordinator,
ETSI

Peter Friess,
CERP-IoT EC Coordinator,
European Commission

SRA Core Authors and Editor Team:

Ovidiu Vermesan, NO,
SINTEF, EPoSS

Mark Harrison, UK,
University of Cambridge, Auto-ID Lab,
BRIDGE, EPCglobal Data Discovery JRG

Harald Vogt, DE,
SAP, SToP

Kostas Kalaboukas, GR,
SingularLogic, EURIDICE

Maurizio Tomasella, UK,
University of Cambridge, Auto-ID Lab,
SMART, BRIDGE

Karel Wouters, BE,
K.U.Leuven, PrimeLife

Sergio Gusmeroli, IT,
TXT e-Solutions SpA, iSURF, COIN

Stephan Haller, CH,
SAP, CoBIS

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

Contact:

Patrick.guillemin@etsi.org

Peter.FRIESS@ec.europa.eu

3.1 Internet of Things Vision

3.1.1 Internet of Things Common Definition

The meaning of "things"

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

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

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

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

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

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

Internet of Things

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

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

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

3.1.2 Internet of Things Vision

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

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

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

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

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

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

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

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

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

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

Figure 3.1-1: Internet of Things.

The Internet of Things allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service. This implies addressing elements such as Convergence, Content, Collections (Repositories), Computing, Communication, and Connectivity in the context where there is seamless interconnection between people and things and/or between things and things so the A and C elements are present and addressed. The Internet of Things implies a symbiotic interaction among the real/physical, the digital/virtual worlds: physical entities have digital counterparts and virtual representation; things become context aware and they can sense, communicate, interact, exchange data, information and knowledge. Through the use of intelligent decision-making algorithms in software applications, appropriate rapid responses can be given to physical phenomena, based on the very latest information collected about physical entities and consideration of patterns in the historical data, either for the same entity or for similar entities. These create new opportunities to meet business requirements, create new services based on real time physical world data, gain insights into complex processes and relationships, handle incidents, address environmental degradation (pollution, disaster, global warming, etc), monitor human activities (health, movements, etc.), improve infrastructure integrity (energy, transport, etc.), and address energy efficiency issues (smart energy metering in buildings, efficient consumption by vehicles, etc.).

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

Under this vision and making use of intelligence in the supporting network infrastructure, things will be able to autonomously manage their transportation, implement fully automated processes and thus optimise logistics; they might be able to harvest the energy they need; they will configure themselves when exposed to a new environment, and show an "intelligent/cognitive" behaviour when faced with other things and deal seamlessly with unforeseen circumstances; and, finally, they might manage their own disassembly and recycling, helping to preserve the environment, at the end of their lifecycle.

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

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

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

In the physical world, things respond to stimuli from the environment in a consistent manner. When white light is shone on a red object the dye absorbs nearly all the light except the red, which is reflected. At an abstract level, the coloured surface is an interface for the object, and the light arriving at object can be a message sent to the thing, and accordingly its reflection is the response from the thing. The consistency in responses received from the interfaces for each message, enables things to interact with their surroundings. Hence to make the virtual world comprehensible, there needs to be consistency in messages and their responses. This is enabled through standard interfaces, which in turn facilitate interoperability.

Table 3.1-1: Characteristics and attributes clustered under functional domains.

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

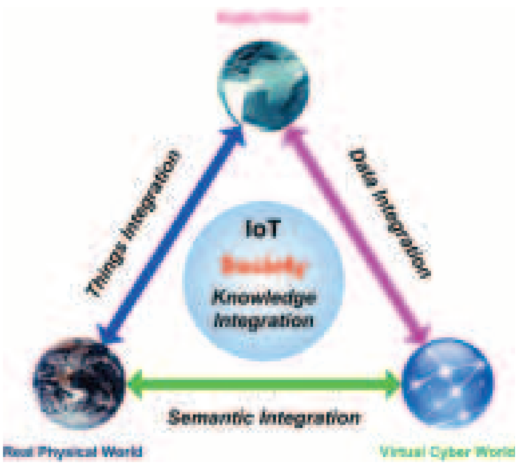


Figure 3.1-2: Internet of Things - a symbiotic interaction among the real/physical, the digital, virtual worlds and society.

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

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

3.2 Internet of Things Application Domains

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

The term "Things" can be perceived in a different way and depending on the domain in which it is used. In Industry, the "Thing" may typically be the product itself, the equipment, transportation means, etc; everything that participates in the product lifecycle. In Environment this might refer to the trees, a building, condition measurement devices, etc. Lastly, in the whole society the "Thing" may be related to devices within public spaces or devices for Ambient Assisted Living, etc.

Hence, and in order to think of the possible applications for the Internet of Things, we need to identify the main application domains, a proposal of which is illustrated in Figure 3.2-1.

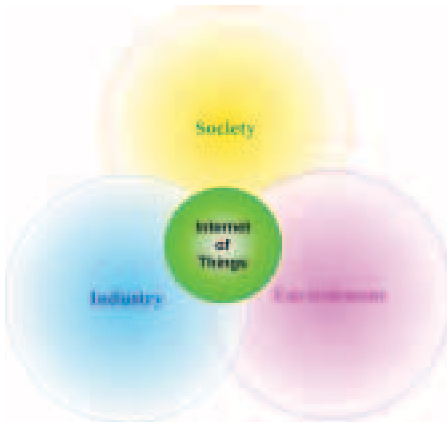


Figure 3.2-1 IoT Applications Domain.

The characteristics of each domain and some indicative examples are presented in Table 3.2-1.

Table 3.2-1: IoT Application Domains - Description and Examples.

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

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

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

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

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

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

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

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

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

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

Applications in the automotive industry include the use of "smart things" to monitor and report everything from pressure in tyres to proximity of other vehicles. RFID technology is used to streamline vehicle production, improve logistics, increase quality control and improve customer service. The devices attached to parts contain information related to the name of the manufacturer and when and where the product was made, its serial number, type, product code, and in some applications the precise location in the facility at that moment. RFID technology provides real-time data in the manufacturing process, maintenance operations and offers a new way of managing recalls more effectively.

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

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

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

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

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

3.2.3 Telecommunications

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

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

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

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

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

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

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

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

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

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

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

The combination of sensors, RFID, NFC (near field communication), Bluetooth, ZigBee, 6LoWPAN, WirelessHART, ISA100, WiFi will allow significantly improved measurement and monitoring methods of vital functions (temperature, blood pressure, heart rate, cholesterol levels, blood glucose etc). In addition, it is expected that the sensor technology will become available and at much lower cost and with built-in support for network connectivity and remote monitoring.

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

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

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

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

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

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

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

3.2.7 Pharmaceutical

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

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

3.2.8 Retail, Logistics, Supply Chain Management

Implementing the Internet of Things in Retail/Supply Chain Management has many advantages: With RFID-equipped items and smart shelves that track the present items in real time, a retailer can optimize many applications [2], like automatically checking of goods receipt, real time monitoring of stocks, tracking out-of-stocks or the detection of shoplifting. The savings potential in a retail store is large. For example, sales losses that occur when shelves go empty are estimated to be 3.9% of sales worldwide [3]. Furthermore, the data from the retail store can be used to optimize the logistics of the whole supply chain: If manufacturers know the stock and sales data from retailers, they can produce and ship the right amount of products, thus avoiding over-production and under-production.

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

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

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

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

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

3.2.10 Processing industries - Oil and Gas

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

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

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

3.2.11 Safety, Security and Privacy

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

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

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

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

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

3.2.12 Environment Monitoring

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

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

3.2.13 People and Goods Transportation

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

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

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

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

3.2.14 Food traceability

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

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

3.2.15 Agriculture and Breeding

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

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

3.2.16 Media, entertainment and Ticketing

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

3.2.17 Insurance

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

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

3.2.18 Recycling

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

3.3 Technologies supporting the Internet of Things vision

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

In this context, this Section will present the technology areas enabling the Internet of Things and will identify the research and development challenges and outline a roadmap for future research activities to provide practical and reliable solutions. This roadmap will form the basis for the research priorities presented in Chapter 3.4.

3.3.1 Identification Technology

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

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

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

By assigning each thing participating in the Internet of Things a unique identity (UID) or potentially several unique identities, it is possible to refer to each thing as an individual, each having its own characteristics, life history and information trail, its own flow pattern through the real world and its own sequence of interactions with other things. It is important that such unique identifiers for things can be globally unique and can have significant consistency and longevity (ideally for the life of the thing), independent of the current location of the thing or the current network connectivity available to the thing, in order that it is possible to gather information about a thing even when that information is collected and owned by a number of different entities and fragmented across a large number of databases and information systems.

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

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

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

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

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

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

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

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

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

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

3.3.2 Internet of Things Architecture Technology

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

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

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

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

When architecting the Internet of Things, it is important to remember that many things will not have permanent network connectivity - indeed some things may have no intrinsic network connectivity, but rely on supporting intelligence in their local environment or in remote information systems. Things will therefore need the ability to communicate their location, state and requirements to information systems that have more permanent or more reliable network connectivity. Through such information systems, a digital counterpart of the thing can be monitored or even displayed in a virtual representation, such that remote authorized entities could query or update the state of an individual thing or influence its destiny. There is therefore a need for the IoT architecture to provide effective caching and synchronisation of information updates in both directions, to support things and application scenarios that lack reliable permanent network connectivity. For example, there may be environments (such as the interior of an aircraft cabin) where network connectivity is not available either because of non-availability, electromagnetic interference or concerns about potential disruption to other mission-critical or safety-critical systems, such as the flight control system and internal communications infrastructure of an aeroplane.

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

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

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

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

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

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

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

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

Issues to be addressed:

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

3.3.3 Communication Technology

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

- Deployment – onetime, incremental or random
- Mobility – occasional or continuous performed by either selected or all "things" in the selected environment.
- Cost, size, resources, and energy – very resource limited to unlimited
- Heterogeneity – a single type of "thing" or diverse sets of differing properties and hierarchies
- Communication modality – Electromagnetic communication - radio frequency, optical, acoustic, inductive and capacitive coupled communication have been used
- Infrastructure – different applications exclude, allow or require the use of fixed infrastructure
- Network topology – single hop, star, multihop, mesh and/or multitier

- Coverage – sparse, dense or redundant
- Connectivity – continuous, occasional or sporadic
- Network size – ranging from tens of nodes to thousands
- Lifetime – few hours, several months to many years
- Other quality of service requirements – real time constraints, tamper resistance, un obtrusiveness.

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

Issues to be addressed:

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

3.3.4 Network Technology

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

In the IoT security, scalability, and cross platform compatibility between diverse networked systems will be essential. In this context the network technologies has to offer solutions that reduced costs that can offer the viability of connecting almost anything to the network, and this ubiquity of access will change the way information is processed. IP provides today end to end communication between devices, without intermediate protocol translation gateways. Protocol gateways are inherently complex to design, manage, and deploy and with the end to end architecture of IP, there are no protocol translation gateways involved.

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

Issues to be addressed:

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

3.3.5 Network Discovery

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

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

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

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

3.3.6 Software and algorithms

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

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

Issues to be addressed:

- Open middleware platforms
- Energy efficient micro operating systems
- Distributed self adaptive software for self optimization, self configuration, self healing (e.g. autonomic)
- Lightweight and open middleware based on interacting components/modules abstracting resource and network functions;
- Bio-inspired algorithms (e.g. self organization) and game theory (to overcome the risks of tragedy of commons and reaction to malicious nodes)
- Self management techniques to overcome increasing complexities
- Password distribution mechanisms for increased security and privacy
- Energy-aware operating systems and implementations.

3.3.7 Hardware

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

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

Figure 3.3-1: IoT Devices.

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

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

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

- Increasing use of "embedded intelligence"
- Networking of embedded intelligence.

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

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

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

3.3.8 Data and Signal Processing Technology

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

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

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

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

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

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

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

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

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

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

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

Issues to be addressed:

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

3.3.9 Discovery and Search Engine Technologies

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

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

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

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

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

Issues to be addressed:

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

3.3.10 Relationship Network Management Technologies

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

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

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

Issues to be addressed:

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

3.3.11 Power and Energy Storage Technologies

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

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

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

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

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

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

Issues to be addressed:

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

3.3.12 Security and Privacy Technologies

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

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

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

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

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

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

Figure 3.3-2: IoT Security and Privacy

Issues to be addressed:

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

3.3.13 Standardisation

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

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

The use of semantic ontologies and machine-readable codification should help to overcome ambiguities resulting from human error or differences and misinterpretation due to different human languages in different regions of the world, as well as assisting with cross-referencing to additional information available through other systems.

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

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

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

Re-allocation of radio spectrum is a slow process, involving government agencies, regulators and international bodies such as the International Telecommunications Union (ITU) as well as regional bodies such as the European Telecommunications Standards Institute (ETSI) or the Federal Communications Commission (FCC). Careful discussions are needed to minimise disruption to existing users of radio spectrum and to plan for future needs. In the meantime, many IoT devices using radio spectrum will need to be capable of using multiple protocols and multiple frequencies.

An example of this is the ISO 18000-6C/EPCglobal UHF Gen2 standard, which is implemented using slightly different frequencies within the 860-960 MHz band, depending on the region of operation, as well as different power levels and different protocols (at least initially in Europe, where the Listen-Before-Talk protocol was required)

Issues to be addressed:

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

3.4 Internet of Things Research Agenda, Timelines and Priorities

3.4.1 Identification Technology

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

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

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

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

3.4.2 Internet of Things Architecture Technology

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

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

IoT nodes may need to dynamically and autonomously form peer networks with other nodes, whether local or remote and this should be supported through a decentralised, distributed approach to the architecture, with support for semantic search, discovery and peer networking. Anticipating the vast volumes of data that may be generated, it is important that the architecture also includes mechanisms for moving intelligence and capabilities for filtering, pattern recognition, machine learning and decision-making towards the very edges of the network to enable distributed and decentralised processing of the information, either close to where data is generated or remotely in the cloud. The architectural design will also need to enable the processing, routing, storage and retrieval of events and allow for disconnected operations (e.g. where network connectivity might only be intermittent). Effective caching, pre-positioning and synchronisation of requests, updates and data flows need to be an integral feature of the architecture. By developing and defining the architecture in terms of open standards, we can expect increased participation from solution providers of all sizes and a competitive marketplace that benefits end users.

Issues to be addressed:

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

3.4.3 Communication Technology

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

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

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

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

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

Issues to be addressed:

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

3.4.4 Network Technology

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

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

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

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

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

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

Issues to be addressed:

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

3.4.5 Software, Services and Algorithms

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

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

Issues to be addressed include:

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

3.4.6 Hardware

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

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

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

Issues to be addressed:

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

3.4.7 Data and Signal Processing Technology

In the context of Internet of Things the devices that are operating at the edge are evolving from embedded systems to cyber physical and web enabled "things" that are integrating computation, physical and cognitive processes. Cognitive devices, embedded computers and networks will monitor and control the physical processes, with feedback loops where physical processes affect computations and cognitive processes and contrariwise. This convergence of physical computing and cognitive devices (wireless sensor networks, mobile phones, embedded systems, embedded computers, micro robots etc.) and the Internet will provide new design opportunities and challenges and requires new research that addresses the data and signal processing technology.

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

Issues to be addressed:

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

3.4.8 Discovery and Search Engine Technologies

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

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

Issues to be addressed:

- Device discovery, distributed repositories
- Positioning and localisation

- Mapping of real, digital and virtual entities
- Terrestrial mapping data
- Semantic tagging and search
- Universal authentication mechanisms.

3.4.9 Relationship Network Management Technologies

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

Issues to be addressed:

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

3.4.10 Power and Energy Storage Technologies

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

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

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

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

Research topics and issues that need to be addressed include:

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

3.4.11 Security and Privacy Technologies

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

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

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

Issues to be addressed:

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

3.4.12 Standardisation

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

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

Issues to be addressed:

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

3.4.13 Future Technological Developments

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

		Before 2010	2010-2015	2015-2020	Beyond 2020
	Data and Signal Processing Technology	• Serial data processing • Parallel data processing • Quality of services	• Energy, frequency spectrum aware data processing, • Data processing context adaptable	• Context aware data processing and data responses	• Cognitive processing and optimisation
	Discovery and Search Engine Technologies	• Sensor network ontologies • Domain specific name services	• Distributed registries, search and discovery mechanisms • Semantic discovery of sensors and sensor data	• Automatic route tagging and identification management centres	• Cognitive search engines • Autonomous search engines
	Power and Energy Storage Technologies	• Thin batteries • Li-Ion • Flat batteries • Power optimized systems (energy management) • Energy harvesting (electrostatic, piezoelectric) • Short and medium range wireless power	• Energy harvesting (energy conversion, photovoltaic) • Printed batteries • Long range wireless power	• Energy harvesting (biological, chemical, induction) • Power generation in harsh environments • Energy recycling • Wireless power	• Biodegradable batteries • Nano-power processing unit
	Security and Privacy Technologies	• Security mechanisms and protocols defined • Security mechanisms and protocols for RFID and WSN devices	• User centric context-aware privacy and privacy policies • Privacy aware data processing • Virtualisation and anonymisation	• Security and privacy profiles selection based on security and privacy needs • Privacy needs automatic evaluation • Context centric security	• Self adaptive security mechanisms and protocols
	Material Technology	• Silicon, Cu, Al Metallization • 3D processes	• SiC, GaN • Silicon • Improved/new semiconductor manufacturing processes/technologies for higher temperature ranges	• Diamond	
	Standardisation	• Standardization efforts for RFID security • Standardization of passive RFID tags with expanded memory and read/write capability for product serial numbers, repair and warranty information.	• IoT standardisation • M2M standardisation • Interoperability profiles	• Standards for cross interoperability with heterogeneous networks	• Standards for automatic communication protocols

3.4.14 Internet of Things Research Needs

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

		Before 2010	2010-2015	2015-2020	Beyond 2020
	Communication Technology	• Sensor networks, ZigBee, RFID, Bluetooth, WirelessHart, IAA100, UWB	• Long range (higher frequencies –tenth 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	• Broadband • Different networks (sensors, mobile phone, etc.,) • Interoperability framework (protocols and frequencies) • Network security (e.g. access authorization, data encryption, standards etc.)	• Grid/Cloud network • Hybrid networks • Ad hoc network formation • Self organising wireless mesh networks • Multi authentication • Networked RFID-based systems – interface with other networks – hybrid systems/networks	• Service based network • Integrated/universal authentication • Brokering of data through market mechanisms	• Need based network • Internet of Everything • Robust security based on a combination of ID metrics • Autonomous systems for non stop information technology service
	Software and Algorithms	• Service oriented architectures • Embedded software • Generation of domain specific events • "Things" Semantics / Ontologies • Filtering • Probabilistic and non-probabilistic track and trace algorithms, based upon the analysis of tracking data concerning some kind of unique ID.	• Self management and control • Micro operating systems • Context aware business event generation • Interoperable ontologies of business events • Scalable autonomous software • Software for coordinated emergence • (Enhanced) Probabilistic and non- probabilistic track and trace algorithms, run directly by individual "things". • Software and data distribution systems	• Evolving software • Self reusable software • Autonomous things: ▪ Self configurable ▪ Self healing ▪ Self management • Platform for object intelligence	• Self generating "molecular" software • Context aware software
	Hardware **Devices**	• MEMS • Low power circuits • Silicon devices • Smart multi band antennas • Beam steerable phased array antennas • Low power chip sets • Low cost tags • Small size, low cost passive func-	• Paper thin electronic display with RFID • Ultra low power EPROM/FRAM • NEMS • Polymer electronics tags • Antennas on chip • Coil on chip • Ultra low power circuits • Electronic paper • Devices capable of tolerating harsh envi-	• Polymer based memory • Molecular sensors • Autonomous circuits. • Transparent displays • Interacting tags • Collaborative tags • Heterogeneous integration • Self powering sensors	• Biodegradable antennas • Autonomous "bee" type devices

		Before 2010	2010-2015	2015-2020	Beyond 2020
		tions • High-Q inductors • High density capacitors, tuneable capacitors • Low loss switches • RF filters	ronments (extreme temperature variation, vibration and shocks conditions and contact with different chemical substances) • Nano power processing units • Silent Tags • Biodegradable antennae	• Low cost modular devices	
	Hardware **Systems, Circuits and Architectures**	• Integration of hybrid technologies sensor, actuator, display, memory • Power optimised hardware-software design • Power control of system on chip (SoC) • Development of high performance, small size, low cost passive functions e.g. high-Q inductors, tight tolerance capacitors, high density capacitors, low loss switches, RF filters, tuneable capacitors • Mobile RFID readers with increased functionality and computing power while reducing the size and cost • Miniaturised and embedded readers (SiP)	• Multi protocol front ends • Multi standard mobile readers • Extended range of tags and readers • Transmission speed • Distributed control and databases • Multi-band, multi-mode wireless sensor architectures • Smart systems on tags with sensing and actuating capabilities (temperature, pressure, humidity, display, keypads, actuators, etc.) • Ultra low power chip sets to increase operational range (passive tags) and increased energy life (semi passive, active tags). • Ultra low cost chips with security • Collision free air to air protocol	• Adaptive architectures • Reconfigurable wireless systems • Changing and adapting functionalities to the environments • Micro readers with multi standard protocols for reading sensor and actuator data • Distributed memory and processing • Low cost modular devices	• Heterogeneous architectures. • "Fluid" systems, continuously changing and adapting.
	Data and Signal Processing Technology	• Grid computing • Heterogeneous modelling of sensor data • Virtual Things identification (i.e. things identified based on A/V signal processing) • Sensor virtualization (vendor/technology independent modules)	• Common sensor ontologies (cross domain) • Distributed energy efficient data processing	• Autonomous computing • Tera scale computing	• Cognitive computing

		Before 2010	2010-2015	2015-2020	Beyond 2020
	Discovery and Search Engine Technologies	• Simple ID based object lookup • Local registries • Discovery services	• Scalable Discovery services for connecting things with services while respecting security, privacy and confidentiality • "Search Engine" for Things • IoT Browser • Multiple identities per object	• On demand service discovery/integration • Universal authentication	• Cognitive registries
	Power and Energy Storage Technologies	• Thin batteries • Energy management • RF • Thermal • Solar	• Printed batteries • Photovoltaic cells • Super capacitors • Energy conversion devices • Grid power generation • Multiple power sources	• Paper based batteries • Wireless power everywhere, anytime. • Power generation for harsh environments	• Biodegradable batteries
	Security and Privacy Technologies	• Power efficient security algorithms	• Adaptation of symmetric encryption and public key algorithms from active tags into passive tags • Low cost, secure and high performance identification/authentication devices	• Context based security activation algorithms • Service triggered security • Context-aware devices • Object intelligence	• Cognitive security systems
	Material Technology	• Polymer • Assembly and packaging techniques for RFID tags (protection against high/low temperature, mechanical, chemical substances, etc)	• Carbon • Conducting Polymers and semi-conducting polymers and molecules • Conductive ink • Flexible substrates • Modular manufacturing techniques	• Carbon nanotube	
	Standardisation	• RFID • M2M • WSN • H2H	• Privacy and security cantered standards • Adoption of standards for "intelligent" IoT devices • Language for object interaction	• Dynamic standards • Adoption of standards for interacting devices	• Evolutionary standards • Adoption of standards for personalised devices

3.5 References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Acknowledgements

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

Ali Rezafard, IE,
Afilias, EPCglobal Data Discovery JRG

Andras Vilmos, HU,
Safepay, StoLPaN

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

Antonio Manzalini, IT,
Telecom Italia, CASCADAS

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

Daniel Thiemert, UK,
University of Reading, HYDRA

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

Dimitris Kiritsis, CH,
EPFL, IMS2020

Florent Frederix, EU,
EC, EC

Franck Le Gall, FR,
Inno, WALTER

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

Harald Sundmaeker, DE,
ATB GmbH , CuteLoop

Humberto Moran, UK,
Friendly Technologies, PEARS Feasibility

Jean-Louis Boucon, FR,
TURBOMECA, SMMART

John Soldatos, GR,
Athens Information Technology, ASPIRE

Mario Hoffmann, DE,
Fraunhofer-Institute SIT, HYDRA

Markus Eisenhauer, DE,
Fraunhofer-Institute FIT, HYDRA

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

Paolo Paganelli, IT,
Insiel, EURIDICE

Wang Wenfeng, CN,
CESI/MIIT, CASAGRAS

Zsolt Kemeny, HU,
Hungarian Academy of Sciences, TraSer

Chapter 4 Articles

Articles

Teams from research projects and initiatives, that are members of CERP-IoT were summarising their perspectives and experience gained. The following articles are presenting results from currently running projects and initiatives as well as from finalised research activities:

SToP – Harald Vogt, Nina Oertel, Thorsten Staake, Mikko Lehtonen:

Anti-Counterfeiting and how to deal with it in an IoT

CuteLoop – Harald Sundmaeker, Matthias Würthele, Sebastian Scholze:

Challenges for Usage of Networked Devices Enabled Intelligence

StoLPAN – Andras Vilmos, C.M. Medaglia, A. Moroni:

NFC Technology and its Application Scenarios in a Future IoT

SMART & TRASER - Cleopatra Bardaki, Katerina Pramatari, Elisabeth Ilie-Zudor, Zsolt Kemény:

RFID-enabled Tracking and Tracing in the Supply Chain Lessons Learnt from the SMART and TRASER projects

CASAGRAS – Ian G. Smith:

An EU FP7 Project defining and accommodating international issues concerning RFID with particular reference to the emerging "Internet of Things."

GRIFS – Josef Preishuber-Pflügl:

Standardisation issues challenges on RFID and a future IoT

BRIDGE – Marc Harrison, A. Brintrup, T. Sanchez Lopez, Maurizio Tomasella, D. C. McFarlane:

Developing and Piloting the Next Generation of Networked RFID Systems

ASPIRE & HYDRA – Neeli R. Prasad, Markus Eisenhauer, Matts Ahlsén, Atta Badii, André Brinkmann, Klaus Marius Hansen, Peter Rosengren:

Open Source Middleware for Networked Embedded Systems towards Future Internet of Things

Indisputable Key – Janne Häkli, Kaarle Jaakkola, Åsa Nilsson, Kaj Nummila, Ville Puntanen, Antti Sirkka:

Usage of RFID in the Forest & Wood Industry and Contribution to Environmental Protection

RACE networkRFID – Ian G. Smith:

Stimulating the take-up of RFID in Europe

EPoSS – Ovidiu Vermesan:

Outlook on Future IoT Applications

The editors would also like to thank the review team for their support and contributions.

4.1 Anti-Counterfeiting and how to deal with it in an IoT

SToP Project

Harald Vogt, Nina Oertel / Thorsten Staake, Mikko Lehtonen

SAP Research Karlsruhe, Germany / ETH Zürich Zürich, Switzerland

Abstract: In the emerging Internet of Things, it is easy and cheap to make information available about virtually all physical objects as this information can be automatically created, distributed, and processed with the help of automatic identification systems. Thus, virtual counterparts of physical objects are being created, which provides links to services around these objects. Together with specialized technologies for the detection of physical tampering, software-supported systems for product authentication become universally available. This is a critical component to protect consumers, distribution channels, and markets against counterfeit products. We demonstrate how a prototypical system for product authentication can be integrated to existing business processes and be applied in various fields.

1 Introduction

The counterfeiting problem is growing worldwide, affecting more and more product categories and industry sectors. Counterfeits damage the reputation of brand owners, produce economic losses, promote inferior working conditions, and put the safety and health of consumers at risk. Though one might argue that counterfeiting and piracy have positive societal effects, such as giving more people access to (what appears to be) luxury hand bags, counterfeiting is never a win-win-win situation between the consumer, the brand owner, and the affected government.

Moreover, there seems to be a natural demand for counterfeit goods that will almost always be matched by a supply. Parallel markets for many such goods exist, driven by huge financial incentives. Some counterfeit goods are targeted at end-customers, while others are distributed in specialized business areas.

In industries such as the pharmaceutical and aviation industries, the targeted customers of a counterfeiter are typically composed of pharmacists and buyers of spare parts. Since elaborate control mechanisms exist in these areas, counterfeit products can only be injected into the supply chain if they comply with the quality test requirements. End-customers would be strongly interested in the use of high-quality products only. Injection of counterfeit products is therefore likely to happen from within the (otherwise legitimate) supply chain.

The market for luxury goods, including products such as clothing and accessories, is quite different. Customers are non-experts, and products are purchased usually not for functional reasons but for the "experience" and interpersonal value they provide. These aspects at the same time provide a motivation to buy counterfeit products consciously for customers for which genuine products are otherwise out of reach.

The liberalization and globalization of markets is often regarded as a threat to the integrity of supply chains. Globalization is still an ongoing process, so consumers might be exposed to an increasing number of counterfeits in the future. Some activities have been initiated on the political level, which target consumer protection but which also aim at facilitating the enforcement of rights in cases of copyright violations and counterfeiting. This will most likely lead businesses to implement measures, mostly based on standard technologies and off-the-shelf solutions. One of the results of the SToP project has been the drafting of guidelines that should help brand owners to find the approach that best suits their needs for protecting their products.

Usually, anti-counterfeiting measures include cost-intensive field investigations, case-by-case analyses, technical authentication, and legal actions. In general, their success of containing the problem and preventing the production of counterfeit products is limited. They are not sufficient to protect consumers from mass-produced faked products in a globalized market. For example, unless a high-enough percentage of counterfeit goods are seized, producing counterfeits still remains a profitable business. Thus, in a world where massive amounts of goods are shipped world-wide each day, information technology should be employed to automate the required tasks as much as possible, in order to extend their reach and to cover a larger amount of goods that can be checked.

The SToP project has analyzed the markets for counterfeit products in order to get a better understanding of the enemy. In order to select the most effective tools, the technical possibilities for brand owners to protect their brands and products, have been investigated, and systems have been drafted that help brand owners to plan their implementation of an approach for product authentication. This chapter gives an overview of the most important aspects of this work.

2 Markets for Counterfeit Products

A detailed understanding of the problem of counterfeiting is needed to derive sound requirements for solutions based on ubiquitous computing and ambient networks, which are part of the technological portfolio of the Internet of Things. An analysis of the main drivers and mechanisms of illicit trade, the roles of the different licit and illicit actors, as well as the supply and demand side of product counterfeiting is the foundation of a deep understanding.

2.1 Counterfeit Production

An analysis of producers of counterfeit goods reveals that they can be separated in different categories with different strategies. Depending on the presumed structure of a counterfeit market, appropriate counter-measures can be designed.

The first group produces counterfeit goods with the lowest average visual quality. The average functional quality has been rated as medium, in most cases allowing the owner to use the product but requiring an abdication of durability, stability, performance, or contingency reserves. The typical product complexity is low to medium, and a further analysis showed that many producers within this category target branded articles with high interpersonal values. The expected conflict with law enforcement in the country of production is the lowest among all groups. Since members within this group primarily utilize the disaggregation between brand and product, they can be labelled Disaggregators. Typical products in this group include clothing and accessories.

The second group produces counterfeit articles with the highest visual and functional quality. Product complexity is highest among all groups, often allowing for an actual consumption or usage of the counterfeit articles. Counterfeit actors within this category seem to face only limited pressure by local enforcement agencies. Since the product-related characteristics of the members within this group resemble those of the genuine articles the closest, this group can be referred to as Imitators. Typical products in this group include clothing and accessories but also fast moving consumer goods and computer hardware.

The third group is made up by producers of articles with a high visual but low functional quality. Products are typically of medium complexity and are likely to pass as genuine articles if not carefully examined. They may result in a substantial financial loss for the buyer or even endanger the user's health and safety. Consequently, their producers often face considerable punishment if their activities become known. Since the deceptive behaviour towards the buyer of the corresponding article constitutes the main characteristic of the producer, this group of counterfeiters can be labelled Fraudsters. Typical products in this group include perfumes and cosmetics.

The fourth group contains producers of goods of medium to high visual quality, but with the lowest functional quality and product complexity. Products within this category are likely to severely endanger their user or consumer. Consequently, their producers potentially face extensive conflicts with enforcement agencies. Actors within this group are termed Desperados, pointing out their unscrupulous behaviour. Typical products in this category include pharmaceutical products and mechanical parts.

The fifth group is made up of producers of articles with an average high visual and functional quality and a medium complexity. In this respect, they resemble imitators. However, the expected conflict with law enforcement agencies is significantly higher since most actors within this group target branded products upon which the state imposes high taxes. They can be referred to as Counterfeit Smugglers since they primarily profit from circumventing taxes rather than from realizing brand name related earnings. Typical products in this group include cigarettes and alcoholic drinks.

2.2 Counterfeit Consumption

The role of consumers is critical with regard to their awareness and buying behaviour, as well as their reasoning for and against purchasing counterfeit goods. Buying behaviour with respect to genuine branded goods appears to be highly similar among counterfeit consumers and others, indicating that many customers of genuine articles also purchase counterfeit goods. This demonstrates that consumers are often indifferent regarding the originality of products as long as their perceived value is appropriate.

Counterfeits are often available in good quality, which provides a strong motivation to go for a cheaper counterfeit product instead of a high-priced original one. Quality is often judged by superficial features, which are easy to verify but not necessarily give an indication about the functional quality of a product, for example a pharmaceutical product. But sometimes counterfeit products hold up to the quality of original ones even in such sensitive cases as pharmaceutical products, making the difference between an original and a counterfeit item marginal. It is much harder to argue for the original product in such a case. Of course there are good reasons to go for an original product, such as the continuity in quality. However, the casual consumer will likely be more attracted to the lower price associated with the counterfeit.

Consumers refrain from buying counterfeits if they are of poor quality, or if their availability is limited. A product of poor quality cannot provide the same value as an original product and is much less attractive to consumers even if it has a low price. Consumer goods are mostly judged based on their visible features, while for many products their functional quality is most important. However, functional quality is much harder to verify and thus often the buyer relies on proper looks or documentation. In many business areas, insufficient documentation leads to the rejection of products out of formal reasons, e.g. in the aviation industry.

Limiting the availability of counterfeits in the market can be a powerful tool to prevent consumers from buying them. Strong penalties prevent counterfeits from being offered openly in many countries, but whenever law enforcement is weak, counterfeits are more widely available. Distribution over the Internet has reached great importance, since law enforcement is often very difficult. However, popular distribution channels like auctioning or classified advertisement web sites are often cooperative and remove dubious offerings.

The indifference of consumers might be overcome through education, which conveys the values of continuous availability of high-quality products, cross-funding for research, or warranties. But these have to go hand in hand with trust in the distribution channels since otherwise consumers will have no means to ensure that a claimed original product is indeed one. Technologies for identification and authentication can help to establish that trust.

3 Automatic Identification and Authentication

The genuineness of an item can only be established by verifying its source. Even if it is physically equivalent to an original item, it may still be an imitation, and thus its use may raise, for example, legal or tax issues. In order to establish the source, an elaborate material analysis may be performed, or accompanying documentation may certify that the item in fact originates from a legitimate source. Authentication features provide a strong connection between the documentation and the item itself. This is done by physically attaching encoded information, which refers to a document, to the item such that the carrier of this information cannot be copied and thus transferred to imitated items.

In order to provide for an effective and efficient means for verification throughout the supply chain, an authentication feature must be easily accessible and automatic verification must be possible. Technologies for automatic identification provide a good starting point to meet these requirements. They can be seamlessly integrated in logistic processes and may not even require additional dedicated equipment. A background infrastructure provides the services that are necessary to access authentication information across organizations.

3.1 Authentication Features

For each type of product, such as pharmaceuticals, plane spare parts, or luxury goods, appropriate tags that comply with the manufacturing processes have to be identified or developed. Different aspects of the product packaging and product materials need to be considered. A wide range of products from several vendors are available. A key challenge is the integration of the tags into real life products. Factors to consider include cost, durability, reading speed, information capacity, and of course security.

As an example, consider an RFID tag that was developed within the SToP project to fit into the metal casing of a watch (Figure 4.1-1). The main challenge was to be able to reliably scan the tag through the metal casing while meeting the watch maker's requirements. In particular, there was a strong need to increase the reading distance of the RFID tag in a metallic environments.

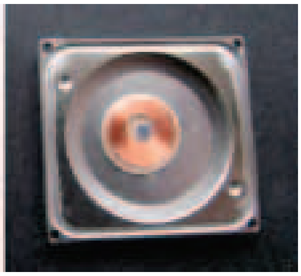


Figure 4.1-1: RFID tag embedded in the casing of a watch

Necessary adjustments of manufacturing processes to enable production of tagged products were investigated together with industry partners. The results of this task have been found to be an important factor for the real-world applicability of the concepts. Here, new requirements imposed by the utilized smart tags, such as maximum pressure or temperature, have been taken into consideration.

RFID is a wireless technology designed for automatic identification – and potentially a very effective one. Each RFID tag carries a unique identifier that can be captured with a reading device without requiring a line of sight, which makes it an appealing technology that can replace barcodes in many areas. However, standard RFID tags cannot be considered secure as it is technically feasible to clone RFID tags. Therefore, the uniqueness of an identifier cannot be guaranteed. Thus in the strict sense, standard RFID tags are not suitable as a tool for authentication. This weakness can be overcome by linking an RFID identifier with an online database, where the current status of an identifier is kept. Only if this status is valid in the current context, the item carrying the respective tag should be considered authentic.

There are developments under way that extend the standard functionality of RFID tags by secure authentication mechanisms that rely on a challenge/response protocol between the reader and the tag. The basic idea is that the tag is accepted as being genuine if and only if it responds correctly to a challenge given by the reader. The response depends on a secret key which is stored in the tag, and on a cryptographic algorithm. This however, requires more elaborate capabilities from such tags, such as securely storing the key and performing a cryptographic calculation, which increases their cost.

Due to their low cost, printed features are highly attractive as security features. One example is the "copy detection pattern" (CDP), which is a random-looking pattern of small dots that can be printed with any printing technology. Within the pattern, information such as a serial number can be encoded. The trick however is the fact that it is impossible to create a copy of this pattern that would be accepted as the original pattern. Since each scan/print cycle creates small deviations within the pattern, a statistical analysis of the pattern reveals the fact that it is a duplicate. However, the use of CDPs requires an extensive knowledge of printing technologies and they are not a "plug and play" solution.

Both technologies, RFID and printed features, have distinctive advantages and drawbacks. In general, RFID tags need not be visible and therefore they neither require dedicated space on a packaging nor do they disturb the visual appearance of an item. They can be covered by a layer of material and are thus protected against environmental forces. However, achieving high reading rates of RFID tags is still a subject to engineering challenges regarding tag integration and reader installation. In contrast, printed features are very cheap to produce and provide a high level of protection against cloning. The devices that can read tags, either RFID or printed, are widely available, for example in mobile phones. Some models include RFID readers, and almost every model includes a digital camera. Overall, this demonstrates the versatility of technologies that are building blocks of a pervasive Internet of Things.

3.2 Authentication Infrastructure

For every item that is being checked, somebody or something has to take a decision whether the item under study is genuine or not, based on the captured tag data (and possibly additional data). This means that anybody who is using a device to verify items must be connected to a background infrastructure that routes the captured data to a suitable authentication service and relays back the result of the verification.

The infrastructure must be flexible with regard to the type of checks being performed, since authentication features are evolving over time and might be replaced with others. This leads to a mix of features even on the same type of products. Depending on the outcome of a verification process, the infrastructure should also be able to trigger certain actions. For example, in case of an unsuccessful verification an automated notification could be sent to an incident response unit. As a final requirement, the infrastructure should be easy to integrate in existing business systems, since verification can be regarded as a sub-process of other business processes.

Figure 4.1-2 shows the overview architecture of a verification infrastructure, including internal components and dependencies on external entities. It is important to note that the infrastructure covers the processes relevant throughout the lifecycle of a product, including the initialization of the verification process, the execution of the verification itself, and reporting the results.

The architecture of this system is rather generic, but it has proven valid for a number of scenarios that have been tested during the SToP project. These scenarios included packing in a warehouse, verification of incoming goods in a pharmacy, verification of returned goods in after-sales service, and maintenance work on an airplane. For each scenario, specific adaptations have been made, since for each scenario, different authentication modules have been used.

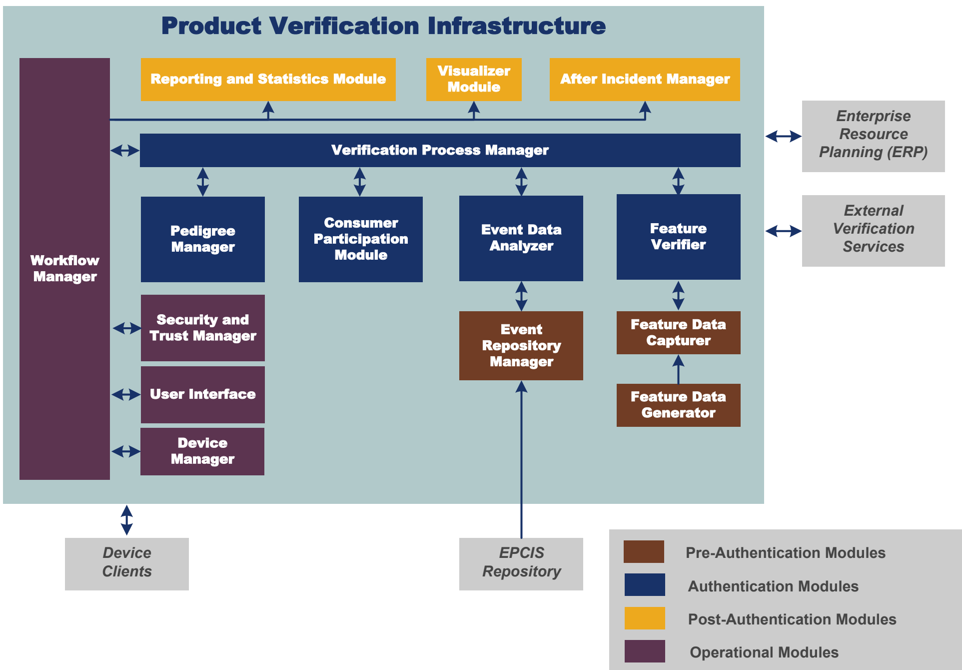


Figure 4.1-2: Architecture of a product verification infrastructure

4 Business Process Integration

Seamless integration of product authentication is important since it minimizes the costs associated with extending the involved systems and performing the authentication during usual business operations. The field trials within the SToP project have demonstrated how this can be achieved in various settings. As a first example, consider the processing of orders in a warehouse (Figure 3), where multiple packages are bundled together for outbound shipping. During bundling, items are checked using RFID tags (including background checks on the item's status). The worker gets immediate visual and acoustic feedback about the result of the check such that the workflow is only interrupted in case a non-authenticable item occurs.

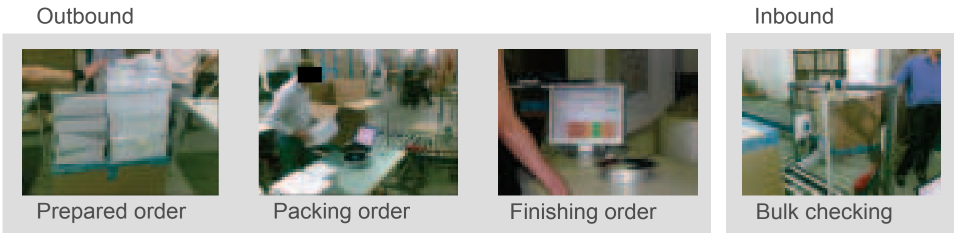


Figure 4.1-3: Outbound and inbound checking at a warehouse

Using an RFID gate, a complete bundle of items can be checked. This, however, is not completely reliable with the RFID technology (HF) being used. There are also other issues related to the use of RFID. For example, during bundling false reads can occur due to the long range of RFID readers. This can be mitigated by designing the workplace appropriately. The checks ensure that only authenticated goods are handled within the warehouse. Inbound checking is necessary if a number of external suppliers are shipping goods to the warehouse. Outbound checking is important for quality assurance and the foundation for further tracking down the supply chain.

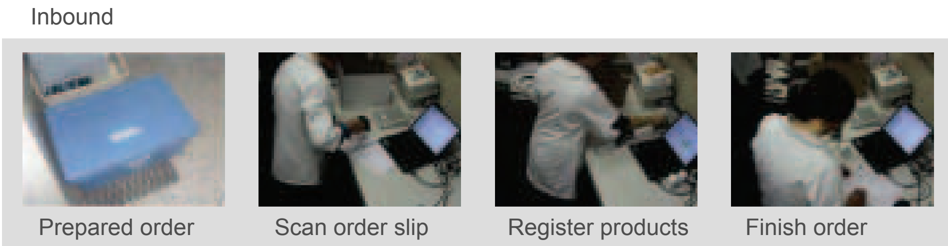


Figure 4.1-4: Inbound process in a pharmacy

The second example is a similar process in a pharmacy (Figure 4.1-4). Due to space restrictions, a small-range RFID reader is being used, which excludes false reads but requires more precise handling. The check provides immediate feedback on the authenticity of the goods and additional data, such as expiry dates. Inbound checking is preferable in this environment, since the pharmacist is interested in securing the internal processes at the pharmacy. An additional check at the point of sales is therefore not required. It is feared that such a check would erode the trust of customers in the pharmacy.

5 Summary

Technologies for automatic identification are the basis for a seamless interaction of goods handling processes with IT systems. The reading of an identifier from an object can trigger a process in the "virtual world", which in turn provides feedback to the physical world. This simple mechanism can be enriched with further attributes of a physical object and information about the status of the virtual representation of such an object. For example, an attribute can be provided by cryptographic authentication of an item, which establishes the presence of a secret key. Another example is the presence of a certain pattern on the item, which is established by a visual reading. Complementary to this information gathered from the physical world is the associated status information that is represented in the virtual world. By matching cryptographic data or the captured pattern data with its internal database, an IT-based service establishes the authenticity of an item.

Technically, seamless integration of the physical world and the virtual world is challenging, for example, due to limitations of wireless communications, or since implementing a secure authentication mechanism with computationally limited devices is hard. Moreover, there are practical issues when handling augmented objects, and no single identification technology is universally suitable for any kind of items. This poses difficulties for the implementation of these technologies in a business environment. Extensive testing and evaluations are usually required before a technology is chosen.

The SToP project has demonstrated how IT-based systems, Internet connectivity, and automatic identification can be used in business settings to establish a system for product authentication. Seamless integration in business processes can be achieved, thus making it possible to secure supply chains and minimize the availability of counterfeits. Ultimately, this should lead to a high detection rate of counterfeit articles and thus reduce illicit actors' financial incentives to engage in the counterfeit business altogether.

4.2 Challenges for Usage of Networked Devices Enabled Intelligence

CuteLoop Project

Harald Sundmaeker, Matthias Würthele, Sebastian Scholze

ATB Institut für Angewandte Systemtechnik Bremen GmbH, Bremen, Germany

Abstract: The availability of mobile and distributed networked devices dramatically increased over the past decade in both private and business environments. They are covering a wide spectrum from passive RFID tags up to personal computer like "all-in-one" devices. This current infrastructure of "digital things" is already connecting the internet to a certain scale, facilitating communication and access to information, including business as well as technology related challenges to realise business benefits. The CuteLoop project is researching a framework for using such networked devices for enabling an intelligent support of business processes within the integrated enterprise – realising a Networked Devices Enabled Intelligence. Due to complexity of interrelationships and number of actors in supply chains, specifically the decentralisation of business process coordination and the reduction of required information exchange is addressed. Innovative features were identified based on the requirements analysis in food chain and craftsmen business environments. Those features are seen as enablers to decentralise the intelligence from central entities in the overall ambience to networked devices, representing decentralised things in the integrated enterprise. Therefore, a contribution to an evolution from classical client-server architectures towards the Internet of Things is envisaged. A framework is developed, combining a multi-agent system for usage on networked devices and using both a service oriented and an event driven architecture for dynamic interaction of distributed actors. Furthermore, decentralised mechanisms for ensuring security and trust are addressed as well as an infrastructure for supporting basic interaction models of the integrated enterprise.

1 Introduction

The European market imports its supplies from all over the world as well as exports its products and services globally. The businesses are changing in fundamental ways – structurally, operationally and culturally in response to the imperatives of globalisation and new technologies [Palmisano06]. As one of the key enabling technologies, the Internet evolved into an "aorta" for communication and cooperation between integrated enterprises and individuals, representing a high performance infrastructure for global information exchange at low costs, allowing robust interconnection as well as ubiquitous connectivity.

In parallel, networked digital devices have evolved dramatically, providing their own computing capability and are even able to interconnect with an increasing number of other devices and services, representing the evolution towards an Internet of Things (IoT). High performance devices like the iPhone have become already multi-purpose tools. In contrary to previous process organisations, such devices are connected to the human actor or to real world objects and not to a specific workplace. Hence, communication between human actors with workflow supporting systems turn to be independent from a physical location. Nevertheless, the location awareness of human actors and things represents an essential requirement when aiming at the realisation of services that target to offer intelligent support in the ambience [Satoh04]. Therefore, technologies like Radio Frequency Identification (RFID) and Global Navigation Satellite Systems (GNSS) are required, presenting key enablers for assuring specifically the "self-awareness" of the devices or "things" within the ambience in terms of identity, position as well as time.

Mobile networked devices are adding new features to business processes with respect to the chronological workflow dimension. New process architectures are allowed, where different work steps need not to be executed synchronously or linearly anymore [Picot09]. A human actor can use its mobile device to carry out certain work steps like maintaining a technical installation, while implicitly documenting problems, improvement measures and schedules locally and remotely as soon as there is a stable and secure connection. Even the reordering of perishable food products can be immediately initiated while being executed asynchronously as well as automatically, only creating an exception in case of a problem.

The realisation and usage of a “Networked Devices Enabled Intelligence” (NDEI) seems to be within reach. Most business processes are already ubiquitously covered with an overwhelming amount of networked devices or could be easily equipped with e.g. RFID tags and positioning systems. However, especially in business environments incorporating many small and medium sized enterprises (SMEs) with quite limited innovation budgets and dynamically changing business relationships, the realisation of homogeneous infrastructures and a central governance of ICT is fairly unachievable. In addition, centralised approaches of especially large enterprises are under suspicion of jeopardising the SMEs’ competitiveness.

Therefore, the project CuteLoop has analysed two business environments with a significant amount of SME type actors to identify key business related challenges as well as to search for promising application cases for a Networked Devices Enabled Intelligence. Based on those results that are presented in the following sections 2 and 3, a framework of technological enablers is under development, that is outlined in section 4, presenting both the technological challenges addressed and framework features for implementing services, that are essentially required for realising a Networked Devices Enabled Intelligence.

2 Analysed Business Environments

The CuteLoop project has analysed two business environments, represented by supply chain scenarios from the food chain and craftsmen business. These environments were selected, assuming that especially the large amount of SMEs in those environments could benefit from using mobile networked devices.

2.1 Fruits and Vegetables Food Chain Environment

In the area of fruits and vegetables the food supply chain includes steps from the producer, over cooperatives, traders, distribution centres up to retailers and finally to consumers. Many business connections are on a temporary basis and are dynamically changing. The cooperation spans relations from classical trading up to spot market relationships. In each step of the chain, the actors are interacting with dynamically changing suppliers as well as customers. In general there are relatively small producers, medium traders and a mixture of a few very large retailers and micro enterprise type retailers. The communication is usually linked to the products, which are perishable goods having individual characteristics that can change even during the product’s route from producers to consumers. Wrong treatment during the supply processes can directly influence the product lifespan, while quality changes can even lead to a total loss of a delivery. Especially fresh fruits and vegetables have a relative short life-span from days to weeks. The products are transported in non-returnable packaging like cardboard boxes or returnable packaging like foldable crates. Currently, available returnable crates and containers are enabling their identification via barcode (1 & 2-D), a human readable number and RFID via one plate on the box while usage of such returnable crates is even cheaper than for cardboard boxes and at the same time avoids waste.

Figure 4.2-1:Identification ‘license plate’ RFID UHF for returnable packaging crates.

Information exchange between SMEs is fairly lacking ICT support, highly characterised by personal interaction. In recent years, a one step up and one step down traceability to customers and suppliers regarding the specific products is regulated by law. Nevertheless, this need not to be realised with ICT support nor requires the documentation of which products from which supplier (upstream) are forwarded to which subsequent customer (downstream).

2.2 Maintenance and Refurbishment Craftsmen Environment

The addressed environment from construction industry focuses on craftsmen offering maintenance and refurbishment services in small projects. Such projects are including one or more craftsmen enterprises of one specific or different trade. The works of different craftsmen represent one step in the supply chain, receiving their supplies from construction related suppliers, which are generally represented by medium to large enterprises. Each time when starting maintenance and refurbishment work, project based contracts of changing actors are defined, establishing a unique and ad-hoc group of craftsmen and the customer. A certain sequence of different craftsmen work steps need to be considered and harmonised, while the project is generally coordinated by a relatively inexperienced customer or specific work managers (e.g. architects, main contractors). Nevertheless, the customer's work specification is quite general, often not able to detail the current state of the existing building or installations. The craftsmen work represents a service type product, while also physical products are prefabricated and are resold to the customer. Long warranty and maintenance periods need to be assured, whereas there is often only very little documentation of work available. Subsequently, also future work and product replacement lacks information concerning the existing installations. Moreover, fairly no feedback can be given from craftsmen to customers or from industry to craftsmen in case of deficient products or in case of potential improvement measures. In addition, most customers are not prepared to handle craftsmen related information electronically.

2.3 Key Challenges within the Analysed Enterprise Environments

The workflows in both analysed enterprise environments are characterised by cross-organisational interaction, requiring the operation of highly dynamic and ad-hoc relationships. At the same time, only a very limited ICT support is available and especially facing the following key challenges when aiming at an improvement of the cross-organisational information exchange and planning & control of process execution:

- The supply chains are generally characterised by temporary supplier-customer relationships and are missing efficient and at the same time trusted models for information exchange.
- The business scenarios include a large number of SME type actors in open and distributed network topologies (i.e. chain, star & general collaborative network topologies) and are specifically lacking an integrated ICT support.
- A direct electronic access to product related data from previous or later steps in the SME type chains is generally not feasible, starting from 2nd tier supplier to customer relationships (i.e. beyond one step up/down).
- There is a dilemma of product related data exchange over several steps in a supply chain. The regular provision of certain information could jeopardise the competitiveness of chain members, leading to reluctance towards a standardised and open data exchange.
- SMEs do not often accept models for ICT based information exchange that are centralising system governance and storage of access details, while being driven by large enterprises in a business domain.
- Currently available ICT based information exchange models within SME environments rely on synchronous query-response behaviour, difficult to be applied for distributed and decoupled mobile work in terms of security, trust and costs.

The basic assumption is that by employing ICT based functionality, which is provided by one or several mobile networked devices it will become possible to decentralise the intelligence that need currently be kept within heterogeneous decoupled systems. This decentralisation is envisaged to facilitate interaction of actors and at the same time disburden the actors from non-added-value tasks within the workflow. The process related groupings of such ICT functionalities is considered as a Networked Devices Enabled Intelligence, representing a key enabler to cope with identified challenges.

2.4 Application Cases for a Networked Devices Enabled Intelligence

The project is based on the assumption that with higher levels of technology, like the vision of the Internet of Things, the level of organisational complexity and need for central initiatives can be decreased. This could even facilitate implementation and increase acceptance [CuteLoop09]. Based on the analysed enterprise environments and taking into account the key challenges several application cases for a networked devices enabled intelligence were elaborated. These application cases are considered as both drivers for elaborating new technology enabled business scenarios as well as test cases for validating practical applicability and readiness of IoT related technologies.

2.4.1 Self-Aware Product

The idea of the Self-aware product is to enable a product (or a "thing") to react on problems related to itself. If there is an irregular status of the product or someone detects that deficient or even dangerous products are being distributed within the chain and could have reached consumers, the product itself shall warn its environment about its status, avoiding harmful consequences. This need to consider how to generate such an awareness, requiring both knowledge concerning the "local product status" as well as remote knowledge that is located at previous owner(s) of the product.

2.4.2 Delivery by Product Characteristics

The food chain imposes critical constraints on product delivery. Especially fruits and vegetables are perishable products which could change quality related characteristics during delivery. Medium or longer-term storage of products is generally not possible. Therefore, the business environment depends on short delivery times between production, traders, retailers and consumers[42]. An early awareness concerning unexpected changes of product characteristics could initiate activity in order to change transportation conditions (i.e. avoiding waste) or to support planning initiatives in due time (e.g. re-order) that could assure timely supplies.

2.4.3 Proactive Tendering

Ordering products by the "receiving end of the production chain" (usually retailers) incorporates diverse information needs that are available at the producing source. Especially the product quality of food is extremely varying, customers need new methods to respond to appropriate offers. Based on a vision of pro-active products that will be authorised to support tendering mechanisms, reaction times and process efficiency will evolve towards a new dimension. In addition, as some of the product related information might not be available at the time of purchase (e.g. laboratory examinations), there is a need for a more efficient communication after sales, which spans several supply chain steps.

2.4.4 Health Book of the House

The idea of a 'health book of the house' is defined as a document describing the main technical and functional characteristics of the house/ building, reported by the time of completion of construction, reconstruction, extension or modification. As a basic idea, such a document could serve as reference for planning and preparing future maintenance work as well as facilitating quality assurance and warranty claims. Even when selling the house, the owner could easily hand over all information related to the house, the installations and equipments (e.g. HVAC systems, electricity installations, etc.). Furthermore, also information on e.g. maintenance history, refurbishments or renewal procedures could be successively included. The idea is to generate the health book based on a type of mesh network of available devices in the house also paving the way towards an intelligent house without the need for exhaustive infrastructure installations.

2.4.5 Customer Experience Improvement Programme

The Customer Experience Improvement Programme (CEIP) application case focuses on realisation of feedback mechanisms between products, installations and equipment at site with suppliers, manufacturers and service providers. Feedback would be provided in relation to installed, used, operated or maintained products & equipment in the house. Anonymous feedback could even be enriched with related problem experience in case of maintenance, repair or refurbishment. Data could be used as an ideal basis for life-cycle analysis and for generating a maintenance-related knowledge base. Finally, resulting knowledge could be used as guidelines for craftsmen's work as well as input for self-diagnosis features of an intelligent house.

3 Networked Devices Enabled Intelligence

3.1 Towards an Intelligent Support of Business Processes

The work was based on the assumption, that a decentralised and distributed usage of networked devices would enable the provision of ICT related features in the context of a certain situation in a business process or workflow, triggered by corresponding events. Physical objects or "things" like products, tools or vehicles can be combined with networked devices. Those things and devices can change their physical location, being owned by different actors as well as changing ownership according to the workflow.

---

[42] Product losses in food transportation due to temperature mismanagement and quality decay can reach up to 35% [Jedermann09].

A reaction of things could be triggered by a certain event, that could be e.g. a result in terms of a context change in the ambience or monitored by the networked device itself (e.g. temperature sensor, position information). Based on such an event and required knowledge in relation to the process, ambience and related actors, a device can react according to three types of basic behavioural patterns: (1) explicit response, (2) implicit response (i.e. internally registering/processing the event) or (3) deciding that no reaction is required. Such an ICT based functionality provided by one or several networked devices is considered as an intelligent feature, if it is envisaged to facilitate the interaction of human actors in the business process and at the same time disburden the human actors from executing non-added-value tasks within the workflow. Therefore, to enable a networked device to provide such a type of intelligent behaviour[43], a networked device need to be empowered to:

- autonomously initiate the execution of an ICT based functionality, representing a response to its environment in relation to an explicit or implicit input/ trigger received from the business process, the physical/virtual environment[44] or from a human actor and
- make decisions/ reasoning, based on available knowledge and predefined rules, while it needs to be assured, that also the rules can be dynamically changed[45].

Furthermore, when considering the elaboration of Networked Devices Enabled Intelligence from an over-all architectural view, the following basic challenges need to be addressed:

- distributed execution of ICT based functionalities in relation to the location of
  - things in the product flow and
  - networked devices in the workflow.
- decentralised control of operation and interaction, not requiring a central contact point,
- asynchronous operation due to the partly disconnected operation of a networked device.

In addition, the networked device – also in accordance to the IoT paradigm [EPoSS08][46] – needs to be enabled to autonomously execute certain functionalities, assuring trust, privacy and security mechanisms, while being able to establish a connectivity to the ambience.

In a classical scenario, the business system is focusing on the organisation, which is also overtaking the governance. By focusing ICT system support on processes, the assignment of the governance is blurring. It can be overtaken by the supplier as well as by the customer. Alternatively, also service providers that are highly specialised in operating such a process (e.g. transport service providers) can overtake the provision of the ICT system support. Nevertheless, the governance is still explicitly assigned to one actor. When using a networked devices support within a workflow, the governance is shifting to the owner of the networked device or thing. Therefore, when aiming at the realisation of an IoT based solution, the governance in relation to the networked device will change possibly several times in relation to the product life-cycle. On top of that, the owners of things will need to cope with the governance of diverse heterogeneous networked devices, each type including certain data fragments, features and interfaces. Therefore, when migrating technology towards that paradigm (see Figure 4.2-2), especially the handling of governance related principles have to be adapted towards the Things and Networked Devices.

[43] A logical grouping of functionalities that could be assigned to one or several tasks in the workflow are considered as a Net-worked Devices Enabled Intelligence.

[44] Environment is considered as the ambience in which a networked device is operated. Ambience is understood as both physical and contextual environment [Stokic06] in which networked devices & human operators are acting.

[45] Updating decision rules of a networked device in response to continuously changing processes, various interaction/ contractual agreements with different business partners, change of ownership of the related things and the location of the networked device.

[46] The authors of this paper are considering an NDEI as an IoT type solution, even if there is only a connection to a local area network, an intranet or only temporary connections to the Internet.

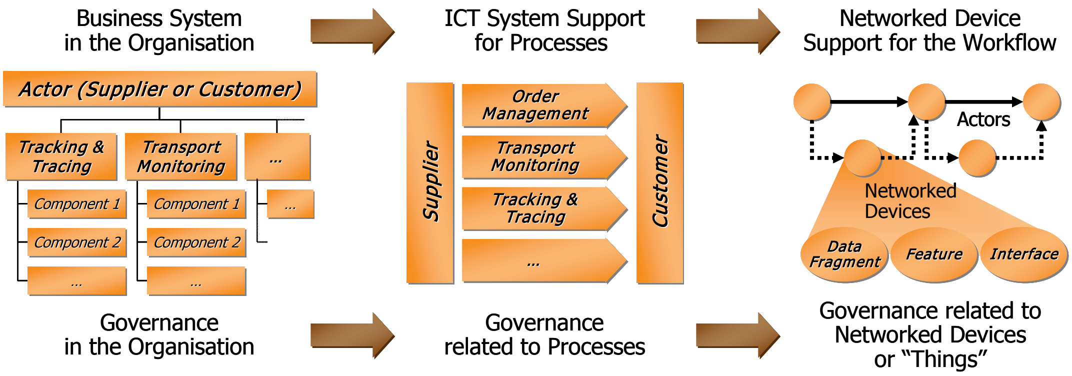


Figure 4.2-2: Transition from business systems in the organisation towards the usage of Networked Devices Enabled Intelligence.

3.2 Required Capabilities for realising a Networked Devices Enabled Intelligence

Application cases as listed above are specified from a business process and user perspective. The requirements were translated in more technical terms in so called capabilities to identify those features that are envisaged as key enablers for realising an intelligent workflow support:

- Event-based operation, to perform a functionality due to an event as opposed to a permanent operation.
- Self-localisation to be aware of the thing's own position, time and environment.
- Satellite-based communication for satellite footprint related multicast.
- Sensor integration to dynamically enhance the self-awareness in relation to the things.
- Self-diagnosis, to detect malfunctions, potential error causes or deficiencies.
- Detection of events originating in the ambience of a networked device and analysing the relevance of such an event as trigger for initiating subsequent reactions.
- Tracking encountered devices to be aware of things which have been in a certain proximity.
- Context and identity based access rights to data decentralised stored on a device.
- Device independent usage of decoupled user interfaces due to proximity.
- Granting call-back access to legacy systems, by adding access rights and related procedures to a networked device, before it changes ownership.
- Network knowledge retrieval built from distributed storage on multiple networked devices.

3.3 Application Cases versus Capabilities

The capabilities can be considered as a type of technology enablers for addressing challenges in relation to different application cases. Those capabilities are also envisaged to serve as a baseline when developing an IoT related solution, facilitating a translation of application case features (i.e. formulated from an end-user perspective) to a more technical perspective of a solution developer. Such a mapping of application case features and capabilities is presented in the following Table 4.2-1.

Table 4.2-1: Application Case Features in relation to addressed capabilities.

Addressed Capabilities	Self-Aware Product	Delivery by Prod. Char.	Proactive Tendering	Health Book	CEIP Programme
Event-based operation	X	X	X	X	X
Self-localisation	X	X	X	X	X
Satellite communication	X	X			
Sensor integration		X	X	X	
Self-diagnosis		X	X	X	
Detection/analysis of events	X	X			X
Tracking encountered devices	X			X	X
Context based access rights	X		X	X	X
Netw. Dev. based user interface	X			X	
Call-back access			X		X
Network knowledge retrieval				X	X

The application cases and the capabilities to be supported by envisaged results of the CuteLoop project, served as reference to elaborate the CuteLoop concept [CuteLoop09], outlining underlying technological components as further presented in the following sections.

4 The CuteLoop Framework

The CuteLoop research analysed the envisaged technological challenges when aiming at provision of envisaged capabilities as presented above. The following section 4.1 tries to provide an overview of some of the most important challenges from a networked devices perspective. Section 4.2 is further detailing envisaged technology related results (CuteLoop framework) that are realised in the project.

4.1 Technological Challenges Addressed

The project identified technology related challenges that need to be specifically overcome when aiming at the realisation of Networked Devices Enabled Intelligence. These were especially grouped according to the following aspects:

- ***Decoupling***: Commonly applied synchronous approaches for information exchange are hardly applicable in settings of ad-hoc interaction and dynamic open groups of partly unknown actors. Technical mechanisms need to provide features for decoupled interaction in terms of time and location.
- ***Heterogeneity***: IT solutions and especially mobile networked devices (innovation cycles of 1-2 years) are very heterogeneous in open and loosely coupled business relationships. Different operating systems are in place and hardware related functionalities vary especially in terms of connectivity, I/O-channels, performance, human operator related interfaces and system governance.
- ***Distribution and decentralisation***: Business relationships of independent actors in dynamic networks are based on a distributed processing and decentralised management of data. Within such infrastructures the client and server roles cannot be easily defined, while this need to be mixed with an architectural approach of peer-to-peer networks.
- ***Connectivity***: The use of various mobile networked devices for interaction leads to a high dependency of communication but due to the lack of a ubiquitous, scalable and affordable network for all potential "things", unavailability and intermittent connectivity is not the exception but the rule. Applications therefore need to change their communication approach of a "staying connected" to a "connect and transmit if possible" approach.
- ***Scalability and Costs***: Typically, when forwarding fresh food products transported in uniquely identified returnable packaging, 5.000 to 20.000 RFID tags (i.e. one truck) need to be read regularly,. This need to be realised in human operator's speed. The used installation reads UHF passive tags, while the writing of tags cannot be realised due to time constraints. Usage of active tags is currently beyond scope, especially due to hardware costs and maintenance as well as with respect to the related dilemma of communication capabilities versus[47] battery capacities.

[47] There would be a need to deploy different communication strategies due to the ambience and related workflow step which returnable packaging is located. To save energy an RFID tag would need to represent an active, semi-active or even semi-passive mode of operation to represent (a) hubs for communication management, (b) quiet tags only listening for events, (c) sleeping tags only able to be woken up for further operation.

- ***Trust***: Realisation of security and trust related services usually relies on a centralised infrastructure. In decentralised and distributed networks as described above, related infrastructure need to be individually provided by collaborating actors. Especially features for discovery and revocation of access rights need to be carefully managed to assure acceptance of the supply chain actors.

4.2 Features of the CuteLoop Framework

The technical approach to realise Networked Devices Enabled Intelligence was to integrate all the required basic functionalities covering process related interactions, the device communication as well as the security and trust features in a framework. This framework has to be usable on diverse heterogeneous devices, supporting various communication networks. It also needs to serve as a type of template when implementing the required capabilities and integrating software services, legacy systems and existing hardware like sensors, GPS or RFID readers. The following Figure 4.2-3 presents a basic architectural structure for realising Networked Devices Enabled Intelligence.

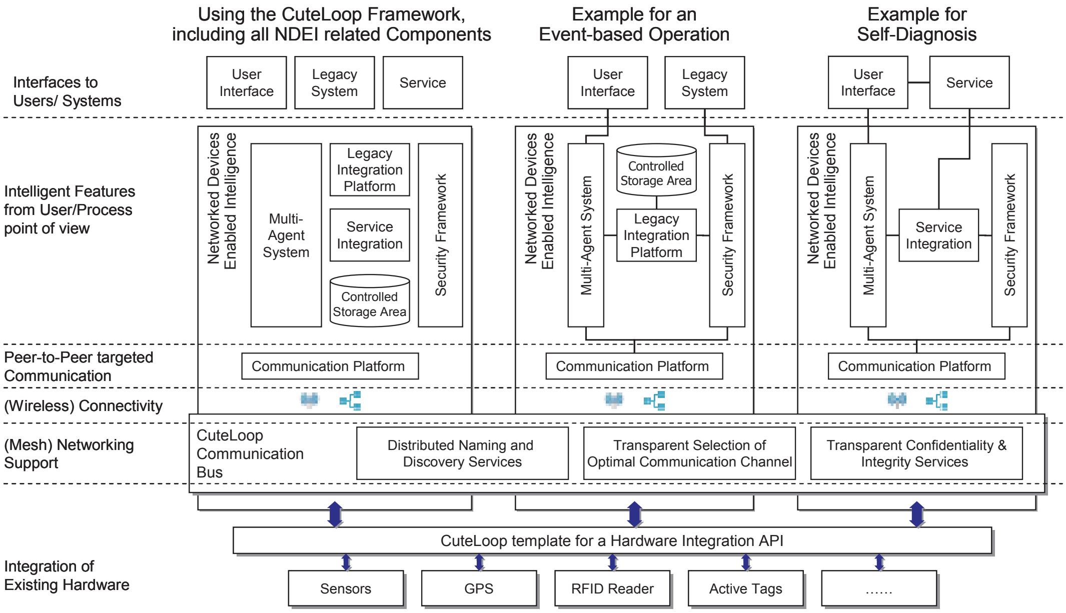


Figure 4.2-3: Basic architectural structure for realising a Networked Devices Enabled Intelligence, based on usage of the CuteLoop framework.

For a particular application like the indicated examples (event-based operation & self-diagnosis), the CuteLoop framework based platform needs to be extensible and highly customisable. From an overall software design and an interaction pattern point of view, the NDEI services[48], as presented in the following Table 4.2-2, are considered as the key elements of the framework to support solution design of application cases in real world settings.

[48] Service as a function that is well defined, self-contained and does not depend on the context or state of other services [Barry02], while from the project and a more technical point of view, such services could also include functionality provided by software agents, which would be specifically characterised by being adaptable (e.g. to different platforms), mobile (i.e. able to change their physical location) and autonomous/ ruggedness (i.e. being able to perform their tasks without direct intervention of humans) [Murch98, Paolucci05].

Table 4.2-2: Services for realising a Networked Devices Enabled Intelligence.

NDEI-Service	Key Capabilities	Communication	Autonomy	Security
Information Brokerage	Context based access rights Call-back access	Assuring transparent access between services on application layer.	Decoupled generation of access rights, routing details and content encapsulation	Multilevel authorisation, intersecting domains and decentralised access rights revocation
Awareness	Self-diagnosis Sensor integration Tracking encountered devices	Coordination of monitoring via a network of master nodes	Distributed and decoupled event stream processing and monitoring	Actor & device authentication and authorisation; linked local name spaces
Reactivity	Event-based operation Detection/ analysis of events	Virtualisation of devices to actively represent passive hardware behaviour	Coordinating running components & generation of functionality; considering functionality routing	Certificate based authentication and verification of remote and mobile agents
Situational Interaction	Networked Devices based user interface Network knowledge retrieval	Managing diversity of network nodes using characteristics and functionalities of available peers	Autonomous selection of appropriate/ optimal peers to fulfil context related requirements	Assuring integrity and confidentiality of exchanged data and communication
Ubiquitous Notification	Satellite communication Self-localisation	Satellite multicast and mesh based transparent communication channels	Identification of communication requirements.	Decentralised authentication

From a software engineering perspective the application layer related functionality for assuring an autonomous behaviour within decentralised and decoupled infrastructures, will mainly be based on a multi-agent platform. Instances of such platforms deployed on distributed devices will be able to transparently connect via the communication platform, that covers the transport layer functionality, providing so-called binding components. Finally security framework as integral part will enable the separation of information and communication amongst NDEI devices into protected domains within the supply chain.

Envisaged functionality will be provided by both software agents as well as software services. Therefore, the runtime environment needs also support the combination of both technologies. While an agent and agent platform can quite easily cope with the characteristics of a software service, a service execution environment is lacking the ability to coordinate agent related functionality. Therefore, it is still being researched how to realise a type of a service integration framework that will mediate between the agent and the service world.

A concept for a controlled storage area (CSA) is applied for facilitating the distributed and decentralised data-exchange between systems. Actors can put their own data in a CSA which is also available for access by other agents. In addition, other agents can be permitted to store data in the CSA as well. This approach enables data-exchange between actors without directly exposing their existing systems.

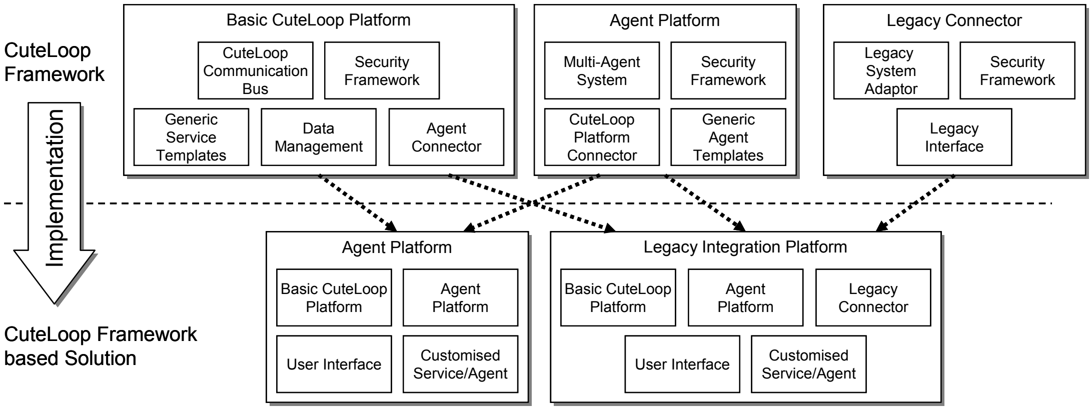


Figure 4.2-4: Reference structure for implementation, using the Framework for realisation of CuteLoop Framework based solutions.

Finally, the CuteLoop framework is OS platform independent, hence applicable on different types of networked devices. While analysis of current devices from active RFID type platforms over mini-PC to multi-purpose devices like smartphones and netbooks indicates that at least a certain JAVA support is required. Low performance devices are also envisaged to be integrated, when developing an overall solution. However, an initial architecture already needs to be driven by the process related requirements to find an appropriate distribution of higher level functionality in relation to networked devices. Such active devices operating an agent platform specifically include a management agent that will coordinate an intelligent workflow support. However, main elements of the CuteLoop Framework are a basic platform, an agent platform and a legacy connector, as presented in Figure 4.2-4.

Based on specific requirements of a defined scenario, appropriate elements with their entities would be composed to a specific CuteLoop solution. Such a solution would be highly customised and based on real business processes with their defined actors and existing applications.

5 Conclusions

The CuteLoop project is addressing two business environments that are characterised by a large amount of SMEs that are collaborating in open chains with dynamically changing relations between enterprises. A significant amount of human operators are working in decentralised and distributed settings, lacking an integrated ICT support. The related business challenges were analysed as well as innovation aspects of using Networked Devices Enabled Intelligence. Several application cases of NDEI were elaborated. Required technology related capabilities were grouped in a framework, facilitating the realisation of ICT solutions that provide an intelligent and human centric support for the integrated enterprise.

To assure an impact on the business environment, attention was paid to neither a specific hardware device nor on a certain operating system, but on elaborating a framework of key features that are specifically required when aiming to develop certain capabilities and services that are required for implementing Networked Devices Enabled Intelligence. Hence it is targeted at the reuse of available/state-of-the-art infrastructures and devices. In the ongoing work of the project, software components are under development that will be tested and demonstrated in business environments. Grouped in accordance to a reference structure of capabilities and business process related interaction models, also methodological guidelines will be provided for using the CuteLoop framework in developing solutions in relation to innovative application cases. These results are envisaged to directly address identified challenges, while from an SME perspective specifically addressing aspects related to trust, scalability and costs.

6 Acknowledgement

The presented work is carried out in the scope of the CuteLoop project (Customer in the Loop: Using Networked Devices Enabled Intelligence for Proactive Customers Integration as Drivers of Integrated Enterprise – http://www.cuteloop.eu). The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 216420. It is carried out by an international consortium from France, Germany, Luxembourg, Portugal, The Netherlands and UK.

7 References

[Barry02] Barry, Douglas; Getting Ready for a Service-Oriented Enterprise Architecture. Distributed Enterprise Architecture Advisory Service, Executive Report, Vol. 5, No.8, 2002.

[CuteLoop09] CuteLoop Project; CuteLoop Concept - Public Project Report. Download via the Project Website: http://www.cuteloop.eu

[EPoSS08] INFSO D.4; INFSO G.2; RFID working group of the European Technology Platform on Smart Systems Integration; Internet of Things in 2020 – A Roadmap for the Future. Report based on a expert workshop on February, 11th-12th 2008 in Brussels. Published on September, 5th 2008.

[Jedermann09] Jedermann, R.; Lang, W.: The minimum number of sensors - Interpolation of spatial temperature profiles. In: Rödig, U.; Sreenan, C.J. (eds.): Wireless Sensor Networks, 6th European Conference, EWSN 2009. Springer, Berlin/Heidelberg, 2009, pp. 232-246.

[Kirchhoff04] Kirchhoff, Uwe; Sundmaeker, Harald; San Martín, Fernando; Wall, Brian; Campos, José; Xeromerites, Stathes; Terziovski, Mile; How to Speed-up the IMSS Related Innovation in Manufacturing SMEs. International IMS Forum 2004; May 17.-19. 2004; Villa Erba - Cernobbio - Lake Como (Italy).

[Murch98] Murch, Richard; Johnson, Tony; Intelligent Software Agents. Prentice Hall; London, 1998.

[Palmisano06] Palmisano, Samuel J.; The Globally Integrated Enterprise. Foreign Affairs, Volume 85 No. 3, pp. 127-136; May/June 2006.

[Paolucci05] Paolucci, Massimo; Sacile, Roberto; Agent-Based Manufacturing and Control Systems – New Agile Manufacturing Solutions for Achieving Peak Performance. CRC Press, Boca Raton, 2005.

[Picot09] Picot, Arnold; Schmid, Martin S.; Mobilisierung von Wertschöpfungsprozessen durch innovative und sichere Informationstechnologie. Study in the scope of the SimoBIT programme of the German Ministry of Economics. Institut für Information, Organisation und Management; Munich, 2009.

[Satoh04] Satoh, Ichiro; Software Agents for Ambient Intelligence. Proceedings of SMC 2004 - IEEE International Conference on Systems, Man, and Cybernetics. pp. 1147-1152. The Hague, The Netherlands.

[Stokic06] Stokic, Dragan; Kirchhoff, Uwe; Sundmaeker, Harald; Ambient Intelligence in Manufacturing Industry: Control System Point Of View. The Eighth IASTED International Conference on CONTROL AND APPLICATIONS CA 2006; pp. 63-68, Montreal, Quebec, Canada, 2006.

[Sundmaeker08] Sundmaeker, Harald; Proactive Customers Integration as Drivers of an Integrated Food Chain. 110th EAAE Seminar 'System Dynamics and Innovation in Food Networks', 18.-22.02.2008. pp. 485-495 Innsbruck-Igls, Austria.

4.3 NFC Technology and its Application Scenarios in a Future IoT

STOLPAN Project

A. Vilmos / C.M. Medaglia, A. Moroni

SafePay / "La Sapienza" University of Rome (CATTID)

Abstract: Over the last few years, the growing availability of automatic identification technologies such as Radio Frequency Identification (RFID) has allowed users to interact with smart objects (i.e. objects connected to the Internet) in the real world, realizing the so-called Internet of Things (IoT) paradigm. An example of this scenario is the retrieval of additional product information in a department store simply by touching a tagged object with a smart device.

Among RFID technologies, Near Field Communication (NFC) is the most customer-oriented one, as it can be looked at as the integration of an RFID HF reader into a mobile phone. As mobile phones are the most popular personal devices worldwide, extending them with an RFID reader allows more and more people to interact with smart objects and the environment.

One of the main problems in creating a network of smart objects that talk to each other and with the users, is the lack of application level standardization and interoperability: even if NFC technology was standardized by ISO/IEC in 2004 (ISO/IEC 18092:2004), there are still significant differences between NFC implementations (devices, operating systems, etc.) that have to be taken into account.

The StoLPaN (Store Logistics and Payments with NFC) consortium has worked on creating a single platform multi application environment where many kind of NFC based services can coexist and interoperate irrespective of the handset or network specifics thus creating a homogenous user experience for the customers and a transparent technical environment for the service providers.

Moreover, the StoLPaN team has been working on the solution to introduce personalized NFC services into the EPC (Electronic Product Code) based smart shopping environment, by specifying and implementing a complete shopping and payment process based on contactless technology.

The NFC technology will greatly contribute to the future development of IoT. It will provide the necessary tool for anyone to be connected, to be able to communicate with any type of smart objects, people and services. However there are still numerous challenges that need to be overcome before this vision can be realized. Further standardization to ensure openness and interoperability, business and logistical models to provide wide access to services are needed and the elaboration of some legal issues are top short term priorities.

1 IoT and NFC

The term "Internet of Things" was coined by the researchers of the Auto-ID Lab at MIT of Boston in 1999, to describe a network of objects connected to the Internet by means of the RFID technology. Even if the first definition of IoT given by Auto-ID lab was related to RFID, actually the IoT is linked not only to Radio Frequency Identification, but also to other technology solutions: sensor networks, TCP/IP, mobile technologies, and in general to all the automatic identification technologies which allow to identify objects, to collect and process information about them and to link the physical world to the virtual one.

In the CERP-IoT Research Roadmap, NFC is explicitly addressed as one the potential IoT domains:

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

Each one of the technologies mentioned in this definition is suitable for a particular context of use, within a specific scenario, but undoubtedly NFC is the most user-friendly among all of them. The RFID-based interaction of NFC is familiar also for "non-technological users", as interaction with an object by means of NFC technology replicates the act of "touching" something to produce the correspondent action in the same way that people press a button to move the elevator toward a given floor or touch a switch to light a room [1, 2].

NFC technology is not only convenient to use by anyone, which makes it a perfect carrier of the IoT concept, but it also has very versatile usage potential which may bring IoT to diverse domains of daily life.

Mobile phones equipped with NFC technology (a mobile handset coupled with an RFID HF reader and preferably also with a secure storage unit – secure chip-) can soon establish the largest RFID reader architecture of the world including hundreds of millions of mobile handsets.

Mobile NFC also has the capability to turn the mobile handsets into various types of smart objects. In this operating mode the handsets and the information carried by them can be read by external interrogators, reader devices using legacy or newly established architectures, just as if they were any types of contactless cards, or other type of smart objects.

Another interesting feature of NFC mobile phones, which can open interesting opportunities related to the IoT paradigm, is that they can also communicate with each other, reading, storing and sharing information in proximity (NFC) or remotely via an over-the-air connection (GSM, UMTS, WiFi). The real power of the technology lies in the combination of the two – remote and proximity -communication channels.

2 NFC technology

Near Field Communication is one of the newest short-range wireless technologies.

From technical point of view, NFC operates within the unlicensed Radio Frequency band of 13.56 MHz; the typical operating distance is up to 20 cm (in special circumstances could be longer), but the actual communication distance strongly depends from the antenna diameter: as integrated in a mobile phone, the antenna is typically very small, so the communication distance is about 3 to 5 cm.

The Near Field Communication Interface and Protocol-1 (NFCIP-1) [3] was adopted by the European association for standardizing information and communication systems as ECMA-340, published by ETSI (ETSI TS 102 190) [4] in March 2003 and then approved as an ISO/IEC standard in April 2004 (ISO/IEC 18092:2004). The NFCIP-1 specifies, in particular, "modulation schemes, codings, transfer speeds, and frame format of the RF interface, as well as initialization schemes and conditions required for data collision control during initialization. Furthermore, this International Standard defines a transport protocol including protocol activation and data exchange methods"[5].

As abovementioned, an NFC device can operate in reader, card emulation, or Peer-to-Peer mode: the Near Field Communication Interface and Protocol-2 (NFCIP-2) (ISO/IEC 21481:2005 and ECMA 352) specifies the detection and selection mechanism between these communication modes [5].

When the NFC device operates in card emulation mode, it behaves as an ISO/IEC 14443 smart card, so it is compatible with the contactless infrastructure already on the field, as well as with Mifare® and FeliCa™ smart cards.

Besides ISO/IEC, ETSI and ECMA, there are a number of standard bodies and industry organizations - the NFC Forum, Global Platform, Open Mobile Alliance, etc. - that deal with NFC technology. Nevertheless, all these organizations are dealing with basic technology issues or industry related matters, while application distribution and management, application interoperability, multi application environment and related challenges are still not adequately taken into account.

The StoLPaN (Store Logistics and Payment with NFC) consortium indentified this need and was concentrating on issues contributing to multi-application management and the establishment of multi-service NFC environments.

3 Services and use-cases

The short communication distance of NFC and its data collision control, provide a solid underlying security framework for the operation which makes NFC the perfect choice of technology for sensitive services and use-cases.

NFC can be used to enable a wide range of services.

Initially payment and ticketing were the darlings of the industry. These are services with many repeat users, established operating framework and acceptance architecture as well as solid revenue streams and charging models. After a first set of pilot projects however, the complexity of these use-cases were identified: the lengthy preparation for commercial implementation, the involvement of a number of actors with different and sometimes conflicting interests. Payment is nowadays seen as the last step for an NFC-based implementation.

Conversely, one of the most interesting short-term scenarios is the use of NFC phones for interacting with smart objects as, for example, smart posters for mobile proximity marketing, mobile tourism or mobile loyalty programs, as well as with tagged products in a retail environment. By touching a product with an NFC device, the user can retrieve additional information, such as its origins and authenticity, linking a physical object with its virtual identity. Another interesting trend in NFC based services is related to mobile social networking, using the mobile phone as an access point to the virtual world of social network. There is a number of interesting NFC based mobile social networking applications, where the mobile phone is respectively used as a friend connection platform (Hot in the City by the University of Oulu)[6], a location based social ticker (Friendticker by Servtag) [7] or a way to ease the collection of location information (NFCSocial by Atos Worldline) [8].

NFC can also support a lot more complex service scenarios which may transform people's habit, may substantially improve quality of life. With the combination of smart objects and NFC-enabled mobile phones mobile health monitoring, smart travel planner and smart retail services including payment can be provided, just to mention a few examples.

In case of mobile heath monitoring small wearable sensors capture the patient's health information which is collected through the proximity NFC interface of the mobile handset, then data is pre-processed by the device and forwarded to a clinical monitoring centre. The course of communication and interaction can be reversed too, and using the handset's mobile and NFC communication capability the operation of the sensors can be adjusted from the remote monitoring centre.

The mobile health monitoring scenario, the combination of mobile NFC technology and smart sensor networks can be implemented in more complex scenarios in accord with the Ambient Assisted Living (AAL) concept and help people to improve the quality of their lives. It can provide the flexible, remote monitoring of the preferred environment of the older people, or the people in need.

Another potential application of the mobile NFC technology is the smart travel planner that can personalize the overall travel experience and can take out many of the unnecessary nuisances from one's trip. By using the internet, contactless technology and mobile handset the following futuristic concept becomes reality. The person books a hotel on the internet and receives the room key over the air onto his/her mobile handset. The key is stored securely in the secure storage part of the handset just like as if it were a plastic key card. The tourist also wishes to travel in the city by using public transportation. If the trip is to cities, where contactless transport infrastructure is available, the tickets can also be sent over the air to the tourist's mobile phone. These tickets are also stored in the secure storage part of the mobile phone. Similarly museum and event cards can be ordered and received. Upon arrival to the hotel the tourist can proceed directly to the room, avoiding the sometimes lengthy check in procedure and simply enter the room by touching the mobile handset to the lock. Similarly when the tourist enters the metro, the mobile handset is touched to the entrance gate and the gate opens just as if normal tickets were presented.

Besides pre-arranging part of the trip the NFC enabled mobile handset can also assist in service discovery. The handset can read so called "smart posters" and receive direct information – like provisioning of e-coupons – or the smart poster will initiate the phone to launch mobile data communication with remote servers that provide the information needed. In case of a bus station this can be the schedule of the next bus, or the best connection to a selected destination, whereas in case of an exhibition this interaction can result in the download of an entry ticket. To make the experience more complex, contactless payment can also be integrated into the NFC service line.

The smart retail concept holds similar convenience benefits for the customers and also provides increased efficiency for the store operators.

By using NFC enabled mobile handsets customers can read the smart tags of the merchandizes and retrieve product information from a remote server or check the product pedigree. By touching the phone to certain advertisements customers can receive smart coupons into their phones which can be redeemed at check out. (With this solution spam can be avoided and customers really only get the coupons and promotions they need.) The greatest benefit however can be realized if the shopping environment is modernized as well and smart shopping carts are used. In this case the customer's mobile handset can communicate with the shopping cart, can query information, but most importantly can perform payment without the need to line up in front of a cashier.

4 StoLPaN project results

The StoLPaN consortium has published two White Papers presenting proposals for the post issuance procedures and for multi-application management that were distributed in wide industry circles (NFC Forum, ETSI, GlobalPlatform, etc.). In fact, the remote, post issuance and application management procedures have been identified as the key issues to be addressed in order to offer users a variety of NFC applications on the same device and so to build a real ecosystem. Indeed, even if the users involved in NFC trials declared to appreciate the ease-of-use and the convenience of the NFC technology, they have been able to test only one or two applications per time, without the possibility to remove or insert any new or un-used applications. To have just one or two NFC services hard coded into the mobile requires a simple usage and a simple loading, but it does not have real benefits as it is just a new form factor compared to card based interaction. Moreover, it is quite expensive for the players involved, as each service provider has to build the application starting from zero. From the user's point-of-view, to have separated applications for each service (payment, transportation, access-control) is hostile, as they have to interact with different menus, causing a fragmented user-experience.

In order to provide a fully functional, economic and convenient service, which exploits the real capabilities of the NFC technology (i.e. to use the same device for emulating different types of cards in a dynamic environment) a set of roles have been considered. Besides the Card Issuer, OTA (Over the Air service) provider and the application issuer, the role of multiple TSMs (Trusted Service Manager) was identified. The TSM will be in charge to provide the technology and service support in order to optimize the efforts and to give the user a homogeneous user-experience. Although the involvement of a TSM in the service distribution process has already been discussed in the industry, but to have more of them participating simultaneously in the service provisioning workflow and the need to establish interoperation between these actors is a completely new approach. This scenario can open up the NFC service environment and make it suitable for multi-application, multi-service provider operation. This concept was introduced and described in the 1st StoLPaN White Paper. [9]

To have multiple services side by side stored in the user's handset a transparent service environment needs to be established. The project called it the StoLPaN "Host" which lets users operate multiple services according to the same principles providing a homogenous user experience. The Host also simplifies the service development process as the service providers only need to develop one single version of the application and the Host ensures that they will run across diverse handset types. Actually the Host is to establish a single-platform, multi-application service environment. The design still allows adequate room for differentiation between the service providers, as branding is still possible and customers are still related exclusively to the individual service issuers (banks, transportation companies, etc.). This concept is discussed in the 2nd StoLPaN White Paper. [10] A proof of concept prototype of the Host application was also implemented and demonstrated.

The project described and implemented an end-to-end contactless shopping and payment scenario, using smart tags, smart shopping devices and the users' NFC enabled mobile handset.

In this environment a smart shopping cart plays the central role. This cart is communicating with the customer's handset using NFC and is also linked remotely to the store back office system using WIFI. The cart has proximity antennas to read smart tags, and a display to communicate with the customer. When customers enter the store, they can log-in into the loyalty system of the store which stores a shopping list for them that they may have prepared at home, using the store's website. The cart's screen also provides orientation about the location of the desired products. When products are placed into the cart the display provides information about their price and promotion related to them. If more detailed information is required by the customers they can access the store's database using the cart's interface. During the course of shopping customers may collect with their NFC handsets e-coupons from smart posters which they can redeem at payment. When the shopping is completed customers may proceed with the payment. The great novelty of the StoLPaN solution is that also payment can be performed between the customer's handset and the smart shopping cart. Customers do not need to go to a cashier they simply select the payment function on the display of the cart. If they pay with bankcard or loyalty points the handset is touched to the cart and the necessary payment credentials are transferred securely to the store back office, where the usual payment authorisation process is performed. During the payment process the collected coupons can also be redeemed and by transferring them from the mobile handset to the cart the related benefits/discount will be deducted from the invoice. When payment is completed customers may proceed to check-out, without the need to line up and wait in front-of any cashier or counter. The smart shopping process is also integrated to the security environment of the store. When leaving the retail area customers need to pass through a security gate, which remotely reads the products in the cart, and compares the cart content with the related payment information.

Such retail operations do not only make the shopping and payment process more user-friendly and convenient but also substantially increase the efficiency of the retail operation.

5 Conclusion and Future Work

The StoLPaN project had two major focuses:

- multi-application operation in the mobile handset
- elaboration of the smart retail purchase and payment process.

The targets are/were met. The project:

- has published, and widely circulated its underlying theory in two White Papers;
- has built a proof of concept prototype of the multi-application mobile Host;
- has elaborated the retail scenario and the concept and solutions were not only tested in the Libri bookstore as planned, but were also demonstrated to a much wider audience at the Cartes 2010.

During the work however, it was identified that there are still important issues to be solved before the above described complex NFC use-cases can be introduced an masse, can be commercialized.

In all present pilots the NFC environment, the available services – usually only one at a time – are static, customers do not have the opportunity to add or change services, to freely configure their NFC service portfolio. The service partners knew each other, the customers had to pre-register, the applications were loaded and stored in advance into the handsets, every technical and service detail was pre-arranged and pre-organized by the trial participants. All known solutions were/are proprietary there is no interoperation capability between the various locations. All is static, monolithic and artificial.

The real, the commercial operation is different.

People do not want a single contactless service, but many, and their service needs are constantly changing so their service portfolio will need dynamic reconfiguration. Customers are dealing with many service providers who are often providing similar, or identical, competing or complementary services. There is not just one mobile operator involved in NFC service provisioning, but many. Various services have diverse security and legal requirements and widely different business models.

All these actors, their interests, requirements and operating specifics need to be integrated into an operating, technical and business framework to allow multiple contactless services to coexist in the users' mobile handset, in order to provide satisfactory user experience to the customers as well as the potential of efficient service delivery for the service providers.

A full-fledged NFC service environment can only be realized based on high level interoperability, thus ensuring that a large number of independent, ad hoc parties can seamlessly communicate and interact with each other based on known and generally accepted technical specifications, operating rules, service guidelines and standards.

This openness and interoperability needs to be established in order turn NFC from a promising technology to a fundamental component of the Internet of Things.

6 Acknowledgment

The authors would like to thank their partners in the IST-FP6 project StoLPaN (Store Logistic and Payment with NFC).

7 References

[1] Levialdi, S., Medaglia C.M., Moroni A., Sposato, S., "NFCTicketing: a prototyping and usability test of an NFC-based virtual ticketing application", in Proceedings of First NFC IEEE Workshop, Hagenberg, Austria, February 2009.

[2] Biader Ceipidor, U., Medaglia C.M., Moroni A., Sposato S., "Design, Prototyping and Evaluation of SIMpliCity: an NFC system for the mobility of citizens", in Proceedings of CHI 2009, Rome, Italy, 17-19 June 2009.

[3] ISO/IEC 18092 (ECMA-340): Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1). First Edition, 2004-04-01.

[4] ETSI TS 102 190 V1.1.1: Near Field Communication (NFC) IP-1; Interface and Protocol (NFCIP-1) 2003-03, URL: http://www.etsi.org.

[5] ISO/IEC 21481: Information technology Telecommunications and information exchange between systems Near Field Communication Interface and Protocol -2 (NFCIP-2). January 2005.

[6] http://hic.vtt.fi/.

[7] http://www.servtag.com/en/losungen/friendticker/.

[8] Fressancourt A., Hérault C., Ptak E., "NFCSocial: Social Networking in Mobility through IMS and NFC," in Proceedings of First NFC IEEE Workshop, Hagenberg, Austria, February 2009.

[9] StoLPaN consortium, Dynamic Management of multi-application secure elements, Public White-paper, available at www.stolpan.com

[10] StoLPaN consortium, Dynamic NFC wallet, available at www.stolpan.com

4.4 RFID-enabled Tracking and Tracing in the Supply Chain Lessons Learnt from the SMART and TRASER projects

Cleopatra Bardaki, Katerina Pramatari / Elisabeth Ilie-Zudor, Zsolt Kemény

ELTRUN Research Lab, Department of Management Science and Technology Athens University of Economics and Business / Computer and Automation Research Institute, Hungarian Academy of Sciences

Abstract: The paper summarizes the results of two 6FP-funded projects aiming to establish tracking and tracing services relying on RFID. In the lifespan of the SMART project (IST-2005, FP6), two RFID-enabled services, supporting dynamic-pricing of fresh products and management of promotion events, have been deployed on a service-oriented architecture that utilizes RFID technology, data stream management systems and web services. The two services have been field-tested in three retail stores in Greece, Ireland, and Cyprus. The valuable lessons learnt, concerning RFID readability challenges, consumer privacy, customers and store staff health concerns, investment cost, and so on, are reported to provide guidance to future developers of RFID-integrated supply chain services as well as to set an agenda for academic research. The TraSer project pursued the introduction of track-and-trace services especially in the lower end of the application spectrum, i.e., small-scale users as SMEs and other smaller organizations. TraSer provided a free, open-source solution platform using web services for communication and a variety of possible physical ID carriers (not limited to RFID) for unique identification. An architectural overview gives insight into design preferences and choices determining the framework architecture, while a report on relevant cases selected from a wider range of application pilots outlines the experience gathered with deployment on different scales.

1 Introduction

Radio-frequency identification (RFID) is a key technology today that drives developments in the area of the Internet of Things. RFID is a wireless communication technology that uses radio-frequency waves to transfer identifying information between tagged objects and readers without requiring line of sight, providing a means of automatic identification (Sheng et al. 2008).

Although some of the underlying technologies for RFID have been around for more than half a century and both technically feasible and practically usable solutions have appeared already more than a decade ago, only recently have supply chain partners started to explore its potential to support core business processes. This shift of attention should be primarily attributed to the decrease of acquisition costs for the technology parts (readers, tags, printers), the availability of related services and functionalities, as well as the emergence of proof-of-concept application prototypes by large retailers and suppliers. Currently, RFID is emerging as an important technology for revolutionizing a wide range of applications, including supply-chain management, retail sales, anti-counterfeiting, and healthcare (Nath et al. 2006).

The advent of RFID, as an enabling Auto-ID technology, generated significant interest to the retail sector mainly because of its capability to streamline core supply chain management operations. As a result, over the past few years several research projects emerged discussing different flavours of RFID-augmented applications in such supply chain management areas as inventory management (Fleisch et al. 2005) and customer relationship management in the form of 'smart' personal shopping assistants capable of guiding and assisting consumers throughout their shopping trip within the physical store (Kourouthanassis et al. 2003).

Nevertheless, the majority of existing literature in RFID systems is primarily at a prototype or simulation stage. In effect, very few publications discuss the actual deployment effects of RFID technology in the field. Notable exceptions are the works of Ngai et al. (2007) and Delen et al. (2007). In a commercial setting, the most renowned example is the Metro Future Store, located in Germany, which comprises an aggregated test-case laboratory showcasing the potential of Auto-ID technologies in the retail setting.

In this context, the SMART project (IST-20005, FP6) proposes RFID-enabled supply chain services in the retail industry, building on the capabilities provided by RFID technology, data stream management systems and web service orchestration. The retail services that have been selected, namely dynamic-pricing and promotions management have been deployed in three commercial sites at different European countries with participating user companies being European grocery retailers and suppliers from the fast-moving consumer goods sector. As a result, valuable lessons have been learnt for the deployment of RFID applications spanning the whole spectrum, from RFID readability issues, integration with the legacy systems, cost, web-service synchronization, consumer privacy to name but a few areas where experience was gained. The acquired knowledge is shared through this paper to provide guidance to future developers of RFID-enabled supply chain services as well as to set an agenda for academic research.

The TraSer project (IST-033512, FP6) already bears its focus in its acronym, being assembled from the words tracking and services. As opposed to concentrating on the sole use of RFID itself, the project pursued the provision of a general service background for tracking and tracing of uniquely identified entities. The targeted user range were small-scale users such as SMEs (small and medium-sized enterprises), therefore, affordability, lean infrastructural demands, cross-company transparency and easy adaptation to legacy IT components and external protocols/requirements were the key preferences to meet. Central output of the project was a free, open-source track-and-trace solution framework relying on web services for communication and XML/XQuery for handling the data of the items tracked. Largely independent of the physical ID carrier (and thus also transparently allowing other means of unique identification than RFID), the platform has been tested in a wide range of applications, from tracking of physical items to distributed version control of electronic design documents, both in closed-circuit asset management and supply chains. The TraSer solution platform is listed on Sourceforge, and can be also downloaded from the project website http://www.traser-project.eu.

2 Lessons Learnt from the SMART project

2.1 RFID-enabled Services over the SMART Architecture Framework

In the course of the SMART project (IST-20005, FP6) with participating user companies being European grocery retailers and suppliers from the fast-moving consumer goods sector, a layered, distributed, service-oriented architecture framework is proposed to support RFID-enabled supply chain services in the retail industry. The SMART architecture utilizes the automatic, unique identification capabilities of RFID technology; data stream management systems (Chatziantoniou et al. 2005) and web service orchestration (Muehlen et al. 2005) to enable information sharing and collaboration among retail supply chain partners.

Figure 4.4-1 illustrates a high-level logical view of the SMART architecture framework (Bardaki & Kourouthanassis 2009). It is a distributed architecture framework, where the application layer runs on the system of each collaborating partner and web services implement the interface between the different partners' systems using SOAP requests and responses. The data layer is implemented by both a relational database management system (Object Instance Information Service) and a data stream management system (DSMS) providing the application layer with continuous real time reports after processing unique product identification data streams generated from the RFID infrastructure. The orchestration engine coordinates the exchange of messages between the partners' web services following the logic of the specific supply chain application services. The service repository provides an interface for the orchestration engine to execute queries and discover the exposed services from the partners. The object instance directory stores partners' identifiers that can provide information for unique object instances. It accepts queries about unique object instances (electronic product codes-EPCs) and replies with the partner's identifier that can provide the required object instance information. The partners' registration directory stores all partners' registration information and relationships among partners.

The proposed framework builds on the EPCglobal architecture framework. However, SMART suggests a service-oriented approach, utilizing web services, to enable EPC-related information exchange between retail partners opposed to the object-oriented approach of EPCglobal.

In addition, SMART differentiates from the EPCglobal architecture framework by utilizing a data stream management system (DSMS) to aggregate EPC data per capture location and enrich them with object-related pieces of information (such as object ID/ barcode and object tagging level e.g. case/ item) enabling aggregation at various levels.

The proposed architecture can potentially support various RFID-enabled supply chain services in retail industry. However, during SMART, research focused on eight RFID-integrated retail supply chain services, such as back-room and shelf inventory tracking, smart recall, promotion management etc (Bardaki et al. 2007). To evaluate the business relevance of the alternative services, an industry survey was conducted, addressed to top executives representing retailers and suppliers/manufacturers in the European fast-moving consumer goods (SMART 2007, Lekakos 2007). In addition, a consumer survey provided useful input regarding the evaluation of Innovative Retail Consumer services. The findings of the two surveys (SMART 2007) prioritized the design and implementation of the two following RFID-enabled retail supply chain services in the course of the project.

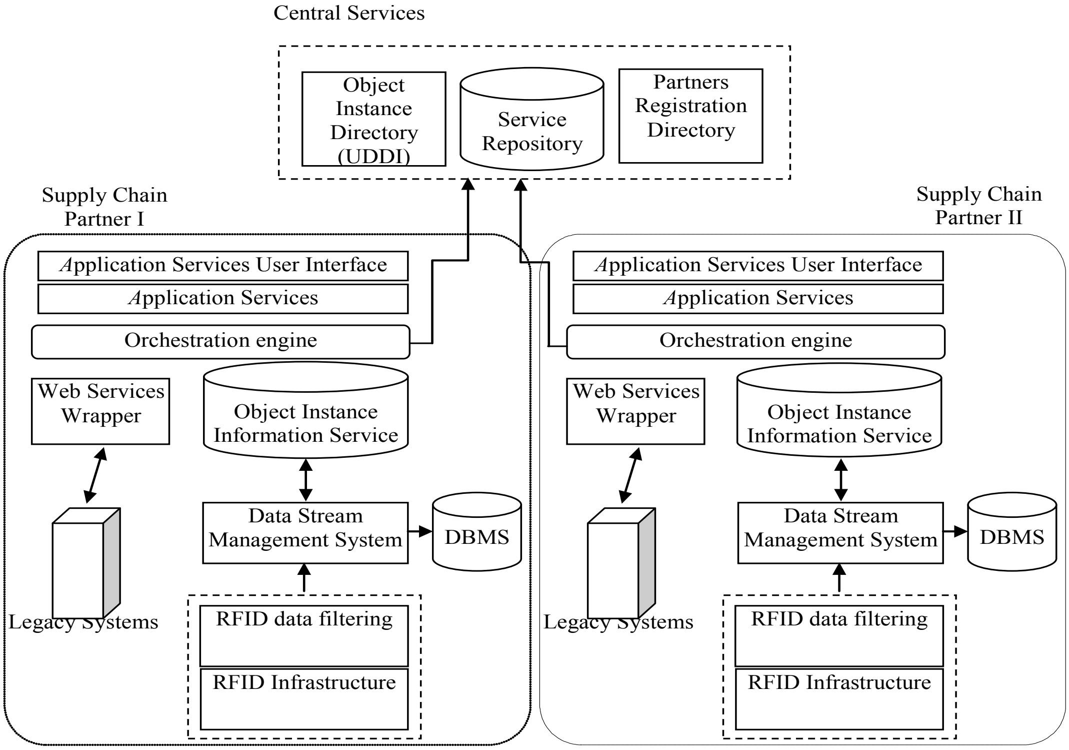


Figure 4.4-1: Logical view of the service-oriented SMART Architecture Framework.

At one hand, Promotions Management service supports the design, execution and evaluation of in-store promotion events that emerge into a prevailing promotion strategy in the retail industry. It provides to both retailers and suppliers the means to efficiently monitor the products availability on the promotion stands, the backroom and the regular shelves, the launch date of promotion events per store, the sales performance of the promotion events stand, etc. This is meaningful key performance information that can support the design of more efficient future promotion plans; this information is not provided by the current information infrastructure in retail stores, i.e. the point-of-sales (POS) scanning systems.

In addition, an innovative consumer application is included. The consumers interact with the system via a touch screen placed on a shelf of the promotion stand (figure 2). The touch screen interface offers: (a) product information: a list of the products under promotion appears on the touch screen and consumers can learn more just by clicking on them, (b) support for product selection: customers answer to a number of questions and, through a decision tree , they are guided to the product that fits best their needs and (c) alternative gifts: customer can select between a conditioner, a small shampoo (250 ml) or a discount coupon. The discount coupon provides discount one euro for the product the consumer selects. This coupon is printed on demand from a coupon printer placed on the promotional stand (see Figure 4.4-2).

To implement this service, case and item-level tagging are required and RFID readers are placed on the store back-room gate, on the back-room to sales-floor entrance and on the promotion stand shelves. Foam bath shower gels and shampoos were the products used during the pilot experiments.

On the other hand, Dynamic-pricing is suited for products that require frequent price adjustments and it supports different product instances to be sold at different prices (a strategy that is widely used for e.g. airline tickets). It can be used in food industry to generate demand for products approaching their expiration date, such as fresh or frozen products, and are soon to become out-of-date gathered stock. The proposed RFID service provides with the product availability on the shelves and the backroom per expiration date, the sales volume per store, etc. via a graphical user interface. It also proposes with price mark-downs based on an algorithm utilizing products expiration date, stock availability, etc. Both retail store managers and product suppliers collaborate to decide on the price mark-down after thinking on the services' price suggestions.

Figure 4.4-2: RFID-enabled Promotion stand with touch screen.

Moreover, an innovative consumer application is included. Consumers are informed about the discounted product items from an electronic display placed above the shelves (Figure 4.4-3). Specifically, the screen depicts: the number of products per expiration date, the price discount and the new price.

To implement dynamic pricing service, case and item-level tagging are required and RFID readers are placed in the product packaging line, where the expiration-date property is assigned to each product instance, on the store backroom (coldroom for fresh products) gate and on the fridge shelves. Packaged fresh minced-meet was the product used during the pilot experiments.

Figure 4.4-3: Electronic display above RFID-enabled fridge shelves.

A step-by-step approach was adopted to decide on a "realistic" implementation of the above services by assessing their technical feasibility and to what extent the potential benefits gained by RFID outweigh the value of investment in such an initiative. This approach is based on a detailed business process analysis, technical laboratory experiments and a cost-benefit assessment (Bardaki et al. 2008).

2.2 Technical and Business Lessons

The two services have been deployed in three real-life pilot sites in the course of SMART project. Specifically, the Promotions Management service has been deployed in two retail stores in Greece and Cyprus, while the Dynamic Pricing service has been deployed in a retail store in Ireland. Two rounds of pilots (at least 10 days per round) per store have been executed in order to identify technical and business pitfalls and to capitalize on the knowledge generated during the deployment of the services. Some of the lessons learnt coping with these challenges are summarized below to provide guidance to future developers of RFID-enabled supply chain services.

2.2.1 Readability issues

The ability to read without requiring line-of-sight makes missed reads an unfortunate reality with RFID systems. The material of the tagged items and of the surfaces of the surrounding area, the multi-path effect, the environmental conditions, the tag collisions and the tag placement are between the factors that interact with the electromagnetic nature of the RFID system and, as a result, influence the readability of the RFID system.

Both RFID-integrated services involve items containing liquid, i.e. foam bath shower gel and frozen packaged minced meat, which are radio frequency absorbing. In addition, the metallic surfaces of the promotion stand and of the trolley that transfers the packages of minced meat marked another physical constraint, because metal reflects the radio energy and causes multipath interference to the receiving antenna. Also, the multiplicity of tagged items on the shelf, with small distance between them, has generated conflicts because the simultaneous transmitted radio signals caused collision interference to the RFID reader. Finally, the orientation of the antennas on the shelves, in association with the tag location on the shelves orientation, was found to affect the radio wave received.

To cope with the aforementioned challenges, the performance of tags and readers of leading RFID manufacturers was evaluated in a lab environment (similar to the real environment and free of interference), in order to select the RFID infrastructure. Then, with key requirement the item-level visibility of the product on the shelf, we performed small-scale proof-of-concept testing in the lab environment executing several experiments with alternative tag positions associated with respective antennas positions and orientations. After the lab tests, we found out that the tag on top of the foam bath bottle and the minced meat package, i.e. the point where the liquid ends, as well as the antennas on the top and back of each shelf of the promotional stand and only on the top of each refrigerated shelf ensured the best possible readability for our target number of tagged items placed on the shelves.

We continued with comprehensive on-site testing executing several tests on the shelves with varying items density and distance between them, random or controlled placement of products and human interaction. We realized the cases of tag collisions and that the metallic surfaces of the promotional stand seriously infer the reading performance. Ultimately, both the lab and the on-site testing led us to the tight integration of the RFID infrastructure with the operational environment, i.e. the promotional stand and the refrigerated shelves; as a result, we embedded the RFID infrastructure in the refrigerated shelves and in the promotional stand that we customized with plastic surfaces.

2.2.2 Data Management and Aggregation issues

To present accurate and correct information, RFID-enabled services for the retail sector should encapsulate proper data cleaning, filtering and aggregation mechanisms. In essence, these data processing mechanisms incorporate the necessary smartness to the RFID application in order to cope with exception events referring to:

- Missing reads, i.e. the RFID reader fails to read a valid tag in a given reading cycle.
- Multiple consequent reads, i.e. the RFID reader registers a tag that should not have been read on this reading location or it re-registers a missing tag after several reading cycles.

In our initial pilot deployment, we witnessed several incarnations of these exception events that result in poor SMART service performance. For example, each time a consumer was picking up a product item from the promotional stand's shelf and then placing it back, he was removing it from the reader's antennas range for a short time interval. Initially, since a reduced quantity of products is RFID-captured and reported, the application considers the difference in the current inventory level of the shelf as sales; but then, it registers it as a shelf replenishment when the consumer puts the product item back on he shelf. Similar data quality problems appeared also when the connectivity between the readers and the middleware application was temporarily lost over a wireless connection in the store.

Our solution to these exception events was the development of a temporary database (buffer mechanism) that stores all unique EPCs of tags per reading cycle. Every time a product was placed on the promotional stand's shelves, the buffer mechanism is queried on the product's EPC; this is a replenishment only if this EPC is not already stored in the buffer. In case the query resulted to a success hit, meaning the product was placed on the stand in the past, the sales quantity is automatically reduced by one product. The buffer was reinitialized on a daily basis.

To summarize, the execution of the real-life pilots showcased that the aforementioned efforts to cope with the readability differences, as well as the combination of the RFID data filtering with the data stream management system effectively handles all the exceptions that might occur in a retail environment while at the same time it supports exceptional readability for the pilot applications. In particular, in each pilot we performed several audits comparing the system logs with the information displayed by the system and the actual products' quantity on the refrigerator and promotion stand shelves. The results of these tests proved that the system continuously presented accurate information on a real-time basis.

2.2.3 Consumer Privacy

To investigate whether consumer privacy affects the acceptance, and subsequent use, of our RFID-integrated services, we experimented with a disclaimer sign placed on the promotion stand at only one of the pilot sites and informing the consumers about the potential use of their personal data. At the remaining two test sites, we did not use the disclaimer sign. The experiment revealed that sales were significantly increased in the stores where we did not use the disclaimer sign. Furthermore, it was observed that many consumers avoided picking up products from the promotion stand simply because they had read the disclaimer sign. Interestingly, in the two pilot sites where the disclaimer sign was not used, consumers did not complain about RFID nor did they express any confound or puzzlement about the placement of RFID tags on the products.

2.2.4 Health Concerns

The pilots revealed that health concerns were the most emotive issue for both consumers and store personnel. In particular, the store personnel in all three pilot sites was significantly worried by the potential radiation effects of the RFID antennas in the backroom (antennas were visible). Similar concerns were expressed by the consumers in our initial pilot when the RFID antennas on the promotion stand were fully visible. It should be highlighted that some consumers complained directly to the store manager and asked for proof that the RFID infrastructure is harmless for their health. In our second round of pilots, when we hided the RFID infrastructure, we did not witness any health related concerns by the consumers. We acknowledge that this issue has gained importance due to the recent excessive, conflicting press coverage of all the possible ill effects of mobile phones and base stations.

2.2.5 Organizational Impact and Support

The top management's commitment and the cost have been identified to be the most critical issues that affect the organization's expectations of the RFID impact; and as a result, the support needed to engage in the RFID applications.

Semi-structured interviews with the users of the two RFID-integrated services, i.e. top management and store personnel, were conducted during the requirements analysis and after the first round of the pilot studies. They are expecting enhanced shelf products' availability and management of the promotional events capitalizing on the RFID capability to provide complete, accurate information on the location and the status of product items on a real time basis. Hopefully, the top management was found committed to give RFID technology a chance and test it, in order to really assess the cost vs. the expected benefits.

Furthermore, the top management underlined that the cost is the biggest challenge their organization faces with the RFID adoption. A key matter remains how to justify the investment and they believe that the cost will gradually be shifted to the consumers. The main cost of the RFID deployment comprises of the hardware and software investment, the tags cost, the cost of integration with the legacy systems and the staff training cost. It was also found that it is best to engage in RFID implementation with a preliminary cost vs. benefit analysis and then proceed with a small scale RFID application. Thus, we limited the RFID deployment to only two products and three reading points in three retail stores. The results of the real-life pilots at the three countries will open the way for the widely deployment of the RFID-integrated services.

3 Lessons learnt from the TraSer project

3.1 Architecture of the TraSer Framework

A detailed architectural description of the TraSer solution platform would be far beyond the limits of this contribution (those interested can find in-depth material either at the project's website at http://www.traser-project.eu, or at the corresponding project page on sourceforge.net). Still, it may be advisable to examine the major application requirements and the resulting architectural principles before looking at the experience gained with application pilots.

In order to understand the reasons behind the particular choices in the TraSer architecture, it is useful to recapitulate the recognized typical or expected requirements of the targeted application domain. TraSer is meant to serve as an entry-level solution package for small-scale users (typically the lower end of the SME sector, smaller institutions or networks, as well as education) that are either pursuing the establishment of lightweight tracking without too heavy burdens in IT investment, or are still in the phase of getting acquainted with item-level tracking as such. Therefore, both the service/network layout, as well as choices regarding identification carriers and formats were aligned with the following major requirements:

- An entry-level solution should be as simple and lightweight as possible to lower the initial threshold of adoption, allowing learning-by-doing practices. It should be clear that such a "beginners' solution" is likely to be replaced by a more elaborate system if larger-scale demands develop over time. Therefore, the introductory solution platform should not be expected to master more complex functionalities and larger volumes (likely at the cost of a larger initial threshold which would contradict the intention behind an entry-level solution).
- The typical user in the targeted application domain has no noteworthy experience in item-level track-and-trace practices. For such users, it is most attractive if they can easily carry out limited-range experiments without globally visible consequences and obligations to large authorities (including the associated administrative burden and organisational dependencies).
- Allowing a very low-cost entry and reasonably low total costs of operation are of key importance for successful adoption by small-scale users that have, by nature, very little—if any—accumulated financial resources. This is well-served by giving users a relatively free choice of physical ID carriers, independent and free-of-charge ID allocation, and general software components offered in a free and open-source package.
- In the small-scale user range, occasional participation in tracked operations and a frequent change of collaborating partners are fairly common. This should be reflected by i) the possibility of occasional participation in a network without major changes in the participant's IT infrastructure, and ii) flexibility of the solution package, allowing easy adaptation to other tracking networks (well noted, adapting a TraSer network to larger, more elaborate and more rigid tracking networks is technically much more justified than the other way around).

The implementation of the TraSer solution platform (Monostori et al. 2009) relies on Web Services (WS), a widely supported standard with a large spectrum of off-the-shelf frameworks and specific extensions, both commercial and open-source. WS allow more flexible configuration of communication (as opposed to "classical" EDI (Electronic Data Interchange; see Burrows, 1996) which small enterprises may find too cumbersome and costly to configure and maintain). The TraSer solution platform allows participants to build a TraSer network where two components can be distinguished: servers and clients. Figure 4 depicts a simple TraSer network—also note that several of such networks can exist independently without any central governing service or authority, i.e., there is no such entity as "the TraSer network".

TraSer servers store item-related data accessible to authorized parties. A given unique item is assigned to one and the same server for the entire life-cycle of its ID, and the TraSer-internal notation of the item's unique identifier directly specifies the address of the corresponding server (see also comparison with ONS/EPCIS at the end of this section).

The servers can process requests in the form of XML queries (Boag et al, 2007) which allow more flexibility in customizing the data models used by the partners, and, in the longer term, enable the establishment of explicitly defined and negotiable data models as a foundation for efficient cross-company communication. TraSer servers can also forward queries or updates to each other—these server-to-server connections span a part of the TraSer network (see Fig. 2: part a) depicts a small network of several servers and part c) stands for a company which operates a TraSer server within its own IT infrastructure).

Server-to-server communication in the form of forwarded updates or queries is practiced if the set of item information in question is maintained by different servers, and as a consequence, queries or updates need to be forwarded. This is typical for production networks where the products of several manufacturers are combined to a composite item, and information about the sub-assemblies possibly resides in different servers of the same TraSer network. Also, the data of a given item can be extended by further properties which are not necessarily located in the same server (e.g., when a manufacturer wishes to add its own relevant notes to the item description of its supplier).

TraSer clients form the other main group of components in a TraSer network. Clients connect the servers with the rest of the world by providing external interfaces and addressing one or more servers with item-related queries or updates. Clients can be fitted with various kinds of interfaces, i.e., they can be designed for human operators, peripheral devices (readers, etc.), other components of the enterprise infrastructure (stock management, ERP), and other tracking and tracing systems. Since TraSer interface specifications are freely available, users can develop specific clients tailored to their given needs. Figure 4.4-4 shows several specialized cases of client use. Companies which do not have their own TraSer-tracked items (e.g., logistics partners not maintaining their own transportation asset data in a TraSer system but updating the shipment information of a manufacturer's products; or a small supplier which lets a larger partner care about hosting its product data) are not required to operate their own server, as shown in part b). The company in part c) operates, aside from the TraSer server, several specialized clients. One of these serves as an adapter for accessing other components of the manufacturer's IT infrastructure (part d)), while another client was customized as an interface towards another tracking network (part e)). Clients acting as adapters to other infrastructure components or networks are vital for lifting compatibility-related access restrictions to an isolated TraSer network.

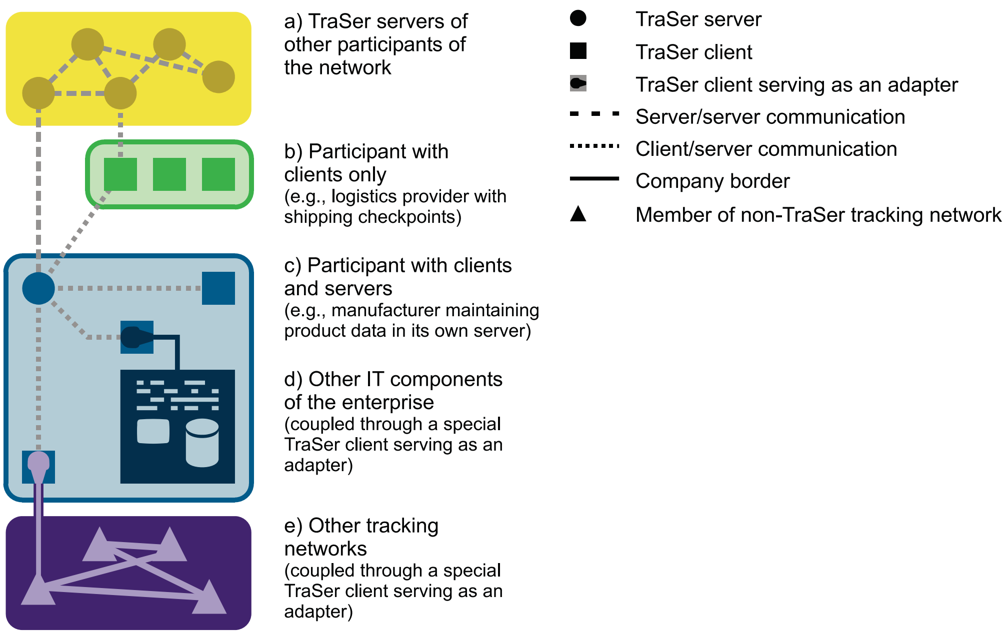


Figure 4.4-4: Simplified example of a TraSer network.

TraSer favours small-scale users in keeping a reasonable balance between the freedom of independent issuing of identifiers and the ability to adapt to networks operating by other standards. Most of these advantages are owing to an ID@URI type of identifier notation (Dialog, 2003) used internally by TraSer. Here, the globally unique identifier is composed of two parts: ID and URI, none of them being a full identifier alone. The URI part is a direct pointer to the address where the TraSer server maintaining the data of the given item can be contacted. In our case, URI is, in fact, a URL. This URL is unique to the given TraSer server but not to the item—in other words, the same URL is used for accessing data of several items. The item one wishes to access is then unambiguously specified by the request sent to the aforementioned address—this request also contains the ID part of the unique identifier. The ID part of the notation must, therefore, be unique among all items handled by the same server.

While this appears fairly similar to the principles of Object Naming Services (ONS) and EPC Information Services (EPCIS 2007), there are two fundamental differences (see also Figure 4.4-5), resulting from different main goals being pursued, as well as other user domains being targeted. First, finding the services associated with an item does not require a separate resolution mechanism, since the address of the service access point is already contained in the URI part of the item (and, therefore, only a URL to IP address resolution is needed which is readily done by the DNS lookup). Second, no central authority is needed to guarantee global uniqueness of the identifiers. This is, in a way, "piggybacking" an already existing DNS infrastructure which guarantees global uniqueness of URLs and thus preventing collisions within the URI part of TraSer's identifier notation. Once this is ensured, only the uniqueness of the ID part per each URI—i.e., not per each single ID@URI type identifier—has to be guaranteed for global uniqueness of the entire identifier. This allows the decentralization of identifier allocation and allows much independence for participants issuing new identifiers. An independent identifier notation may raise concerns of isolation from other networks using other standards. These fears are unfounded as far as TraSer makes it easy to adapt to any "external" numbering scheme by providing means of identifier mapping. While this is facilitated by the possibility of including any instance of another numbering scheme in the ID part of the TraSer identifier, full conversion between identifiers is always performed by the clients. Several ways of implementing a mapping mechanism are at the users' disposal (and have already been tested in various examples), however, their detailed description is well beyond the scope of this paper.

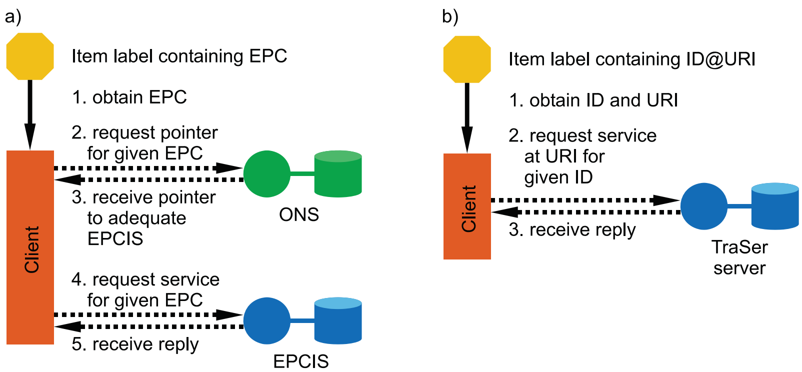


Figure 4.4-5: Comparison of service address resolution and access.

In order to make the TraSer solution platform fit for industrial use, a roadmap of application pilots was followed where subsequent releases moved from simple use cases towards higher levels of functionality, and from closed circulation of relatively few identified items to flow-through identifier handling. This allowed an incremental development and refinement of the TraSer platform where practical experience contributed to the support material for prospective users as well. Due to the specific topic of the paper, examples with relevance to supply chains are highlighted next.

Minimalistic tracking for occasional collaboration. The Hungarian company Disher Kft. is specialized in product development and prototyping, as well as the production of limited batches of smaller plastic and metal components, mainly for the automotive industry. As far as production is concerned, the company often relies on suppliers which are small enterprises and regard their supplier status with Disher Kft. as an occasional collaboration. As occasional suppliers do not find it worthwhile to invest in developments supporting the business processes of the temporary alliance, a solution had to be found which puts the least possible burden on a small supplier (which is, usually, neither financially nor technically in the situation of hosting a major IT investment). The solution was the use of a single TraSer server by Disher Kft. (now assuming the role of a larger central player) that maintains the data of the supplier's products, as opposed to the usual practice of the manufacturer itself caring about the data storage of its own products. Item identifiers (including their physical form of labels) were issued by Disher Kft. as a part of the contract with the supplier, and the latter only had to operate a simple tracking client that could be either a mobile reader or an even more minimalistic web client. The solution largely relied on already existing components of the IT infrastructure of the enterprises, thereby lowering the burden of initial technology pickup—an important aspect for introducing tracking services in the lower end of the spectrum of targeted users.

Tracking across multiple supply chain stages. The Romanian ice cream manufacturer Kubo Ice Cream SRL embarked on installing tracking services in anticipation of future transparency and traceability regulations to be imposed on the food industry in the coming years. Kubo Ice Cream SRL is a manufacturer of regional importance with one manufacturing site producing about 10000 boxes of ice cream per day. These are, once production is completed, grouped onto pallets and transported into several regional warehouses that serve local replenishment partners. The envisaged tracking solution was required to work transparently across the entire supply chain from production to local delivery, taking into account an already existing ERP (enterprise resource planning) solution as well as a restricted time-frame of local updates (local delivery partners can only upload recorded shipping events at certain points of time). In the implemented solution, several field clients, office clients and ERP middleware adapter clients were installed around a TraSer server to keep track of the following stages in production and delivery of ice cream boxes: i) production and box-wise allocation of unique identifiers; ii) creation of pallet instances and linking of box instances loaded onto the given pallet; iii) intermediate storage on the manufacturing site; iv) pallet-level receiving in the regional warehouses; v) distribution of boxes to local replenishment partners; and vi) final delivery to the point-of-sale and confirmation by local delivery agent (see also Figure 4.4-6 for a schematic overview). The successful application at Kubo Ice Cream SRL is, to date, the most complex implemented TraSer solution where adaptation to different timing constraints, material handling approaches and existing IT infrastructure had to be solved.

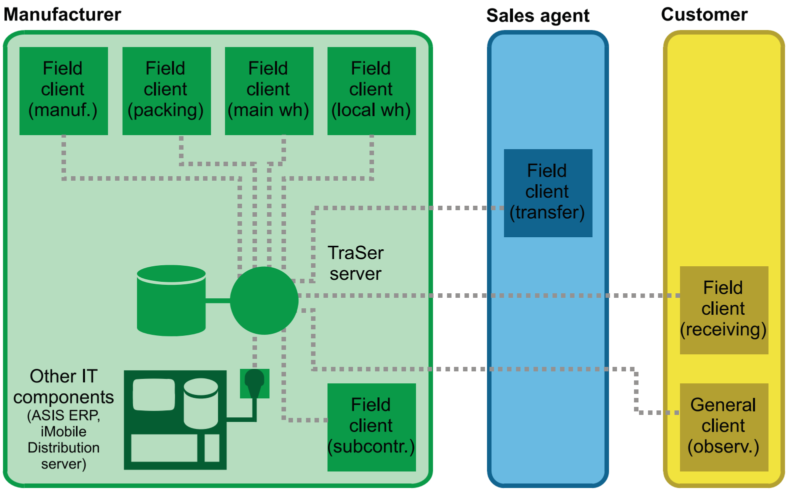


Figure 4.4-6: Use of a single TraSer server with access from several levels of a supply chain. (Note that the TraSer platform is, in this example, also integrated with other IT components of the manufacturer).

Closed-circuit asset tracking with potential for material tracking in supply chains. The Finnish logistics company Itella (formerly Finnish Post) employed the TraSer platform primarily as a test bed for closed-circuit tracking of re-usable metal roll cages where initial hardware-related tests to master typically “RFID-hostile” conditions (e.g., metal surfaces, cross-talk of nearby readers, rough treatment of tags, etc.) formed a substantial part of the challenges. During the tests, the TraSer server was coupled to Itella’s own peripheral middleware that generated discrete, high-level events based on raw readings on the lower end of the architecture, and to administrating user interfaces on the higher end of the architecture (Figure 4.4-7). Upon completion of hardware-related tests and successful adaptation of the TraSer system to Itella’s conditions, possibilities were examined for the extension of established services and functionalities. Initially meant to merely keep track of roll cages (and thus minimize losses currently in the order of magnitude of several ten thousand roll cages per year), plans were examined for offering package tracking services for customers relying on roll cage tracking information, thus enabling a closed-circuit tracking solution to support flow-through material tracking, as it occurs in supply chains. While the tracking project is currently on hold at Itella, and a proprietary system optimized for large volumes and little item variability—more suitable for Itella’s purposes—will eventually replace the TraSer test platform in internal use, a TraSer-based solution still remains a feasible option for building up shipment tracking services for customers.

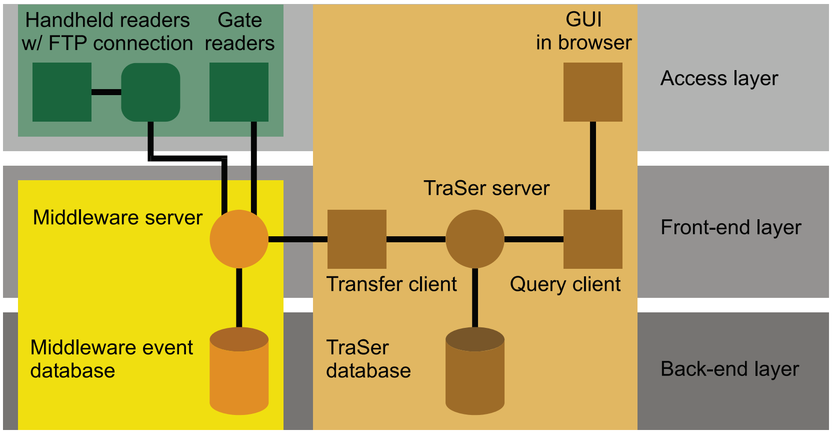


Figure 4.4-7: Inclusion of a TraSer-based solution in the IT architecture of Itella—combination with peripheral middleware and user interfaces.

3.2 Technical and Business Lessons

3.2.1 Tag readability issues

In some cases, the extreme application conditions present challenges where previous experience with other RFID applications is of little help. One of these hard-to-solve situations was the application pilot at Itella where one could as well consider the entire environment downright "RFID-hostile":

- the tracked roll cages themselves were of metal, and at least the usual stacked handling of empty roll cages would impair tag readability;
- the common construction of recent warehouses uses corrugated metal sheets that are certain to cause ambient reflection;
- neighbouring gates are so close to each other that cross-talk phenomena could occur;
- the roll cages are exposed to rough treatment which the tags must also endure.

Itella embarked on an extensive series of experiments with a variety of tags and gate reader antennas—eventually resulting in UHF tags being developed especially for their needs. As mentioned earlier, pre-filtering of raw RFID readings was also needed to overcome occasional read errors experienced especially with gate readers, and to generate discrete events that provided raw readings with a low-level interpretation.

While these readability issues were peripheral from the point of view of the TraSer software, another case proves that handling them is essential for the successful introduction of a complete track-and-trace solution. Elis Pavaje SRL, a Romanian manufacturer of concrete pavement elements, envisaged to cope with replacement losses of damaged stock, and track its output pallet-wise (approx. 250 pallets per day) through the entire delivery process to the vendors. Preliminary studies suggested RFID as a favourable method of identifying the pallets—later tests, however, showed that none of the RFID solutions provided by local vendors delivered satisfactory results. Having no financial means for proprietary solution development, as pursued by Itella, the deployment of a track-and-trace solution did not take place at this time.

3.2.2 Coping with technological and financial barriers

In many cases, the exclusive use of RFID may present a serious barrier to introduction of track-and-trace solutions. While it is well understood that the price of RFID solutions is still too high for most of the small enterprises, another factor also surfaced during the introduction of several TraSer pilots: reluctance to adopt RFID due to the pressure exerted by identifier solutions already in use at the adopting company/companies. This was the case, for example, with the one-tier pilot conducted at Disher Kft., where optically readable identifiers were already employed for box-wise identification of products. Here, the existing solution was "piggybacked" by the new functionalities for tracking, so that participants were not forced to invest in new AutoID solutions. Consultation with piloting partners often revealed that currently, establishing transparency across the entire supply chain may require a combined use of multiple identifiers (or physical ID carriers) to bridge compatibility gaps between different (and possibly proprietary) tracking solutions. One of the most straightforward examples is the combined use of optically readable labels with RFID—this not only lowers the initial investment burden for smaller participants but also serves as a fallback measure, should either one of the identification methods fail.

Small enterprises and occasional participants have shed light on yet another issue that may be critical for successful adoption of a tracking solution across the supply chain: the urge to minimize any additional burden on the IT infrastructure of the company. To this end, it is vital to closely examine the processes to be tracked, as well as the resources required for the solution, including their possible distribution among the participants of the supply chain. As a result, a better choice of TraSer clients can be made (e.g., portable device, automated standalone client, or simple web client), and the storage responsibilities for item-related information (boiling down to server allocation and guaranteed operation over a specified time range) can be distributed more in accordance with the magnitude of participation in the supply chain. Offering “lightweight” alternatives for occasional collaboration may ultimately be a key to successful expansion of tracking solutions and services in the supply chain.

3.2.3 Cross-company transparency—handling confidentiality concerns

Transparency may be a key to successful handling of complex production and delivery processes (Jansen-Vullers et al., 2003; Dejonckheere et al, 2003). Establishing it across a supply chain with several members inherently requires the disclosure of information about the items passing through the supply chain. During consultation with potential users, it became clear that many companies, especially small enterprises without much experience in IT solutions in general, are reluctant to share any production-related information because they fear to disclose important confidential data to unauthorized parties. While the TraSer platform offers configurable access control options, the technical capability itself is not enough to convince sceptics with little insight. Therefore, we found it helpful to establish an “investment vs. benefit” perspective: sharing of data can be regarded as an investment, with savings on supply chain operation, reduction of losses or other competitive advantage being the expected benefits.

Where established, cross-company transparency was flawlessly working in the TraSer pilots concerned, as TraSer is a solution framework where transparency is granted by the network architecture from the beginning. Some of the noteworthy examples are the complex solution deployed at Kubo Ice Cream SRL, the one-tier item goods tracking at Disher Kft, or the collaborative design support (tracking of CAD files in the manner of a distributed version control system) in use at several design companies within the Disher Design group.

4 Discussion and Conclusions

During the lifespan of the SMART project we have investigated issues related to market acceptance and deployment costs for both services. We have evaluated the market attractiveness of the two services through the execution of an industry survey (in the form of a live workshop) in Athens, Greece. From the responses in the survey it is apparent that RFID is still perceived as an immature and expensive technology whose ROI is difficult to quantify and assess. Successful pilots (such as in the course of SMART) may eventually constitute the drivers for widespread acceptance of RFID; and decrease the already high resistance of supply chain management trading partners to invest. Hence, a fully commercial exploitation of RFID on item level tagging may not be expected before 2010. The prohibiting factors may be summarized to the following: very high procurement and deployment costs of RFID technology and support infrastructure; lack of standardized procedures for tagging products and sharing of information; uncertainty regarding ROI, payback of the investment; immaturity of the technology; lack of a techno-centric culture by consumers and small companies which might lead to a ‘resistance to change’ attitude.

To conclude, through this paper, the SMART project proposes a service-oriented architecture that utilizes: the automatic, unique identification capabilities of RFID technology, data stream management systems and web services, to support RFID-integrated supply chain services. Two such services, i.e. dynamic pricing and promotions management, have been pilot tested in three retail stores in three European countries. The valuable experience gained during the three pilots, concerning RFID readability challenges, consumer privacy, customers and store staff health concerns, and investment costs, have been summarized to support future developers of RFID-enabled supply chain services as well as to set an academic research agenda.

The main goal of the TraSer project was the creation of an open-source framework for tracking and tracing solutions, primarily targeting small and medium-sized enterprises. Reflecting the typical needs for this application area, the TraSer platform allows the easy establishment of a transparent network architecture, and is optimized for large product variability and flexible data models (as opposed to large-scale but more rigid solutions for classical mass production).

The TraSer platform was tested in numerous applications whose range was not restricted to supply chains. Not depending on a particular physical ID carrier, RFID was not the only means of identification employed in the tests—a feature that was found a major advantage in low-end or specialized applications.

General experience gathered in the pilots has shown that RFID-based tracking in supply chains is still hindered by several obstacles. RFID technology itself is, in its current state of development, not always a satisfactory physical ID carrier, and much improvement is due in terms of readability in critical environments (including typical ways of merchandise handling) or in conjunction with certain materials. The penetration of RFID may be also hindered due to its costs, as well as the presence of another, already installed and reliable, AutoID solution. In such cases, interim solutions (such as combination or replacement of RFID with optically readable identifiers) may lower the threshold for adopting a new tracking solution, and may even improve transparency across a supply chain with a variety of different, separately developed, tracking systems. Transparency in the supply chain implies sharing of product data—even though the TraSer platform is well-prepared for secure handling of cross-company transparency, potential users with less experience or less insight into the technological backgrounds are certain to be reluctant about information sharing. In order to overcome such burdens, it proved important to put services and processes connected to cross-company transparency into the appropriate context, i.e., considering information sharing a (scalable) investment in expectation of benefits.

5 References

C. Bardaki and P. kourouthanassis (2009). RFID-integrated Retail Supply Chain Services: Lessons Learnt from the SMART project. In Proceedings of the Mediterranean Conference on Information systems (MCIS 2009), Athens, Greece.

C. Bardaki, A. Karagiannaki and K. Pramatari (2008). A Systematic Approach for the Design of RFID Implementations in the Supply Chain. In Proceedings of the Panhellenic Conference on Informatics (PCI 2008), Samos, Greece.

C. Bardaki, K. Pramatari and G. J. Doukidis (2007). RFID-enabled supply chain collaboration services in a networked retail business environment. In Proceedings of the 20th Bled eConference, Bled, Slovenia.

Boag, S., Chamberlin, D. Fernández, M. F., Florescu, D., Robie, J., and Siméon, J. (2007). XQuery 1.0: An XML Query Language, W3C Recommendation 23 January 2007. http://www.w3.org/TR/xquery/

Burrows, J. H. (1996). Electronic Data Interchange (EDI), Federal Information Processing Standards Publications, FIPS PUB 161-2. http://www.itl.nist.gov/fipspubs/fip161-2.htm.

Chatziantoniou, D., & Johnson, T., (2005). Decision Support Queries on a TapeResident Data Warehouse. Information Systems Journal, 30(2), 133-149.

Dejonckheere, J., Disney, S. M., Lambrecht, M. R. and Towill, D. R. (2003). Measuring and Avoiding the Bullwhip Effect: A Control Theoretic Approach. European Journal of Operational Research, 147(3), 567–590

Delen, D., Hardgrave, B. C., & Sharda, R. (2007). RFID for Better Supply-Chain Management through Enhanced Information Visibility. Production and Operations Management, 16(5), 613-624.

Dialog (2003). DIALOG open-source community web site, http://dialog.hut.fi/osc/index.php

EPCIS (2007). EPC information services standard reference page. http://www.epcglobalinc.org/standards/epcis.

Fleisch, E., & Tellkamp, C. (2005). Inventory inaccuracy and supply chain performance: a simulation study of a retail supply chain. International Journal of Production Economics, 95(3), 373-385.

Jansen-Vullers, M. H., van Dorp, C. A., Beulens A. J. M. (2003). Managing Traceability Information in Manufacture. International Journal of Information Management 23(5), 395–413.

Kourouthanassis, P., & Roussos, G. (2003). Developing Consumer-Friendly Pervasive Retail Systems. IEEE Pervasive Computing, 2(2), 32-39.

Lekakos, G. (2007). Exploiting RFID digital information in enterprise collaboration. Industrial Management and Data Systems, 107(8), 1110-1122

Muehlen, M., Nickerson, J. V., & Swenson, K.D., (2005). Developing web services choreography standards – the case of REST vs. SOAP. Decision Support Systems, 40, 9-29.

Monostori, L., Ilie-Zudor, E., Kemény, Zs., Szathmári, M., & Karnok, D. (2009). Increased transparency within and beyond organizational borders by novel identifier-based services for enterprises of different size. CIRP Annals—Manufacturing Technology, 58(1),417–420.

Nath, B., Reynolds, F., & Want, R. (2006). RFID Technology and Applications. IEEE Pervasive Computing, 5(1), 22-24.

Ngai, E.W.T., Cheng, T.C.E., Lai, K., Chai, P.Y.F., Choi, Y.S., & Sin, R.K.Y. (2007). Development of an RFID-based Traceability System: Experiences and Lessons Learned from an Aircraft Engineering Company. Production and Operations Management, 16(5), 554-568.

Sheng, Q. Z., Li, X., & Zeadally, S. (2008). Enabling Next-Generation RFID Applications: Solutions and Challenges. IEEE Computer, 21-28.

SMART (2007). Deliverable 1.2: requirements analysis. EU Project ST-5-034957-STP, ELTRUN, Athens University of Economics and Business, Athens.

6 Acknowledgements

The work presented in this paper has been partly funded by the European Commission through the IST Project SMART: Intelligent Integration of Supply Chain Processes and Consumer Services based on Unique Product Identification in a Networked Business Environment (No. IST-5-034957-STP), http://www.smart-rfid.eu; and TraSer: Identity Based Tracking and Web-Services for SMEs (No. IST-5-033512), http://www.traser-project.eu. The authors would like to thank all the project partners for their contribution.

4.5 An EU FP7 Project defining and accommodating international issues concerning RFID with particular reference to the emerging "Internet of Things."

CASAGRAS Project

Ian G. Smith

AIM UK

Abstract: The CASAGRAS project began in January 2008 with a brief to provide a framework of foundation studies to assist the European Commission and the global community in defining and accommodating international issues and developments concerning radio frequency identification (RFID) with particular reference to the emerging "Internet of Things." It has proved a fascinating project. The partners are leading experts in these fields from China, Korea, Japan, USA and across Europe. Their input helped develop and produce a detailed report. The project partners have been unanimous in reaching the published conclusions and the range of recommendations. The final conference which disseminated the conclusions and recommendations was held in the Central Hall, Westminster, London on October 6th and 7th 2009. Speaker power-points are available on the CASAGRAS website (www.iot.eu.com) and video films of the individual presentations are also available from the site.

1 The CASAGRAS Initiative

Europe has made a very significant investment in the INTERNET of THINGS. When the CASAGRAS Project began in January 2008, the roadmap to realisation was largely fragmented. The international partners recognised immediately that without a substantial international organisational platform to steer its development the IoT would likely evolve in an uncertain, fragmented and potentially troublesome way.

A primary CASAGRAS conclusion has been to propose the establishment of such a platform.

The EC COM (2009) 278 declared the Commission's clear intention to intensify the existing platforms for international dialogue on all aspects of IoT. Current initiatives include cooperation with the USA concerning best practices to optimise the economic and social impact of RFID and cooperation with the Japanese Ministry of Economy, Trade and Industry on, among other things, RFID, wireless sensor networks and the Internet of Things.

CASAGRAS through its remit has considered these international dimensions concerning regulations, standardisation and other requirements necessary to realise a global IoT concept. The project has collaborated with international experts from the USA, Japan, China and Korea.

As the CASAGRAS project reaches its conclusion one of its strongest recommendations to the Commission for the continued development of the IoT is to extend its partnerships even wider and to encourage co-operation across all continents. This will give Europe its best chance to initiate a global platform for an Internet of Things. These requirements for international co-operation will undoubtedly extend beyond those of the established Internet. They will be required to align with cooperative initiatives on the evolving Internet. The more demanding aspects of the IoT include:

- The nature of essentially autonomous networked structures that will facilitate interfacing with the physical world, to both collect and deliver data and information
- The structures to facilitate actuation and control in situations where there is no immediate human intervention to deal with problems of functionality.
- The complexity of structures in terms of numbers and functionality of devices

- The importance of identity management within the world-wide ICT infrastructure.
- A major Public relations initiative with respect to services and applications.

The CASAGRAS recommendations for progressing the realisation of an IoT and the associated international cooperation needed to achieve such a goal can be partitioned into those which will impact on IoT development and those upon which an action plan can be based.

The findings of a Support Action initiative such as CASAGRAS, can only provide a superficial look at the detail that is necessary, particularly with a concept that is so far reaching in respect of the technological multi-disciplinary factors, principles and issues involved.

The partners believe the real value of CASAGRAS has been to draw attention to the wider, overarching issues and provide the framework for an appropriately funded future international platform for development.

2 CASAGRAS Conclusions

The development of an IoT requires attention to foundational features as well as those of infrastructure, architecture and technological significance. There is an initial requirement for the overarching framework to define and accommodate the development of the IoT, without the diversion of attention presented in considering detail in the absence of a defined goal. The foundational features are significant in this respect.

2.1 The foundational features

The foundational features relate to:

- Further understanding and exploitation of object space, object grouping and object-based connections as a basis for identifying applications and services and developing a design methodology to facilitate more effective solutions.
- Further development of the applications and services framework, through better understanding of processes and service requirements, and again as a basis for identifying applications and services and developing a design methodology to facilitate more effective solutions.
- Identification and development of services infrastructure and particular global network services geared to exploiting international sources of information, knowledge and resources that can better serve international needs through cooperation.
- Foundation principles for direct Internet connection applications and services.
- Further extending the principles of object-connected ICT to encompass the evolving ICT features of the IoT and as a basis for accommodating the attributes of supporting technologies and underpinning design and application methodology.
- Attention to harmonised and non-harmonised standards in respect of regulatory control and issues of interoperability.
- Establishment of a central, global library of regulations regularly updated to satisfy design and support needs.
- Attention to social and economic issues, including privacy and security of personal information and their significance with respect to IoT applications and services development.
- Governance and the need to establish a model that is built on transparent, fair and non-discriminatory international principles, free of commercial interest.
- Policy issues in respect of international cooperation, including their significance with respect to governance.

It is recommended that all these topics be pursued through research as a foundational base for the IoT and as a framework for supporting on-going IoT development.

2.2 Infrastructural and architectural features

While it is possible to distinguish the principal architectural features for an IoT in terms of physical interface and data transfer structures, host information systems, networks and Internet access, the definition will change as relevant new technology comes into use. However, the CASAGRAS team believe the key architectural requirements for implementing a technologically inclusive IoT include:

- Development of an identification resolver approach for accommodating the need for global coding for identification, designed to accommodate legacy identification systems, and extendable to cover other issues of identity and identity management.
- Development of the architecture and infrastructure for direct object-to-Internet applications and services.
- Exploitation of Service Oriented Architecture (SOA) and associated network architecture for IoT services design.
- Development of universal data appliance protocol (UDCAP) for plug-and-play exploitation of conventional AIDC technologies and other object-connectable edge devices.
- Developing a unified approach to exploiting wired and wireless communications which will exploit appropriate developments in identity management to ensure the most efficient and effective use of the communications capabilities.
- Monitoring and adoption of relevant developments in ubiquitous computing and networks, wireless sensor networks, and translating relevant technologies and adopting an approach to unified solutions.
- Development of predictive analytical techniques, automated network management and self-repair networks, through exploitation in identity management to facilitate automatic computing across the IoT infrastructure; accommodating developments in advanced data management which, through open implementation of the main standards will lower the barrier of entry to the IoT for smaller organisations.

The latter is particularly significant for the elements of the IoT infrastructure handling object-connected to object-connected functionality, independent of human intervention to handle problems. Self-configuring auto-discovery as well as self-diagnosis and repair should also be a consideration in the automated network management. Identity management is crucial to such developments.

2.3 Technological Development

With RFID having been recognised as a primary technology driver for the IoT in the remit presented to CASAGRAS it is important to view RFID as a key on-going consideration in further international cooperation. Whilst RFID remains a significant platform for IoT it must be recognised that its take-up is still constrained by the perceived high costs of application. Technological developments, including printable devices that are geared to reducing device costs will clearly need to feature in on-going collaboration. Parallel considerations must also accommodate the exploitation of other lower cost AIDC technologies including linear bar codes and two-dimensional codes.

Further recommendations for technological development include:

- Development of standards-compliant RFID devices and readers.
- Lower cost, lower power sensor and processing platforms, to support the design and realisation of sensory networks.
- Development of location and positioning technologies to support IoT applications and services.
- Development of object-connectable communications platforms, including near field communication structures.
- Lower cost, higher performance energy harvesting and other powering techniques to support the development and exploitation of IoT wireless devices.
- Biometric-based interfaces for IoT applications and services.
- Privacy and security support technologies, including cryptographic devices based upon natural feature identification (physical one-way function devices).
- Intelligent embeddable processing and communication devices to facilitate automatic nodal functionality, including developments to support automated network management, self configuration and self-repair.
- Physical natural feature identification readers and IoT interfaces for exploiting natural feature identification.

- Middleware and other software developments, including intelligent processing platforms to support IoT functionality and services design.

3 Recommendations

In devising a plan of action for Europe to pursue the development of an IoT it is clear that on-going international cooperation is the key requirement.

Extending the number of international partners and gaining agreement on the structural, governance and foundational features will help to better define and accommodate the development of the IoT.

What can be seen from the CASAGRAS study and the CERP-IoT initiative is the substantial investment that has already been made by the EC towards realising this IoT concept, and its importance within the European strategy for ICT development.

However, there can also be seen a need for rationalising this and subsequent investment to better utilise its potential.

Governments, industries and businesses are clearly unaware of what the IoT is and what it offers. Awareness and education programmes are key requirements in creating a better understanding of the potential and the benefits.

These programmes should be particularly directed to the SME community. Follow-up business development initiatives will be critical in taking the IoT concept to effective reality.

- The establishment of an overarching, internationally-partnered, organisational platform to help to steer the IoT development. These partners should represent a cross section of interest including Governmental and Standards agencies; industry, business and academe.
- The development and delivery of a strategic migration plan for developing an IoT from a minimalist model to a more inclusive model, including identity management and resolver techniques
- The development of a universal or federated data capture appliance protocol to accommodate migratory inclusion of object-connectable technologies.
- The development of an architectural platform for supporting and demonstrating IoT application and services, and for addressing problems associated with IoT development, possibly based upon the establishment of a generic top-level Internet domain.
- The development of the rules for governance of the IoT with attention to social and economic issues including privacy and security
- The initiation of application and service pilot studies and demonstrators, particularly with respect to pathway process applications exploiting extended process functionality and scalable sensor-network applications.
- International cooperation on pilot developments and promotional initiatives directed at enhancing inclusion of national bodies in cooperative developments.
- The establishment and pursuance of a strategic research and development roadmap for IoT development, drawing upon the findings of the CERP-IoT group report, Internet of Things Strategic Research Roadmap (2009).

In addition the CASAGRAS partners believe there is a need to:

- Agree on a definition of the Internet of Things that can be used as a popular point of reference.
- Reduce the number of overlapping and potentially conflicting projects.
- Undertake major education, training and awareness programmes to explain the IoT. Ideally this should be part of the next round of projects aiming at creating global understanding and awareness.
- Set up key European Centres or academies for AIDC and the Internet of Things, underlining the importance or awareness, training and education. This foundational move will ensure the involvement of academe in the educational process associated with IoT development and will underpin further development of the principles in response to technological change.

CASAGRAS has proved without doubt that there is the need and the will for international co-operation. China, Japan, Korea and the USA are on board. Europe has taken the lead and now needs to drive the initiative as a truly global partnership.

4.6 Standardisation issues challenges on RFID and a future IoT

GRIFS Project

Josef Preishuber-Pflügl

CISC Semiconductor Design+Consulting GmbH

Abstract: The RFID standardisation world is currently facing a series of challenging issues that are slowing down the development of relevant standards which should support an efficient deployment of RFID technology. With a wealth of standards developed by different organisations, the challenges are, among others, a lack of clarity for users who have difficulties to differentiate and identify which standards they actually need, a lack of interoperability of standards which often leads to conflicts and difficulties to apply the standards together, a lack of communication and information sharing between standardisation bodies, often synonym with redundancy of work, etc. In this article, we will present how the GRIFS project, an FP7 support action funded by the European Commission and managed by GS1, CEN and ETSI, offers a set of simple tools and a platform involving key international standards bodies to solve these challenges. A first step in the project work was to identify which standards are currently in place and which areas in particular are in need of collaboration. An online database of international RFID standards was created as a sustainable and dynamic tool of reference for anyone in need of information on RFID standards. Listing 175 standards at the time, it facilitates the accessibility, comprehension and clarity of RFID standards. In order to reach the objective of getting the standardisation bodies together to encourage their communication and information sharing, the GRIFS project's main action has been to put in place a Forum of collaboration based on a Memorandum of Understanding. This platform enables the international standards bodies to communicate and collaborate better, without interfering in each other standardisation's processes. The Forum offers a neutral space to discuss about identified issues and find solutions together, based on the good will and common interest of the participants.

1 Organization

1.1 Members

The Global RFID Interoperability Forum for Standards (GRIFS) is a Support Action Project funded by the European Commission with the aim to improve collaboration and thereby to maximise the global interoperability of RFID standards. The GRIFS project initiated a forum that will continue to work constructively and grow after the end of the project through a Memorandum of Understanding between key global standard organisations active in RFID.

GRIFS is coordinated by three major standards organisations:

GS1 (coordinator) www.gs1.org	European Telecommunications Standards Institute – ETSI www.etsi.org	European Committee for Standardization – CEN www.cen.eu

1.2 Objectives

The objective of the GRIFS project is to characterise the variety of standards activities taking place globally to:

- Create a number of liaison activities to disseminate information about the importance of global standards
- Align RFID standards development globally
- Put in place the 'Global RFID Interoperability Forum for Standards' (GRIFS) comprising global stakeholders
- Ensure continuing close collaboration between standards activities.

1.3 Scope

This support action focuses on the use of RFID in supply chain and related activities. These activities primarily encompass the tracking and tracing of objects and items – physical goods – as they move through supply chains in many different businesses, both in the public and private sector. This also includes the tracking of assets, such as returnable assets (pallets, kegs, etc.) involved in logistics, tracking assets to ensure their pedigree (anti-counterfeiting activities) and to maintain service and support objects throughout their life cycle (such as TVs or railway engines).

2 GRIFS – Architecture and Standardisation

2.1 The core architecture

Figure 4.6-1 shows a comprehensive RFID system architecture.

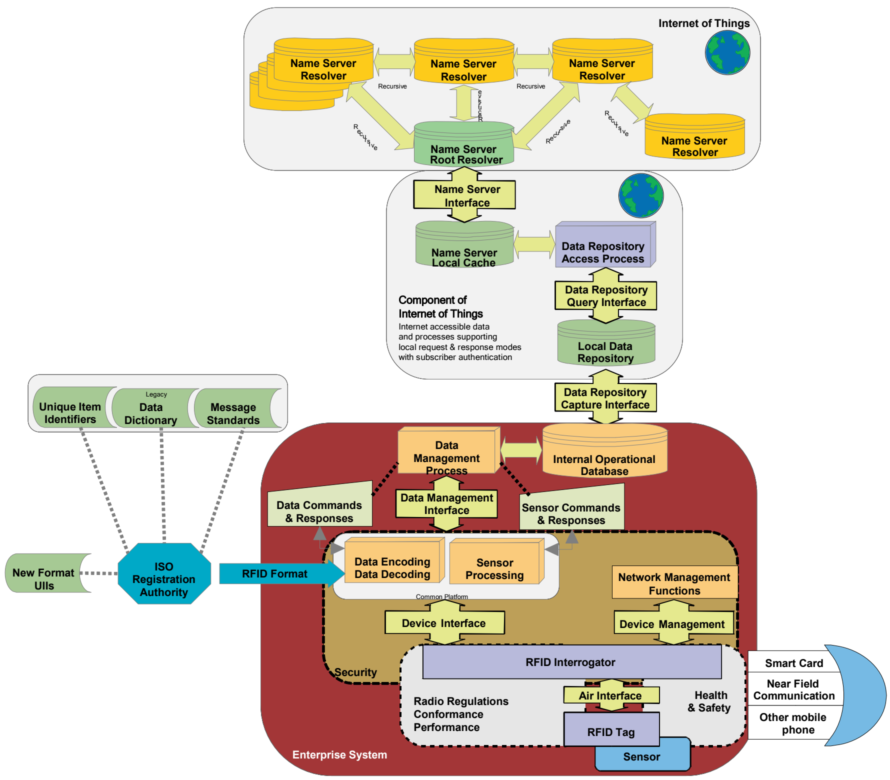


Figure 4.6-1: RFID system architecture.

The RFID system architecture as used for the IoT covers a significant set of standards that put together a comprehensive system architecture.

Within GRIFS the architecture has been sub-divided the architecture into four component parts:

- The enterprise system, dealing with all aspects where RFID as a data carrier is used to assist with some functional aspects of business or commercial operations.
- Internet-based data exchange components that are internal to the enterprise.
- Internet-based data exchange that is external with partners and other stakeholders.
- The ISO Registration Authority for data format that provides support for conversion legacy data and for new forms of unique item identifiers.

2.2 The network of influencing factors

A major part of the GRIFS project was to identify potential standards development areas where collaboration between standards development organizations could reduce some unnecessary work, and even reduce potential conflict between apparent overlapping work. To address this, a simple network model that has two major hubs has been developed. One of the hubs is RFID data capture, effectively dealing with technology aspects; and the other hub is RFID data process, effectively dealing with the information flow. Figure 4.6-2 identifies various developments that we consider might impact on the development of RFID standards.

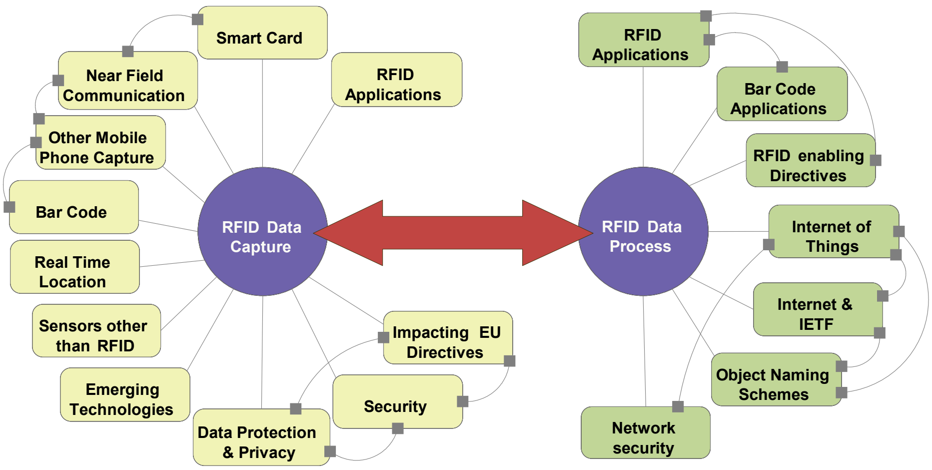


Figure 4.6-2: Network of influencing developments.

3 GRIFS conclusions

Within the GRIFS projects several conclusions have been made. The following points provide a brief excerpt:

- An RFID roadmap defined by the European Commission and developed in conjunction with European experts would provide a sound basis for creating some type of scorecard of areas of standardisation for benefit of European businesses and citizens.
- GRIFS provides a standardization map with managed updates in order to ensure quality and integrity of provided data.
- As there are many organizations involved in same technologies, a first version model of a network of influencing developments has been developed as shown in Figure 2.
- Intellectual Property is a key issue in most standard developments and could endanger adoption. Therefore it is recommended European Commission could take for any mandated application. This recognises the justification in applying FRAND principles for IP, but proposes some legal framework to ensure that EU support for the technology does not result in either vendors or end users being exploited.
- Data protection, privacy regulations and security needs high attention and it is expected that although basically not available yet, privacy enhancing techniques (PETs) to RFID technology will be developed.

- Air interfaces still do have different performance, however, a very important thing for the industry is to avoid parallel work in future.
- For some areas conformance and performance standards are still missing and cause interoperability problems or customer dissatisfaction. This gap has to be filled soon to ensure successful and wide deployment of the technology.
- Besides the ongoing development of the EPCglobal ONS system, there is still significant scope for resolving other types of URN over the Internet. It is essential that various applications that will require or benefit from participating in the Internet of Things have an early understanding of the issues.
- Although the capability of mobile phones being used for data capture purposes has little direct impact on RFID for supply chains, it could be a significant long term driver for the take-up of the technology and acceptance by ordinary citizens.
- Sensor technology will soon be part of RFID.

4 GRIFS standard database

A major output of the GRFIS project was the standard data base available under http://grifs-project.eu/db/, whereas the excerpts in this document present the status as of 15 December 2009.

The database covers multiple application areas and contains standards from a significant amount of publishers as described in 4.1 and 4.2 respectively.

4.1 Areas of applications

4.1.1 Mobile RFID

The potential to read RFID tags with mobile devices has always been possible in the industrial and commercial sector. In contrast, the use of RFID tags and mobile phones presents a possible exponential growth in the number of RFID data capture devices that will be available.

4.1.2 Real time location standards

A Real Time Location System (as defined in ISO/IEC 19762-5) is of a combination of wireless hardware and real time software that is used to continuously determine and provide the real time position of assets and resources equipped with services designed to operate with the system.

4.1.3 Security standards for data and networks

There are four zones in an RFID system where security features can be considered and applied.

4.1.4 Data exchange standards and protocols

Our definition of data exchange systems is intended to cover indirect communications between partners, usually through some hub mechanism. We exclude any direct peer-to-peer communication and any data exchange that can be implemented with in-house systems.

4.1.5 Environmental regulations (e.g. WEEE, packaging waste)

The Directives that are discussed in this section have some small direct impact on RFID, as will be discussed below. Their greater impact is on potential applications using RFID to implement the Directive or to assist in the management of systems associated with the Directive.

4.1.6 Application standards

The application standards of any data carrier technology are independent of the technology standards, but should use them as normative references. They are usually developed by a user body with expert knowledge of the sector being addressed by the application standard.

4.1.7 Data standards

The data standards address the way data is held in business applications. As such, they are associated with the data dictionaries developed by user organisations for encoding in various AIDC data carriers. In some cases, the legacy requirements of encoding in bar code need to be taken into account with encoding in RFID; in other cases, slightly new approaches can be adopted.

4.1.8 Data encoding and protocol standards (often called middleware)

The data encoding and protocol standards address the various types of communication between the RFID interrogator and the application, with the exception of not dealing with the device interface an

4.1.9 Device interface standards

The device interface standards and the data application interface protocol standard (see 7.8) are closely related.

4.1.10 Conformance and performance standards

There are two primary types of standard within this category:

Conformance standards are for evaluating whether a product fulfils the basic requirements to be able to work (interoperate) with other products.

Performance standards are for evaluation of certain properties and especially to provide a common way and method to compare different products.

4.1.11 Health and Safety regulations

There are two primary Health and Safety aspects associated with the use of RFID: Human exposure to EMF (Electromagnetic fields) and EMI impact on implantable medical devices.

4.1.12 Frequency regulations

The frequency regulations govern specific aspects of radio spectrum and permitted power for an RFID system or other radio communication system. Therefore, radio regulations – as they are commonly called – have a direct and indirect impact on the use of RFID technology.

4.1.13 Data protection and privacy regulations

There is significant confusion among the general public – and even legislators – about data held on an RFID tag and the ability to track individual people using the air interface protocol.

4.1.14 Air interface standards

The air interface standard primarily affects the components of the RFID system: the interrogator and the tag by defining rules for communication between the two devices. In particular, an air interface standard specifies physical layer and command structure.

4.1.15 Sensor standards

Often the term "sensor" is used in an imprecise and ambiguous manner. At one extreme this term includes RFID tags that only encode data; another accepts sensors correctly as being within the class of transducers and actuators but ignores significant differences in the means of communication from the sensor to the application and the topology of a sensor network.

4.2 Publisher

4.2.1 ETSI

ETSI is the European Telecommunications Standards Institute.

ETSI produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies.

Membership of ETSI is open to any company or organization interested in the creation of telecommunications standards and standards in other electronic communications networks and related services.

4.2.2 CEN

CEN is the European Committee for Standardization.

CEN works in a large number of sectors, in fact in virtually every area that the partner European Standards Organizations, CENELEC and ETSI, do not.

CEN's National Members are the National Standards Organizations of 30 European countries. There is only one member per country. Associate Members are broad-based European organizations, representing particular sectors of industry as well as consumers, environmentalists, workers, and small and medium-sized enterprises.

4.2.3 ITU-T

ITU is the United Nations agency for information and communication technologies. ITU-T is the Telecommunication Standardization Sector.

ITU is based in Geneva, Switzerland, and its membership includes 191 Member States and more than 700 Sector Members and Associates. The function of ITU-T is to provide global telecommunication standards by studying technical, operating and tariff questions.

4.2.4 IEC

IEC is the International Electrotechnical Commission (IEC).

The IEC charter embraces all electrotechnologies including electronics, magnetics and electromagnetics, electroacoustics, multimedia, telecommunication, and energy production and distribution, as well as associated general disciplines such as terminology and symbols, electromagnetic compatibility, measurement and performance, dependability, design and development, safety and the environment.

4.2.5 CENELEC

CENELEC is the European Committee for Electrotechnical Standardization.

CENELEC's develops electrotechnical standards.

The 30 current CENELEC members are national organizations entrusted with electrotechnical standardization, recognized both at National and European level as being able to represent all standardization interests in their country. Only one organization per country may be member of CENELEC.

4.2.5 ISO/IEC JTC1

ISO/IEC JTC1 is the Joint Technical Committee 1 of ISO and IEC.

The scope of ISO/IEC JTC1 is standardization in the field of Information Technology.

Note: Information Technology includes the specification, design and development of systems and tools dealing with the capture, representation, processing, security, transfer, interchange, presentation, management, organization, storage and retrieval of information.

4.2.6 ISO

ISO is the International Organization for Standardization.

ISO's work programme ranges from standards for traditional activities, such as agriculture and construction, through mechanical engineering, manufacturing and distribution, to transport, medical devices, information and communication technologies, and to standards for good management practice and for services.

Membership of ISO is open to national standards institutes most representative of standardization in their country (one member in each country).

4.3 Statistics of currently included standards

Table 4.6-1: Application areas.

APPLICATION AREAS	NUMBER OF INCLUDED STANDARDS
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

APPLICATION AREAS	NUMBER OF INCLUDED STANDARDS
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
TOTAL	**175**

Table 4.6-2: Publishers.

PUBLISHER	NUMBER OF INCLUDED STANDARDS (PUBLISHED)
CENELEC	5
Commission Decision	4
EC Directive	6
EPCglobal	13
ETSI	23
European Council Recommendation	1
ICNIRP	1
IEC	4
IEEE Standards Association	5
Information and Privacy Commissioner, Ontario, Canada	2
ISO	13
ISO/IEC	60
ITU-T	5
NFC Forum	2
The IETF Trust	4
The Internet Society	27
Washington State Legistlature, USA	1

4.4 RFID Standardization report

The comprehensive report demonstrates the broad scope of the current state of RFID standards on a global scale and highlights the need for more co-ordination between key standard organisations.

The report, produced in the frame of the WP1 led by CEN, provides an inventory of global RFID standards and identifies all RFID-related standards organisations, the geographical and technical scope of their work, and the opportunities and risks of collaboration, including gap/overlap analysis. The scope of the report focuses on the use of RFID in the supply chain including the tracking and tracing of physical objects.

The report's conclusion highlights the need for a significantly greater amount of co-operation between RFID standards development organisations, particularly in the areas of universal identification, security and high frequency standards that are increasingly used on products but that also use smart cards and mobile phones for transmission.

The report is available at http://www.grifs-project.eu/index.php/downloads/en/

5 GRIFS MOU and GRIFS Forum

The MoU serves as basis for the formation of the GRIFS Forum. It is important to note that the current draft MoU is not a definitive document but a work in progress still needing the stakeholders' inputs. The current draft is largely inspired by the famous MoU on Electronic business between IEC, ISO, ITU & UN/ECE.

The core principles contained in the MoU are a strong commitment from the involved standards organisations to collaborate and share information while respecting each other's organizations and existing standards development processes. Another important principle is the involvement of the users community and the priority to meet their needs and answer their concerns.

The Forum is an informal organisation which generates consensus based recommendations on RFID standards to existing standards development organisations. They would implement them using their own standards development processes.

The MoU and the Forum are highly appreciated by the European Commission and Gérald Santucci, Head of Unit, Networked Enterprise & Radio Frequency Identification (RFID), DG Information Society and Media of the European Commission confirmed this with a foreword in the August 2009 GRIFS Newsletter:

"I congratulate the GRIFS partners for their recent achievement of a Memorandum of Understanding which identifies clear objectives and lays the groundwork for increased cooperation through a Forum between standardisation organisations in the RFID field. Today more than 250 standards describing RFID-related solutions have been established by around 30 different organisations. It is therefore essential that standardisation organisations cooperate with a view to leveraging economies of scale and economies of scope. In line with its earlier communication, the European Commission is willing to promote the interoperability of RFID standards across national and regional boundaries as well as across different economic sectors. In the fast-evolving world of RFID, every single standardisation organisation should be able to rise above the narrow confines of its interests to the broader needs and expectations of the whole user community.

Over the past two years, GRIFS has been on the front lines of a global effort to achieve that aim by enabling the emergence of consistent and interoperable RFID related standards. The European Commission praises the GRIFS consortium for its hard work and great deal of promise as it is clear today that the Forum will offer a great opportunity to advance interoperability of international RFID standards, while never duplicating but always complementing and synergizing the works being done in other relevant bodies. Such a cooperative strategy is most necessary to enable faster take-up and adoption of RFID within and across the various supply chains."

The text of the MOU is available under

http://www.grifs-project.eu/data/File/GRIFS_MoU_Version1%201.pdf

4.7 Developing and Piloting the Next Generation of Networked RFID Systems

BRIDGE Project

M. Harrison, A. Brintrup, T. Sanchez Lopez, M. Tomasella, D. C. McFarlane

Institute for Manufacturing, Department of Engineering,
University of Cambridge, UK

Abstract: In this chapter we review the BRIDGE project (2006-2009), which provided significant contributions to RFID technology and implementation in Europe. The project aimed at enhancing RFID and its use in Europe through comprehensive development that hindered RFID technology at the start of the project. The project conducted research in frequently used reasons for non-deployment, such as the high cost of readers or tags, lack of secure frameworks, case studies. State of the art technology such as Discovery Services and Track and Trace analytics were the result of the project as well. Business work packages tested technology developed in the technical development clusters; and investigated how RFID technology could enhance business operations and provide monetary value, serve customers better, and increase competitiveness. As a result of the project, practitioners in Europe have a better chance of successful deployment through improved and novel hardware and software technology supported by a set of case studies; and researchers have a set of research questions that shall be studied to help European organisations reach the full potential in using RFID. This chapter reviews developments in various work strands of the projects, poses key lessons learned and questions for the future.

1 Building Radio Frequency Identification Solutions for the Global Environment (BRIDGE)

The BRIDGE project has played a leading role in envisaging, designing and prototyping the next technology developments required for achieving the potential of networked RFID. Furthermore, BRIDGE developed business support for RFID implementation through a number of case studies, looking into implementation strategies and the operational value of RFID. A fitting example of synergy between technical development and business value is that of design work on Discovery Services for locating multiple sources of information for a specific object. The work strand has already made significant contributions to standardization activities in this area and the working prototype is already being used and was evaluated within the Sony Europe pilot for products in service; showing clear business value in terms of reduced effort in product recalls, and inventory counts, reduced environmental impact through paperless warranty. Another example is the track and trace analytics framework for extracting meaningful business value from the large volumes of data that can be produced by Auto-ID technology. The framework can be used for end-to-end tracking, gathering all relevant event data, automatically following changes of aggregation or containment, then automatically building configurable maps of supply chain networks and learning flow patterns from historical data, in order to predict when and where objects should be seen next and raising alerts when problems or deviations are likely to arise. Such frameworks can be used to monitor delays, shrinkage and can also be extended to specific applications, such as detection of counterfeits within the supply chain. The technology has been tested in the pharmaceutical traceability pilot, which has produced particularly interesting and extensive data for analysis using such tools. The technology resulted in a traceable pharma supply chain, and reduced the manual time and effort dedicated to securing the pharma supply chain through automation.

BRIDGE's structure also allowed cross- work package collaboration and the merging of developed technology. For instance, the security work package worked together with the Discovery Service work to allow seamless integration of technology in the future. The security work has made significant progress on the development of trusted tags and readers to address the privacy implications of using RFID technology, while also developing a comprehensive approach to an access control framework that can be used to protect the confidentiality of information stored in distributed event repositories and also links within Discovery Services, with a very high level of granularity and flexibility. Taken together, many of the technological developments of the BRIDGE project will surely have a lasting impact in extending the architectural design for networked RFID beyond data capture and bilateral information exchange.

Over the three years of the BRIDGE project various business work packages have been dedicated to innovative applications of these technologies to real world problems to highlight the potential of RFID in Europe. The Manufacturing pilots at Nestle and COVAP examined the use of networked RFID in leaner production, quality control, inventory management, automated control and manufacturing resource maintenance, providing practitioners with case studies, business case guidelines and simulation based analysis frameworks. The products in service pilot at Sony looked into paperless warranty and item level traceability. Textile retailers such as Kaufhof, Northland Professional and Gardeur used the technology to enable smart dressing rooms/shelves, to improve inventory checking and in-store visibility of garments. Carrefour utilised RFID for management of reusable assets and inventory management at item-level. As a result, these companies have developed long term visions for using networks of things to improve their business.

To make the technology more accessible to a wider audience, BRIDGE has made considerable efforts on education and dissemination with the development of training material as well as awareness tools to explain the technology. The team held a number of public webinars, provided regular updates through the widely distributed BRIDGE newsletter and presented at relevant conferences and industry events, including dissemination workshops that BRIDGE has initiated. Wherever possible, work strands have tried to issue public deliverables to ensure that the results reach the widest possible audience.

An overview and scope of the BRIDGE work structure is shown on Figure 1. The technical work groups performed research and development aiming to advance the state of the art of the technology while in a number of cases the results of this work were used by the business groups in their pilots.

BRIDGE technologies have applications not only within a business-to-business context but also within a wider Internet of Things embracing active participation also by citizens: for example, secure Discovery Services can complement existing web search engines by allowing contributors of information (e.g. ratings, reviews, photos, video etc.) to effectively link to locations and products, to enable their content to be discovered not only within the public domain but also within more restricted communities and interest groups.

In what follows we outline the achievements of different work strands (Section 2), discuss how the project enhanced European operations with RFID and present an outlook into the future state of RFID in Europe (Section 3), and conclude our findings (Section 4).

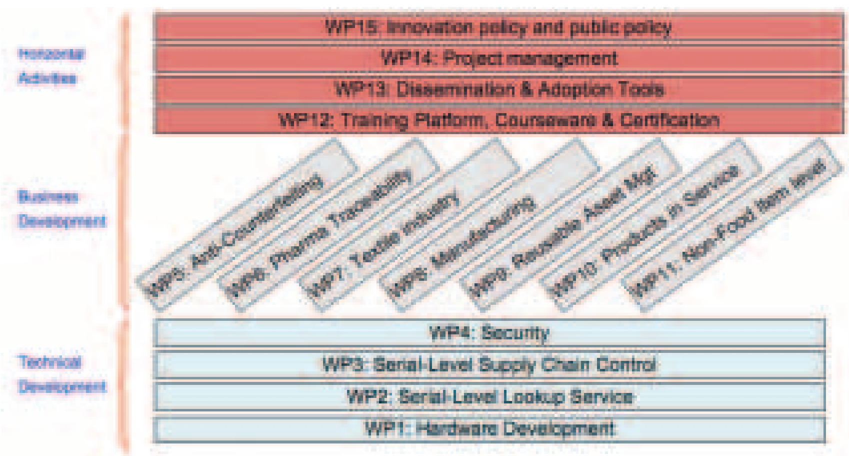


Figure 4.7-1: Work package clusters in the BRIDGE project

2 BRIDGE work strands: achievements and outlook

In this section we highlight the main achievements and developments in each of the work packages.

2.1 Hardware development

WP1 has worked to advance the state of the art of RFID hardware. The goal was to develop:

- New RFID tags: more versatile, sensor-enabled, smaller and cheaper, suitable for use with metals and dielectric objects
- New RFID readers and reader antennas: improved performance and lower cost
- New RFID systems to prototype some smart object environments

In the field of sensor-enabled tags, an initial benchmark study investigated the different technologies, standards, and user requirements. This was compiled into a Handbook for Sensor-enabled RFID that reduces the learning curve for any company seeking to develop this kind of tags. Next, a design effort developed a common platform, proposing operation modes, data management procedures, and protocol extensions to build modular sensor-enabled RFID tags. Finally, some multi-sensor tag prototypes were built based on the proposed common platform.

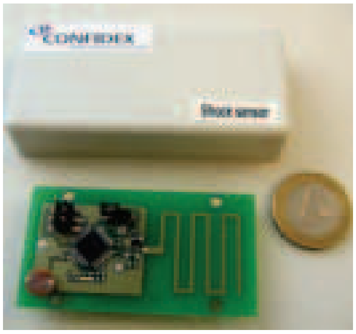


Figure 4.7-2: Prototype of a sensor-enabled tag, compatible with the EPC Gen2 protocol

In response to a high market demand for smaller tags several techniques where investigated for tag miniaturization, from fractal antenna shapes to use of different materials. Finally, a tag with a very high read-range to size was designed, borrowing a concept from meta-materials research: the Split-Ring Resonator (SRR). Tags for metal and dielectric material were designed using the same principle: isolation from the material but with a minimum thickness to keep the tags conformal to the shape of the tagged objects. This has been a very competitive field of research, in which industry has come up with high performance designs. BRIDGE WP1 has contributed a very thin design based on a double bow-tie resonator.

To design a low-cost RFID reader, two different research approaches were followed. The first prototypes in the industry based on specific RFID reader chipsets were designed and prototyped, forecast to reduce costs by 80% versus current market prices. Additionally, we attempted to reduce the price of the RFID chipset itself by designing it using common CMOS processes, rather than using a different process for the RF and the digital parts of the chip. This promises cost reductions of at least a factor-of- ten.

To improve the performance of readers, BRIDGE research focused on the reader antennas. First a novel design of a phased array antenna was tested, improving the read rates of static constellations of tags. It is well known that moving tags are easier to read since multi-path cancellation blind-spots tend to be static. When tags are static, the phased array reader antenna moves the beam slightly, and randomly, moving the multi-path blind spots, and thereby increasing the readability of large constellations of static tags.

Next another difficult RFID problem was tackled: the metallic shelf. The smart-shelf concept, in which the shelf is aware of its contents, is an old RFID paradigm that has faced difficulties in practice since most shelves in use today are metallic and no reliable, robust, and economic way had been found to equip such shelves with RFID antennas. To address this, a specific design based on slot antennas was prototyped and successfully tested in a live retail environment, producing 100% read rates over a full month of testing. In this test, multiplexing was used to reduce the total cost of equipping a supermarket with RFID antennas used on metal shelves.

Finally, a more theoretical research was conducted, with the goal of pushing the limit of how many tags a reader can read each second. This number is limited by the anti-collision protocols. Since all tags communicate with the reader using the same protocol, the reader can only communicate with one tag at a time, and needs to employ a multiple-access strategy, similar to those employed in other one-to-many networks, to resolve collisions. The use of Blind Signal Separation (BSS) algorithms was shown to allow a single reader to communicate simultaneously with up to four tags. For this, readers would have to be equipped with at least four RF front-ends. Each of these receives a different mix of the signals from the four tags. The role of the BSS algorithm is to separate the response from each individual tag. Once this is done, the reader can also communicate back to the four tags simultaneously.

The third area of research demonstrated the use of RFID for building smart-object systems. First, the smart-shelf prototype was equipped with algorithms to use the RFID antennae to manage a stock of books in a store, locating them precisely on the shelf, sending out-of-stock alerts, and producing lists of misplaced items. Second, the smart-object paradigm was applied to the remote servicing of heavy equipment and industrial assets. For this a lab prototype of a washing machine was built, making use of RFID readers and sensors to detect malfunction (over-heating, vibration, water leaks), misuse (wrong washing program for the clothes in the load), use of non-original spare parts, as well as sending warnings when specific parts needed servicing or replacement. A web-based platform was developed to remotely control all of these functions, demonstrating how RFID could dramatically improve the quality and efficiency of the management of a large and geographically disperse fleet of machines (washing machines, vending machines, vehicles, agricultural and mining equipment, etc.).

In summary, BRIDGE research has helped advance the state-of-the art of RFID hardware with a set of prototypes ready for industrialization; promising concepts that require further research in the laboratory; and with some theoretical results. Some of these deliverables will be patented and some will be exploited commercially.

2.2 Serial level lookup services / Discovery Services

Here the focus was on the design and prototyping of a Discovery Service, one of the missing elements of the EPCglobal Network architecture, namely network services for finding source of information about individual objects within open supply chains. This role is complementary to EPC Information Services (EPCIS) and the Object Naming Service (ONS) functionalities; EPCIS provides a standard mechanism for exchange of serial-level information between parties who already know the addresses of each other's EPCIS services, while ONS currently provides a class-level lookup service to indicate authoritative resources, such as those provided by the manufacturer or issuer of the identifier. Discovery Services allow multiple entities to create a link between a specific unique ID and their information resource in order to indicate that they hold information about that ID to clients who query Discovery Services. Because the relationships indicated by such links can reveal commercially sensitive information about volumes and flow patterns of goods, authentication and access control are key aspects of Discovery Services that are not required for ONS query clients nor specified in the existing EPCIS standard.

Discovery Services are a key enabler for track and trace applications with a tremendous potential impact on supply chains especially in highly regulated sectors like food or pharmaceuticals, where traceability information can improve safety for consumers. They also have great value for developing the Internet of Things, as networked nodes (e.g. information resources, devices, smart objects, sensors and actuators) would need to announce themselves and discover other nodes for sharing capabilities, resources and services.

An initial survey with potential users was launched for a four month period. Results revealed a lack of confidence with open supply chain models and concern about sharing information without knowing exactly who would later on access information from Discovery Services. These concerns became the main requirement for Discovery Services and led to minimising the amount of information stored about each resource; Discovery Service basic records would include only pointers to sources of information enabling whoever uses this service to discover the source address, but not releasing detailed information, thereby enabling each company to control access. This early principle was further enhanced in collaboration with the security work package, resulting in the development of a security framework for EPC Network, including EPCIS and future Discovery Services.

A number of design models were evaluated, considering issues such as latency, performance, access control and security as well as ability to link to multiple kinds of resources - not only EPCIS services. In one design, a Discovery Service acts as a proxy, forwarding queries down to resources, allowing ad hoc access control decisions. However, aside from security another important requirement for Discovery Services is the ability to provide synchronous responses to queries, which is difficult for this kind of model. Therefore, a synchronous model, the directory of resources, was selected as the first candidate for prototyping, using Web Services technology and LDAP as the search engine and repository.

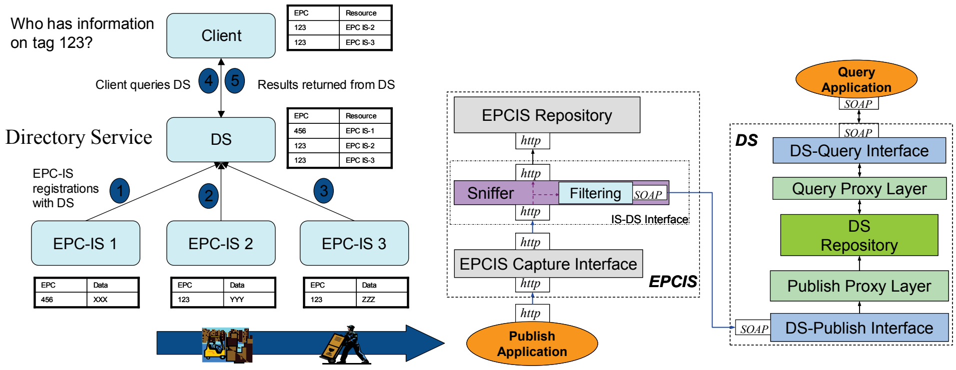


Figure 4.7-3: Directory of resources model. Right: Discovery Service prototype components, integrated to Fosstrack open source EPCIS implementation

This prototype was developed and deployed, and today is in operation and accessible to BRIDGE members for trials, further development and integration with the security framework developed within the scope of WP4. In addition, the Discovery Service prototype source code is being distributed under a Lesser General Public License (LGPL), in order to increase interest from the research community. Various organizations have shown interest in the BRIDGE prototype of Discovery Services including BRIDGE members such as GS1 France, SAP, BT, Bénédicta and Sony and also external parties like Afilias, GS1 Norway and even other EU projects like iSURF led by Intel. For usability purposes, demo applications for publishing were developed together with the open source software.

The group has communicated its work to other research groups and projects and pro-actively contributed its work to standardization activities on Discovery Services within GS1 EPCglobal and the IETF. Members of the BRIDGE team have taken a leading role within the EPCglobal DD JRG to develop a comprehensive user requirements document and it is expected that a technical work group for discovery services will be chartered within GS1 EPCglobal before the end of 2009 and that members of this work package will continue to play an active role in the development of open and extensible technical standards for Discovery Services and related services that are so important for the Future Internet and Internet of Things.

2.3 Serial level supply chain control / Track & Trace Analytics

Although Discovery Services are a useful architecture component for enabling improved supply chain visibility, they are not fully fledged track and trace applications and essentially answer two very simply low-level query criteria, namely:

- where can I find information about this EPC?
- notify me of any additional future providers of information about this EPC?

The work was designed to be complementary to the previous work package, leveraging the Discovery Services work but bridging the gap to provide support for more business-friendly queries about track & trace and supply chain control, while leveraging the benefits of being able to follow individual uniquely identified objects as they move through supply chains or product lifecycles, without requiring business users to know the details of how to interact with EPCIS repositories or Discovery Services.

The first work package deliverable, "Serial Level Inventory Tracking Model", described how to gather event information from across a supply chain, taking into account the need to follow changes of aggregation. We then described how to use this event information with machine learning techniques such as Hidden Markov Models in order to learn the characteristic flow patterns, to answer questions not only about where an individual object was last observed but also predict when and where an individual object is at the current time or future times, based on its previous observation history and the learned flow patterns. Using these probabilistic algorithms it is also possible to give a confidence level about whether an object is likely to reach a particular location by a specified time. This is clearly useful for being able to predict whether ordered supplies will arrive in time for a particular production schedule, as well as for monitoring that manufactured goods are likely to reach specific customers by particular deadlines - or whether there is any need to intervene.

The model may appear as a rather abstract mathematical model for predicting flows of individual objects within supply chains. We therefore took the decision as a work package to develop a working software prototype of a modular Track & Trace Analytics Framework, so that it could be available for use by the business application work packages, for monitoring their supply chains. At the lowest level of the framework, an Event Gathering Layer interfaces with the EPC Network architecture and makes queries or registers standing queries with Discovery Services and EPCIS repositories in order to gather all the available event information about an individual object from all resources across the supply chain. Furthermore, we recognised that as objects move across supply chains or throughout their product lifecycle (including the usage phase), there can be significant changes of aggregation, such as when raw materials and components are embedded within products, which in turn are aggregated into cases, pallets, totes and vehicles for distribution and storage. Conversely, in a number of sectors such as the food or chemical industries, large volumes of bulk product are manufactured and later broken down into smaller packages for use. The team developed techniques for automatically following changes of aggregation, to ensure end-to-end tracking, where necessary switching to tracking a different identifier, such as the identifier of the pallet, vehicle or the identifiers of multiple products that were broken down from the original bulk product.

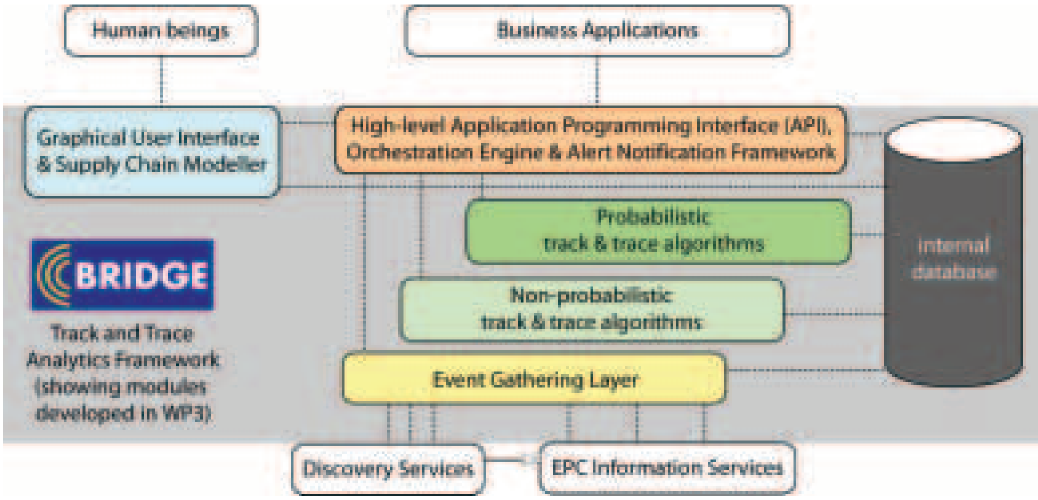


Figure 4.7-4: Conceptual diagram of Track & Trace Analytics Framework

Having gathered the event information, it is necessary to build a model of the supply chain in order to make sense of the movements of the objects. A Supply Chain Modeller was developed, which was able to analyse the received event information and automatically construct graphs of nodes and transitions between those nodes. Further manual refinement of the models is also enabled through the provided graphical user interface.

Track and trace algorithms (both non-probabilistic and probabilistic) were developed in order to learn flow patterns, filter out false positives and false negatives and provide predictions and probability estimates about where an object is now, which path it is likely to have taken and where it is likely to be in the future.

Finally, the modules were integrated and tested using real-time event information from the automation lab in Cambridge, tracking the movement of autonomous shuttles moving around a conveyor track. We also used the track & trace analytics framework to analyse data from the pharmaceutical traceability pilot of BRIDGE.

Deliverable 3.2 on the software prototype was completed at the end of 2008 and the final six months have mainly focused on completion of the contextual models, which examine how such a Track & Trace Analytics Framework can be applied to improve manufacturing processes and traceability, assist with the management of reusable assets (in particular, returnable transport items such as pallets, roll cages, trays, reusable plastic containers, beer kegs etc.) and how it can be further extended to support sensor-based condition monitoring as well as alerting and notification about operational problems within supply chains, such as monitoring of delays and shrinkage, probabilities of non-arrival of goods or supplies or detection of unusual or suspicious flow patterns. Based on the analysis within various deliverables of real-world practices, a number of additional high-level algorithms have been developed as proposal for extension of the Track & Trace Analytics Framework. In addition, an alerting and notification framework has been designed, to support high-level alerting about operational problems within supply chains that are detected using the track and trace analytics framework.

2.4 Securing Collaborative Supply Chain Networks

The security work package operated technical research tasks on both hardware and software security and have performed requirements surveys, interviews and case studies, along with the publication and dissemination of results to both ISO and EPCglobal standards activities.

The tag security research has concentrated on providing an asymmetric cryptographic capability of the tag that can be used to extend the ISO/IEC 18000-6c/EPC Gen 2 protocols to support a wide number of security operations for different scenarios. The work package has analysed different cryptography schemes to select one that requires low silicon area, has low power demands and fast computation. This enables the costs of the tag to be kept low and the performance maintained. The group also examined the potential to perform Side Channel Attacks (such as power analysis) to break such secure tags and recommended to tag developers to consider such attacks in their implementations.

Using the secure tag capabilities the group has implemented a number of security operations including pseudonym schemes and authentication commands. The authentication command has been implemented by two tag manufacturers, and the resulting anti-cloning tag has been demonstrated in an anti-counterfeiting demonstration with the addition of an authentication client, back end authentication server and EPCIS repository for results. WP4 has also produced a prototyping tag that allows researchers to experiment with new cryptographic capabilities and commands. Finally, the tag security research has worked with ISO to start a security working group to standardise the way that secure tags can advertise their capabilities.

The second hardware area involved the development of a Trusted Reader. This has involved developing a new reader control board incorporating a TPM (Trusted Platform Module), along with a software stack to secure the integrity of the operating system and allow multiple parties to instantiate secure local services on the reader. WP4 has shown how the Trusted Reader can offer many advantages to different tag authentication methods, and devised a scheme for controlling the distribution paths of goods using the Trusted Reader to check and authorise the shipment along supply chain paths.

In the area of software security the focus was networked services for inter-company operation of supply chains. A framework of components for access control and access control policies was developed and implemented in the Discovery Service prototyped in BRIDGE. The group also looked at how critical business information can be leaked through raw RFID events and proposed methods to manage the information release. The problem of introducing previously unknown parties within the supply chain and how this can be achieved using the Discovery Service or through other techniques was also considered. Where relevant the work package has shared information with the EPCglobal Joint Requirements Group on Data Discovery.

Whereas access control is mainly about confidentiality, the group looked at the problem of information integrity, which is critical to inter-company operation. Each organization has to be able to trust the data from its peers in order to be able to operate the joint processes. The economics of the problem of information sharing were examined. Technically the group demonstrated the use of visualization to detect integrity problems (either in the information accuracy or in the process itself), along with the use of automated integrity rules checks.

2.5 Anti-counterfeiting

Counterfeiting and product piracy constitute a serious and ever growing problem against legally run businesses and owners of intellectual property rights. Counterfeiting is not specific to any industry but it affects a large number of sectors such as music, software, luxury goods, pharmaceutical, automobile, fast moving consumer goods, and toys. According to the International Chamber of Commerce, "counterfeiting and piracy are growing exponentially in terms of volume, sophistication, range of goods, and countries affected - this has significant negative economic and social impact for governments, consumers and businesses [...]."

The potential of RFID and the EPCglobal network in enabling novel anti-counterfeiting and anti-fraud techniques is well recognised. Even though it seems that there will not be one silver bullet solution against illicit trade, industries and academia see mass-serialization among the most promising single countermeasures. There are two major reasons for using EPCglobal network technology in anti-counterfeiting: First, RFID allows for new, automated and secure ways to efficiently authenticate physical items. Second, as many companies invest in networked RFID technology for various supply chain applications, the item-level data will be gathered in any case – so why not using it to detect counterfeit products?

This work strand of BRIDGE developed anti-counterfeiting techniques for EPC/RFID-enabled supply chains. The solution concepts and prototypes are based on a thorough requirements analysis and they leverage the visibility that the technology provides. Different solution approaches have been studied, developed and demonstrated, including: (i) Tag authentication based on unique transponder ID (TID) numbers; (ii) Synchronized secrets approach that detects if two different tags enter the supply chain with same ID numbers; (iii) Rule-Based Anti-Counterfeiting approach that offers a flexible anti-counterfeiting toolkit which allows users to specify conditions that indicate evidence of counterfeits (iv), and statistical track and trace analysis techniques to detect cloned tags automatically from RFID traces. All the studied and developed approaches represent different possible security measures that enable detection of counterfeit products in supply chains.

The team also investigated the business cases of the studied solutions. When RFID technology is deployed not solely as an anti-counterfeiting technology but also for other purposes, as examined in BRIDGE, not all hardware and tagging costs need to be allocated as anti-counterfeiting costs. However, putting numbers on the benefit side of an anti-counterfeiting business case is extremely challenging. Consequently, the team investigated the value of security in anti-counterfeiting and provides an explanatory model for the benefit side of an anti-counterfeiting investment.

To support affected brand owner and manufacturing companies across industries, the team also produced application guidelines and an implementation roadmap for EPC/RFID based anti-counterfeiting measures. These cover selection of the right security measures, selection of the right supply chain locations for the checks, and steering an anti-counterfeiting system deployment project.

2.6 Pharmaceutical traceability pilot

The pharmaceutical traceability work package implemented and piloted a fully operational drug product tracking system using the EPCglobal network for supply-chain wide data collection and using GS1 Data Matrix symbology on all levels of product packaging, including for the first time, item, bundle, case, pallet and vehicle. The pilot proved to be exciting and innovative on an international scale; since no other project, to our knowledge, has designed, installed and successfully operated such a comprehensive system of Track, Trace and authentication within the 'real' pharmaceutical supply chain in the world. The pilot featured RFID tags at case and pallet level in hybrid labels (with printed bar codes). Some pallets were also fitted with active RFID tags to enable GPS tracking across national borders and shipping routes. This use of interoperable RFID and printed bar code carriers should set an example to all of how such a practical system can function successfully in the real world.

The adoption of the four string data structure, as originally used in the Irish Haemophilia Trial of 2006, was very forward thinking. This structure is now being used by EFPIA as part of its European vision, in Turkey for its new reimbursement system and being considered by California and FDA in US and it may yet become the blueprint for the first globally accepted data structure used in the pharmaceutical industry at item level and beyond.

The serial number element that forms an integral part of the data structure ensured that every single pack of each product being tracked had a unique serial number associated with it. Using this and the process of aggregating the contents to unique serialised packaging the team were able to provide full traceability of a single item from the packaging line, throughout the distribution supply chain to the precise delivery point at the hospital pharmacy and to every associated packaging type along the entire supply chain.

Full use was made of the EPCIS standard and GS1 standards including the GLN (Global Location Number), GRAI (Global Returnable Asset Identifier) and SSCC (Serial shipping container code) numbers for locations, shipments and physical assets as part of this pilot. Linking these GS1 number formats to data carriers such as Data Matrix, GS1-128 and RFID tags and data structures has expanded the knowledge and use of how to integrate these 'tools' into a fully functioning solution. The selection and use of a range of different printing technologies, substrates, line speeds, various types and sizes of container or pack added to the comprehensiveness of the project.

Choosing to work with both original pharmaceutical packers/manufacturers as well as a contract packer allowed the team to test the two most common routes into pharmaceutical supply chains. The choice of generic manufacturers who in general operate at lower margins and higher line utilization rather than branded product (so often used in pilots and trials), also added significantly to the worth of the project.

All of the product and event data was collected locally and then passed via the Internet to the respective EPCIS database (a partial implementation of the EPCglobal Network) created for each of the nine user companies involved. Where possible the team chose different methods of processing data for similar operations in order to compare their functionality and practical application; for example, the dual process for the receiving of the pallets, using either manual scanning of barcodes or an RFID portal to read the pallet tags as the goods-in operator moved the pallet through the portal using a forklift truck. The data collected from these operations was then compared to ensure that both were operating correctly. Mobile technology to scan codes at various ‘remote’ locations was deployed, proving highly successful and adding to the experience and learnings from the practical use of complex code carriers such as GS1 Data Matrix where hardwired or other traditional solutions would have been difficult or impractical.

During the pilot, events were recorded and linked with pre-published master (product) data. This provided the necessary flexibility to enable the support of a number of different applications - not only to enhance patient safety but also to improve supply chain efficiency: the ability to determine the whereabouts of products in the supply chain for speedy recall; the ability to integrate data into back-office applications such as inventory management for better stock utilization with expiry date management and financial reconciliation (e.g. goods received data matched with supplier invoices); as well as the ability to identify non-authentic or non-authorised products.

In summary, this work package demonstrated a practical, workable solution for mass serialization for track and traceability of pharmaceuticals in the open supply chain.

2.7 Supply Chain Management in European Textile Industry

The focus of this work package was the textile supply chain. Its objective was to examine the feasibility of EPC/RFID technology in the textile industry and to develop the adapted RFID technology for successful implementation. Work was conducted by analytical and empirical studies to identify potential RFID opportunities in supply chain processes taking various factors into consideration. The work consisted of five steps:

Market Analysis: As preliminary work we analysed the European textile market to identify the main problems and challenges in the textile industry, the main developments in this market and the opportunities for EPC/RFID technology to optimise existing processes. Nowadays, significant changes can be observed in consumer behaviour, distribution channels and retail structures. Due to increasing competition, price pressure and labour costs, companies are examining opportunities to save costs, e.g. by reducing manual processes, reducing out of stock situations and increasing the visibility of the supply chain.

Requirements Identification: As a second step, the necessary technical requirements for selected use cases and for an RFID implementation were examined. RFID applications could be introduced at the Distribution Centre or the store, in the receiving or outgoing area, in the front or back store, on smart shelves or in dressing rooms. All these applications require different systems and set ups. Different hardware solutions are required, e.g. mobile devices vs. fixed gates, number of tags, antennae and printers.

Business Cases: Business cases for an SME supplier, a department store and a hypermarket were analysed, considering company type, articles and labour costs, to determine the amount of investment, the amortization time and the return on investment.

Empirical Study: The actual state of the textile market combined with the technical requirements and business cases led to the fourth and final part of work: an empirical study using three pilots. The following pilots were conducted:

- Northland pilot: This Austrian manufacturer of outdoor clothing wanted to find out to what extent an RFID inventory process was more effective than a manual inventory. The trial took place in a showroom where the Northland team tagged more than 300 articles to conduct their inventory. They obtained very significant improvements in time saving and accuracy of the inventory, with a reading rate of nearly 99% and an reduction of time for inventory checks by a factor of 20.
- Gardeur pilot: This SME manufacturer of men’s clothing wanted to gain a better understanding of consumer behaviour within the retail sales area and discover how often customers were taking each piece of clothing into the dressing room, how many trousers were ac-

tually sold, at which moment in time the articles were available on the sales floor, etc. Gardeur benefited from more detailed visibility of their flow of merchandise on the sales floor and used this information for planning purposes.

- Galeria Kaufhof pilot: This pilot was carried out in a department store from September 2007 to December 2008 and focused on the customer attitude towards customer-oriented RFID applications. The Gardeur shop within the Galeria Kaufhof store in Essen was equipped with smart shelves, smart dressing rooms and a smart mirror, each equipped with displays to show RFID enabled product information to the customer.

All three pilots were evaluated by a customer survey. Over a period of three weeks, more than 250 customers were interviewed (50% men / 50% women). In general, customers accepted RFID applications and evaluated them as a big advantage regarding their personal shopping experience. 56% and 49% of all respondents appreciated and accepted the smart shelf and the smart dressing room as an informative tool and a useful improvement for their selection of a product. All three pilots – regardless of the structure or size of the company - showed positive results which is highly motivating in terms of further implementation of RFID applications. Nevertheless each company decided they need to investigate their own processes to figure out their potential and to check if RFID is the right technology for their objectives. Following the pilots, this work package produced a set of step-by-step guidelines with the aim of answering frequently asked questions regarding the technology and giving interested companies reliable guidance about how to execute and implement an RFID project in the textile sector.

2.8 Applications in manufacturing

The manufacturing work package aimed to develop tools and methodologies to help organizations give effective decisions on RFID implementation. Implementing RFID within a manufacturing plant requires extensive analysis and experimentation. Resulting from this observation the BRIDGE team developed industrial guidelines for problem and requirements analysis, business case and pilot preparation, using case studies from our application partners: Nestle UK and the Spanish cooperative COVAP. The team devised an exemplary systematic approach to investigate how and where RFID can be used, how priority areas can be detected using Value Stream and UML based analysis, how a business case can be developed and lean manufacturing based value drivers be identified, and finally, how requirements relating to hardware, software, human factors can be drawn, and planned for.

State of the art in literature shows either overly complex analytical models or overly qualitative benefit claims often from RFID consultancy companies. Furthermore, existing modes of analysis are often supply chain focused. As a result manufacturers are in need of reliable decision support methodologies that enable cost effective and time effective expedited testing of alternative solutions. Within this respect the team reviewed current trends in decision making and simulating RFID implementations, and made the case for simulation as a decision support mechanism in RFID implementation. They argued that using the lean manufacturing analogy, practitioners could find as-is and to-be manufacturing waste to be an effective means of analysing the impact of RFID in their operations. Consequently, the team proposed a simulation model where input parameters consist of physical and information flows of the manufacturing process under consideration and output consists of waste reduction what-if analysis. The simulation approach was tested with two industrial case studies: Nestle UK Intermediate Bulk Container Management (IBC), and COVAP Iberian Ham Manufacturing. Both of these processes showed potential in achieving a leaner mode of operations through reduction of different waste types.

A major goal and focus of this work was the development of a successful manufacturing pilot. This goal was achieved and a ham traceability application was created in just 6 months. The Iberian ham is a delicatessen product, manufactured through a highly handcrafted process that lasts three years. COVAP aimed to increase item level traceability at each stage of the manufacturing process, automating inventory counts and manual information records. Due to challenging process conditions such flaming, washing, and greasing, we needed a carefully designed tag encapsulation. Extensive testing pointed to the use of UHF Gen2 tags at three fixed and two mobile read points to ensure the highest read rates. The first mobile read point was used for product classification according to animal feed, weight, origin, and pH levels, whereas the second mobile read point is used for batch scans when products move between different cellars that simulate seasonal conditions. The rest of the fixed readers tracked inventory and work-in-progress.

COVAP developed the ham traceability application to interface read events with its information system, and aims to explore the use of EPCIS and further extend the pilot into its supply chain. After the three years when manufacturing process lead time is complete, the company is intrigued to examine the correlation of various product and process data such as feeding and weight, as well as maturation times in different cellar conditions, with the end product quality. It is envisaged that in addition to a leaner operating environment, and increased traceability, the RFID set up will also enable process innovation through the gathering of statistical data.

The work strand has not only provided comprehensive guidelines to manufacturers for finding value in RFID and implementing an RFID based solution, but also showcased a successful pilot to validate these guidelines.

The scope of this work was to improve reusable asset management in the supply chain, and to evaluate, measure and propose how a secure track and trace solution based on GS1 EPCglobal standards can improve the management of Reusable Transport Item (RTI) between the trading partners. The work consisted of five tasks:

Market analysis: The first task analyzed the current situation regarding asset management in the supply chain, providing a foundation for development of the project requirements and solutions, since it defines its domain objectives and context. A survey analyzed the behaviour of industries regarding assets management in Europe, allowing for complete description of the two management models that exist in the supply chain such as:

- The pooling model, where assets are owned by professional Pool Operators and rented to users. Pool Operators manage the movement of their pools between trading partners
- The exchange model, where assets are owned directly by their users. They are exchanged in equal quantities and quality between trading partners

The analysis of strengths/weaknesses showed a strong lack of efficiency in the management of RTIs circulating within the supply chain, with no common commitment among participants in the supply chain to achieve better RTI control. Only some parties undertake actions to improve the follow-up of assets. Moreover the level of non-commitment from other parties makes it difficult, or even impossible, to control assets in the whole supply chain. This analysis resulted in the compilation of a list of requirements needed for improving RTI management.

Requirements analysis: This task described the business and technical requirements to solve Asset Management issues. Based on the initial survey, the scope was limited to the pooling and exchange models for pallets and crates and mainly focused on the food and beverage sectors. Analysis showed that in order to improve asset management, all actors of the supply chain require more visibility on use of RTIs, tracking and tracing assets within their own internal processes as well as during the trading partner processes. An accurate visibility on assets flow could give the opportunity to improve asset use with better rotation, reducing over stock or pool size, identifying companies responsible for causing problems, reducing damages, losses, fraudulent uses or counterfeiting, as well as optimizing exchanges with partners and therefore reducing the quantity of disputes, and enabling the tracking and tracing of the goods contained in the asset by tracking and tracing the asset itself.

Visibility improvement depends on three functional requirements:

- Identification: Assets can be “traced & tracked” in the supply chain if and only if they are uniquely identified in a way that allows a company to distinguish one type of asset from another (kind of asset, dimension, brand, composition, etc) and one unique asset among others (for reasons of traceability)
- Automated data capture: Companies need to automate their processes in order to improve their productivity (i.e. reduce time per process) and their efficiency (better quality of data collected). Barcode and RFID tags are the best data carriers to use for this automated identification
- Data exchange: The supply chain is an “open loop” world and Asset Management involves multiple trading partners. To improve their visibility, companies need to exchange relevant information with their partners about asset movement in the flow. Certain information needs to be stored in an Information System and shared with partners such as: Asset code, Asset quantity, Asset location, Asset disposition.

For these functional requirements, GS1 and EPCglobal have developed a set of standards such as the GRAI code, the GS1 128 Barcode, the UHF Gen2 RFID air interface, EDI messages and EPCIS events. The pilot was then conducted to find how they could be used by trading partners to reach the objectives.

Business case analysis: Two business cases were developed; one concerning a manufacturer and another concerning a retailer. The goal was to use these business cases to launch two semi-closed loop pilots and one global open loop pilot. To reproduce a typical supply chain, the work team consisted of a food manufacturer (Bénédicta), its logistic provider (FM Logistics), a retailer warehouse (Carrefour but operated by Kuehne Nagel), a store (Carrefour) and, of course, two pool providers (LPR and Smart Flow pooling). It was decided to only focus the analysis on pallets in a pooling model, which represents one of the most commonly used asset management practices in European retail. The two business cases addressed all the different ways to solve the business requirements using technology like RFID and EPCglobal Network. For the actors, they detailed the scenarios of GRAI codification, asset tagging with RFID tags, use of RFID readers in the logistic processes, generation and exchange of EPCIS events between IT systems of the trading partners, and evaluated the cost/benefit of the solution.

Pilot preparation: Two pilots were planned; one with Bénédicta (manufacturer) and one with Carrefour (retailer), but only the retailer pilot took place. The Carrefour pilot aimed to track and trace empty pallets and their shipments (the goods) from a warehouse to a store and vice-versa. It ran from June-November 2008 and resulted in the exchange of a total of 5264 RFID pallets. Each pallet was tagged with two tags encoded with the same GRAI and was identified at each step of the logistic flow. The pilot results showed that two tags fixed in diagonal opposite plots of the pallet achieved a high rate of readability during all the logistic processes. However, the location of the tags has to be studied, especially to ensure robustness to electromagnetic phenomena (detuning, absorbing, and reflection) and damages due to the harsh environment. The results also showed that it is possible to track and trace goods by tracking and tracing pallets if an aggregation between the SSCC(s) and the GRAI is managed in the database and shared with authorized trading partners. Finally, the pilot demonstrated positive improvements of visibility due to RFID and EPCIS event exchange.

Results and recommendation analysis: This task consisted of matching the pilot results with the business cases and requirements in order to validate the expected benefits and propose a set of recommendations of GS1 and EPC standards for asset management improvement. The pilot was able to confirm business opportunities such as increase of number of rotations per pallet, the identification of locations where problems occur, improvement of process productivity and efficiency or optimization of partners account management. Moreover, the possibility to track and trace goods by tracking and tracing assets offer a fantastic opportunity to improve Asset Management as well as Supply Chain Management. The experimentation in a real context during the pilot phase allowed development of a set of technical requirements concerning tag selection, tag encoding, placement of tags, reader configuration, and of course Information System infrastructure for companies who want to improve their asset management by using RFID and EPCglobal standards.

Guidelines and dissemination: The final task concerned the dissemination of the work done since the beginning of the project. Based on the conclusions of WP9 and other work packages, 4 deliverables were issued to improve reusable asset management:

- A Technical Guideline to help solution providers to understand the market needs and develop efficient solutions
- An Application Guideline to help end-users to implement the technology
- A Financial tool to help companies to evaluate the costs/benefits of the solution
- A training toolkit to help companies to plan training sessions on RFID asset management

Products in Service work focused on the consumer electronics sector, investigating many benefits of unique serialization, not only within supply chain logistics up to the retail store, but also in after-sales processes such as warranty management and improved repair processes.

The Sony pilot extended across the supply chain from a factory in Barcelona, where Bravia TV sets were manufactured, through a distribution centre in Tilburg, to the Sony Style retail store in Berlin, then onwards to Sony's network of authorised repair centres. Much of the initial work was concerned with upgrading manual data capturing processes to fully automatic processes, to improve the efficiency of operations. An example of this is paperless warranty management, through which it is possible to determine the date when a specific product was purchased by the customer - and to determine whether or not the product is eligible for repair under warranty, even if the customer can no longer find the original printed receipt or returns the product to a store or service centre other than the store where they originally purchased the product.

Although the number of organizations involved in the current pilot was relatively small, the deployment of Discovery Services allowed first hand experience with EPC data sharing concepts in terms of usability, technical performance and functionalities. It also paved the way for a larger roll-out, since it provided an important scalability mechanism for extending to include a wider range of products as well as additional factories, distribution centres, retail stores, service centres and repair centres that were associated with them.

Like the pharmaceutical traceability pilot, the Sony pilot also experimented with the use of RFID in addition to optical data carriers such as barcodes and DataMatrix symbols. RFID tags are typically only attached to the packaging during supply chain logistics, whereas optical identifiers such as barcode and DataMatrix are used to uniquely identify each product instance, avoiding any privacy issues. Associations between identifiers (including associations resulting from changes of aggregation and containment) are recorded via the EPCIS interface provided by the RedBite system installed at each site. For almost all products, Sony already allocated serial numbers. Together with their solution provider, Sony made use of the EPC Tag Data Translation standard and the open source TDT implementation from Fosstrak in order to construct serialised SGTIN EPC identifiers from their EAN-13 barcode identifiers and serial numbers.

The use of Auto-ID technologies such as RFID and EPC enables easier data capture at key points in the supply chain e.g. on arrival and departure at each site. Automated data capturing and the ability to identify several objects simultaneously without line of sight enable companies to increase the visibility of product flows whilst at the same time reducing the effort for manual object identification. The underlying assumption however is that the read rates are always at 100%, which is not the case in a real life situation. The Sony pilot installation and the developed applications demonstrate how to introduce RFID into an operational environment and how to handle read rate issues in order to reap the benefits of increased productivity and visibility.

Because each product instance can be uniquely identified, each can have its own life history with details about its creation, distribution, usage and any maintenance/repair activities, including details about parts or components that were replaced during its service life. At the level of an individual product, this has the potential to help make more informed decisions during repair or servicing, as well as for extracting maximum residual value at the end of life, especially if some particularly valuable components were only installed recently. Furthermore, when this information can be collected across a 'fleet' of products of the same type, it is possible to do data mining to analyse for any systematic performance issues across a particular product line or production batch - and to be able to take more effective and responsive remedial action. The availability of more granular information in searchable electronic format can ultimately provide better decision support tools for streamlining repair and maintenance processes.

The improved visibility enabled through the use of Discovery Services and track and trace techniques enables manufacturers such as Sony to make more selective phased product recalls to remove any dangerous or defective products from the supply chain, even before they reach the retail stores - and potentially to send more targeted advisory notices if there are any issues with the products in the inventory of particular stores or distribution centres. Through experimental pilots, this work strand investigated and demonstrated how deployment of RFID and the EPC Network architecture could yield benefits not only within the supply chain but beyond the point of sale.

2.9 Item level tagging for non-food items

This work package investigated item level tagging for non-food items sold to consumers. Four pilot activities were executed - two pilots on cultural products (CDs, DVDs, computer games and accessories) - initially at HF, then using UHF technology, a pilot on textiles and finally a pilot on tagging of books.

For each pilot phase, the same five-step methodology was used: 1) reviewing current business processes for the selected products, 2) studying RFID usage and defining target scenarios for the pilots, 3) building the business case, 4) implementing and running the experiment in a live environment, then 5) reporting on lessons learned during the pilot.

The pilot on CD, DVD, video games and accessories demonstrated benefits in receiving, inventory/cycle counting & reverse logistics with time efficiency improvements varying from 57% to 85%. The first pilot used HF technology because of regulatory constraints at the time - but then repeated with UHF and with collaboration with suppliers. Initially UHF gave disappointing results, but after a root cause analysis and redesign, a good solution was found using a mix of far field and near field UHF tags. Particular challenges were the difficulties in reading tags in regions with high concentration of products on the sales area (several thousand tags).

For the textile pilot, the initial focus was on business processes within the retail store and the warehouse, including the distribution centre of one international textile supplier, with tagging at the manufacturer DC and the retailer warehouse, using detachable RFID paper labels. The second step involved successful source tagging at manufacturer factories, with minimal adaptation to existing processes. Staff working in sales area of retail store found RFID to be a real improvement of their working conditions, especially by reducing time spent on inventory counting for stock control by around 80-94%. The textile pilot involved Belgium, France and China, using UHF/EPC technology.

The goal of the book tagging pilot was to re-use infrastructure from the textile sub-pilot, including adaptation of the mobile trolley reader. Improvements were demonstrated in reverse logistics and in general productivity of between 74% and 92%. The book pilot also involved a collaboration with UPC and Keonn to evaluate smart shelves developed in WP1 within the live environment of a retail store. Their smart shelf solution gives a quasi real time inventory and product shelf location, with potential for improved customer service through improved availability based on advanced interactivity.

In summary, RFID tagging at item level has been found to require low effort for adapting existing processes, so the potential of industry rollout is high, although the costs of infrastructure and its management are still important variables in decision-making.

2.10 Training and Education

This work package began by investigating training requirements from various stakeholders to assess topics and preferred delivery mechanisms for each target audience. Particular emphasis focused on provision of training for SMEs, either locally or electronically and in local languages and blended learning solution on EPC / RFID were therefore developed combining classroom material, webinars, e-learning and other training delivery mechanisms.

BRIDGE developed five training courses, publicly available in both classrooms and e-learning formats, beginning with an introduction to the basics of EPC and RFID, followed by 3 advanced courses covering business, technical and implementation aspects of EPC / RFID in more detail. The final course is targeted at senior managers and demonstrates how EPC/RFID impacts the business processes of the supply chain, as defined in the Supply Chain Operations Reference (SCOR) model.

All courses have been tested live and thoroughly reviewed by additional experts. The training requirements analysis and final version of these training courses are publicly available from the BRIDGE website.

2.11 Dissemination and Adoption Tools

WP13 developed tools to enable any interested organization to inform and educate their stakeholders about the findings and results of the various BRIDGE work packages, as well as the impacts and benefits of EPC/RFID in general. Six concept animations were developed, consisting of multi-media learning objects (in Macromedia Flash), that can be used for e-learning courses, presentations etc. to clearly present key applications of the technology. A portable demonstration software tool was also developed to show how the EPCglobal network works in real supply chain conditions and to simulate the kind of information each trading partner would see as goods are transferred between trading partners. WP13 also prepared two impact reports - a market sizing study forecasting the market for passive RFID in Europe for the next fifteen years and a report evaluating the impact of RFID technology on the European economy. A conference package was also prepared, consisting of brochures, white papers, reports and a demonstration setup and presentation material. It can be freely reused by any organization hosting an EPC/RFID related event or wanting to learn more about the findings of the BRIDGE project.

To help with consumer acceptance, WP13 has contributed to the development and translation of the website www.discoverRFID.org to help consumers understand the basics of RFID and EPC and how the technology helps companies, institutions and organizations to make their life easier and safer. WP13 also developed and maintains the BRIDGE website www.bridge-project.eu , where all the adoptions tools are publicly available.

3 Enhancing European operations with RFID and fine-grained information sharing

Over the past three years the BRIDGE project became a significant hub of European activity on RFID research. Both the application and the technical work packages brought valuable lessons to European practitioners and researchers, helping to define the future directions of RFID in Europe. The technical work packages delivered next generation technology such as track and trace algorithms, discovery services, security algorithms and low cost high read range hardware. The application work packages trialled RFID in production, supply chain, retail and asset management. Where possible, they made use of developments in the technical work packages. Some of the key learnings from BRIDGE are summarized below:

- The modular design of the track and trace analytics framework enabled easy extension to other developments in BRIDGE, for example anti-counterfeit detection leveraged the event gathering layer, then added a complex rule system to detect cloned tags, while an high-level application programming interface was designed to support business-level queries and alerting criteria from the various business work packages. The pharmaceutical pilot produced a particularly comprehensive data set, including some interesting features especially in the early stages of a pilot while the staff were still familiarizing themselves with the equipment. These features in the data were useful for developing some of the criteria for alerting about possible anomalies or deviations in the supply chain. Another important lesson was that of data smoothing as it was noted that spurious data could alter the accuracy even if some smoothing was done. It is therefore advisable to try to first improve the physical installation to improve reliability and eliminate spurious reads, rather than relying only on the algorithms to smooth the data.
- BRIDGE has contributed significantly to the development of open global standards for Discovery services, which will finally enable sharing of serial-level information within open supply chain networks. However, there is opportunity for further development to determine a viable business model for operators of Discovery Services and also to integrate support for trading of serial-level information between partners, without incurring significant transaction costs. Future developments could also see Discovery Services providing support for integration of sensor information and agents; discovery of relevant sensor resources allows gathering of information about the state or condition of each individual product instance, while software agents could assist with automation of information discovery. Other key areas that might gain momentum in the near future include ad-hoc wireless networks, semantic tagging of entities, the mapping of digital, virtual and real entities, processing, filtering and aggregation of data and processing of data streams in order to improve quality of service.
- A key learning from the anti-counterfeiting work was the importance of supply chain data sharing, since an accurate system is very much based on traceability and its automated data analysis. Although it was difficult to produce a business case for deploying an RFID infrastructure solely for the combating counterfeiting, anti-counterfeit solutions represent only a small marginal cost when a company is already committed to deploying RFID for other reasons, such as efficiency improvements within the enterprise or supply chain. Key areas of future research in security could be in energy-efficient encryption and data protection technologies, models for decentralized authentication and trust, and privacy-preserving technology for heterogeneous sets of devices. Reducing the cost of security is key to realization of RFID based systems in the supply chain.
- The pharmaceutical pilot showed that a combination of identification technologies such as 2-D matrix codes, barcodes and RFID can co-exist in a supply chain and all be used to achieve unique identification of packages. An important outcome of this pilot was to highlight the various benefits of networked based traceability, as opposed to document-centric traceability. Prior to BRIDGE, work was already in progress to develop a standard for an electronic pedigree document that could be appended and digitally signed at each step as it is passed downstream along the supply chain with the goods. Although the EPCglobal Drug Pedigree messaging standard satisfies the requirements of the US states introducing pedigree legislation, the approach results in a very asymmetric visibility, with no improved visibility benefit for manufacturers, despite their cost of tagging. It also lacks many of the benefits of a more networked approach to pharmaceutical traceability, such as those demonstrated in the BRIDGE pilot. These include opportunities for improved inventory management, improved downstream visibility for manufacturers and the ability to do rapid and selective product recalls.

- The manufacturing pilot provided systematic methods for RFID opportunity identification, application development, and implementation, filling a gap in operations management literature. In terms of installation, it was important to think out of the box to reduce costs. In Nestle UK the solution was built by using a mobile fork lift truck with readers attached, instead of static read points at a large number of processing machines. In COVAP, a mobile reader was used instead of readers at every inventory point. Another important lesson was the importance of human factors. Where it was difficult to obtain high read rates, operators facilitated a higher read rate by following certain process steps. Operators need to be trained and informed of RFID technology and what automation means for them. The work package mostly took existing processes and improved them. A future extension shall be the examination of more innovative applications such as distributed manufacturing or machine maintenance. Another research effort that needs to be continued is the modelling of soft benefits of RFID, such as the prevention of recalls by raising alerts as soon as products go into the wrong state. Such additional benefits are important for justifying the adoption of RFID, although they are difficult to quantify.

- Consumer electronics companies have been using serialized ID for many years but with proprietary systems. The products in service work package demonstrated that existing identification codes could be mapped into Electronic Product Codes (EPCs) for use with EPCglobal architecture standards. As a result, the logistics of the repair process is improved, and so is the repair process by using the information gathered to help technicians to carry out the repair process. However, this approach might not be able to offer a business case for consumer electronics, since these products are becoming smaller and hence more difficult to repair, it may be appropriate for higher value products and industrial assets, especially those with more mechanical parts and equipment that can be repaired.

- In the item level tagging for non-food items, significant time savings were found particularly during inventory checks. The pilot demonstrated greater sale-to-orders ratio than other stores not using RFID, primarily due to fewer inventory discrepancies. RFID also helped staff to adjust orders from suppliers according to remaining stock especially in situations where they were not allowed to return stock to suppliers. The most important result was that significant benefits could be achieved without staff having to do additional work or modify the existing processes in store.

- Despite the BRIDGE initiative, industry-wide deployment in RFID is still at an early stage, which leads to a lack of understanding of organizational change management in the deployment of RFID systems. In addition to leaner processes, future areas of focus could include global cost savings and optimization of supply chain carbon footprint. To this end, enterprise software development companies could look into further development and commercialization of business analytics using RFID data.

4 Conclusions

The BRIDGE project created a state of the art framework for consolidating the use of standardized RFID technology and for contributing to the development of business solutions for global supply chain applications, thereby making a number of lasting contributions that are likely to impact the research in RFID, not only in Europe, but also in the rest of the world. Among these contributions, this chapter presented a number of technology developments, such as the low-cost readers, Gen 2 sensor-enabled tag as well as improvements to the security of hardware and network layers, design and development of discovery services, standardisation activities and track and trace analytics to help business users to make sense of the vast amounts of data. The business work packages have developed business cases in various industry sectors and implemented pilots, generating best practice guidelines.

In summary, BRIDGE has significantly advanced the state of the art in RFID Europe, while highlighting future directions in research that European organizations could pursue for maximizing their return on investment from RFID enhanced operations. In this paper we highlighted a number of key areas of address. These include the impact of spurious data in tracking and tracing, the integration of sensor information and agents in discovery services, energy-efficient encryption and data protection technologies, privacy-preserving technology for heterogeneous sets of devices, reducing the cost of security, examination of more innovative applications such as distributed manufacturing or machine maintenance, modelling of soft benefits of RFID, billing of RFID data and infrastructures, and using RFID to reduce supply chain carbon footprint. We urge researchers and practitioners to spend time helping to address these since networked RFID can play a vital role in preparing the economy for the manufacturing and supply chain landscape in Europe.

4.8 Open Source Middleware for Networked Embedded Systems towards Future Internet of Things

ASPIRE & HYDRA Project

Neeli R. Prasad, Center for TeleInFrastruktur (CTIF), Aalborg University, DK; Markus Eisenhauer, Fraunhofer Institute for applied Information Technology FIT, DE; Matts Ahlsén, CNET Svenska A.B., SE; Atta Badii, University of Reading, UK; André Brinkmann, University of Paderborn, DE; Klaus Marius Hansen, University of Aarhus, DK; Peter Rosengren, CNET Svenska A.B., SE

Abstract: The European Commission (EC) funded Integrated Projects (IPs) ASPIRE and Hydra develop open source middleware for networked embedded systems and focus on the integration of devices with energy and computational power constraints. These devices like sensors, actuators, or RFIDs are the foundation of the Internet of Things (IoT), which will connect objects of our daily life, enabling e.g. their tracking as well as their interaction in service oriented environments. The aim is to reduce time-to-market for developers and total cost of ownership (TCO) for SMEs. Therefore, ASPIRE delivers a lightweight and privacy-friendly middleware, which eases the standard-compliant development of RFIDs, while Hydra enables the connection of heterogeneous devices, offering a secure environment to build model-guided web services on multi-protocol wired and wireless networks. This chapter shows that the combination of both approaches will significantly simplify and speed-up the transformation from manually configured sensor-actor environments to service-oriented architectures.

1 Internet of Things

The users of today's networked world are swamped with information coming from a myriad of applications and services present on their devices, communication infrastructures, and on the Internet. In the near future, this information overload will be magnified many times when the Internet of Things (IoT) becomes a reality, i.e. objects, smart devices, services, sensors, and RFIDs can interact with the user and among themselves to provide services or information. Despite the simplicity of the operational principles of IoT technology (i.e. tags responding to readers requests), the design of a complete IoT system encompasses complex interactions not only between different layers of the OSI (Open Systems Interconnection) model, but it also involves several market, privacy, security, and business issues. This heterogeneous landscape calls for a middleware platform which is able to consider all these complex variables in a flexible and modular way, which is able to provide a starting point for future upgrades and innovations, and which considerably reduces the implementation costs of IoT solutions.

1.1 IoT Scenarios

The IoT is expected to include everything from simple RFID tags and sensors of everyday objects like cars and fridges to intelligent devices with high computing power. One of the main challenges of the IoT is to handle the complexity of the huge number of heterogeneous devices interacting in these environments, which cannot be envisioned by the developers of these devices. Dedicated scenarios discussed both in ASPIRE and HYDRA are the health sector, the apparel industry, and the agriculture domain. Specially being used for tracking and tracing.

An example from the agriculture domain is the creation of an irrigation system, which integrates various systems to enable intelligent control. On the one hand, such systems have to have complex irrigation models with an expert system for advanced scheduling and decision support and dynamic search for up-to-date weather information. This central system is responsible for the optimisation of water distribution on the entire farm, relating to topography, weather and barometric pressure. These parts of the irrigation system typical run on a personal computer connected to the Internet and have access to Bluetooth, wireless Ethernet and cabled Ethernet networks. On the other hand, input to the irrigation control system is today also coming from distributed electrical conductivity sensors that allow mapping of soil characteristics, but new systems will be able to integrate even more accurate water demand predictions based on subsurface soil moisture sensors in preset depths in the fields. The sensors will be spread on the fields and ploughed into the ground. They communicate via RFID technology and a robotic radio transmitter to the irrigation system.

In a different part of the farm, the irrigation control system may also interfaces to the irrigation system installed in the greenhouses, where the farmer grows tomatoes, peppers and cucumbers. A new precision irrigation system based on estimation of crops' water stress with acoustic emission (AE) technique has been installed in the greenhouse. The system acquires real-time acoustic signals and transpiration data from the tomato crop. The system also collects environment parameters of the greenhouse such as temperature, air humidity, sunlight, and carbon dioxide density.

1.2 Requirement Analysis

The presented IoT scenario for agriculture environments contains a number of interesting challenges, which have been the motivation for the ASPIRE and Hydra projects. This section contains a short requirement analysis concerning middleware development for the IoT based on this example scenario.

The first observation is that the amount of different devices interacting in an IoT environment is much bigger than for comparable scenarios in standard IT environments. Nevertheless, the time to market for products and solutions has to be as short as possible, as each single device, like a subsurface soil moisture sensors, has to be as inexpensive as possible, and each single installation, like an irrigation system, can only be cost-effective, if each adaptation can be done in very short time.

These requirements create a demand for middleware solutions, which support both individual device development as well as the interoperability of very different devices, which might be connected by different network technologies and therefore need proxies which help to bridge between these boundaries. The huge amount of sensors and actuators working together in IoT environments also require service discovery procedures as well as means to enforce semantic compatibility between devices. Otherwise it would become too costly to manually configure each device on its own.

Additional complexity arises, when sensor values trigger services inside the IoT. Today's IT environments overcome comparable complexity by introducing service-oriented architectures, which are based on web service interfaces. Similar mechanisms for embedded devices seem a promising approach to introduce service-oriented concepts for the IoT.

Another aspect imminent in many IoT environments, especially in e-Health or home automation, is integrated support for enforcing security, privacy, and integrity policies, which ensure that no information leakage takes place.

This chapter presents the European research projects Aspire and Hydra, which tackle the above mentioned challenges by introducing open source middleware on the device and network level, which will help to significantly reduce time to market for devices and applications, while ensuring security and semantic interoperability.

2 ASPIRE

In order to fill the gap in the development of middleware for RFID applications, ASPIRE will develop and deliver lightweight, royalty-free, programmable, privacy friendly, standards-compliant, scalable, integrated, and intelligent middleware platform that will facilitate low-cost development and deployment of innovative fully automatic RFID solutions. The ASPIRE middleware will be licensed under LGPL v2 (Lesser General Public License). ASPIRE aims to bring RFID to SMEs.

ASPIRE middleware architecture that is fully compliant with the EPC suite of standards [EPC]. The EPC set of standards is mainly concerned with the processing of data in centralized RFID architectures [FLOER]o. This means that this set of standards assumes that a central node or core is in charge of the coordination, configuration, collection and other functions of the platform.

Programmability features in the middleware aim at easing the configuration of ASPIRE solutions. The ASPIRE programmability functionality will offer the possibility to deploy RFID solutions through entering high-level metadata for a company (including the business context of its RFID deployments), rather than through writing significant amounts of low-level programming statements. At the same time programmability functionalities also aim at treating personal data as specified by ePrivacy protection directives. For example through algorithms that clean up unnecessary data and maintain principles of data quality, limitation, and conservation.

Figure 4.8-1: ASPIRE Overview.

2.1 General Architecture

The ASPIRE architecture [AS43b] (see Figure 4.8-1) implements the set of EPC standards and complements it by a set of added value features. Figure 4.8-2 shows the main components of the architecture. Heterogeneous landscape of readers from different providers is displayed. Note that readers that are not under EPC or ASPIRE standards are connected to the platform via a HAL or hardware abstraction layer, which basically converts proprietary into ASPIRE semantics, and vice versa. Readers that deploy EPC reader protocols are directly connected via RP or LLRP to the Filtering and collection (F&C) server, which in turn implements the ALE interface standard to upper layers. The F&C server filters unwanted data and forwards refined streams to different subscribers. In ASPIRE the main subscriber is the BEG (Business Event Generator), which interconnects the F&C and the EPCIS modules and which constitutes and added value solution provided by ASPIRE. The EPCIS module is finally connected to particular end user applications via, for example, web-services. A key element in the ASPIRE architecture is the Integrated Development Environment, which allows a rapid and efficient management of the ASPIRE middleware platform. The management solution is not part of EPC standards and hence it also constitutes an added value solution of ASPIRE.

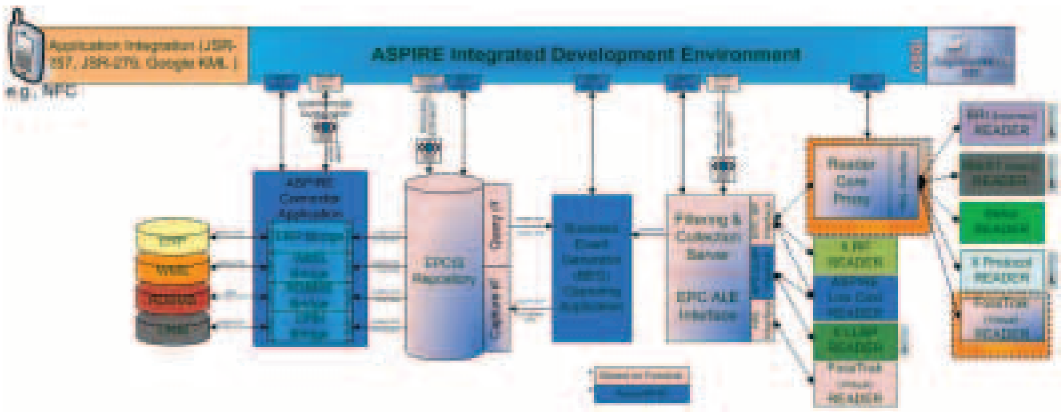


Figure 4.8-2: ASPIRE Architecture for Programmability, Configurability and End-to-End Infrastructure Management.

The ASPIRE architecture identifies the following main middleware modules:

- Middleware modules for virtualising/abstracting reader access i.e. enabling the ASPIRE platform to be flexible in supporting different reader vendors and types.
- Middleware modules for filtering and collection, which decouple the ASPIRE middleware platform from the physical readers' configurations and details, as well as from how tags are sensed and read. The filtering and collection middleware produces application level events.
- Middleware modules for generating business events in a configurable and automated fashion i.e. enabling the ASPIRE middleware to generate business events on the basis of reports produced by the filtering and collection modules.
- Middleware modules and repositories for storing and managing business events.
- Middleware modules acting as connectors to legacy IT (Information Technology) systems such as Enterprise Resource Planning (ERP) systems, Warehouse Management Systems (WMS), as well as corporate databases. Note that some of the above modules are prescribed as EPC (Electronic Product Code) compliant modules i.e. ensuring compliance with a major set of RFID standards. This is particularly true for specifications relating to reader access and filtering.

The ASPIRE architecture novelty lies in following innovative modules and tools which are not yet in any standard:

- A business event generation (BEG) middleware module, which translates filtered reports into business events in an automatic fashion.
- Management modules enabling the end-to-end management of the whole RFID infrastructure, comprising both RFID hardware and middleware.
- A set of tools enabling business process management over the ASPIRE middleware.

Business Event Generator: The architecture introduces a Business Event Generator (BEG) module between the F&C and Information Sharing (e.g. EPC-IS) modules. The role of the BEG is to automate the mapping between reports stemming from F&C and IS events. Instead of requiring developers to implement the mapping logic, the BEG enables application builders to configure the mapping based on the semantics of the RFID application.

With the help of the AspireRfid IDE, it is possible to create required business events. In EPC terms, BEG can be seen as a specific instance of an EPC-IS capturing application, which parses EPC-ALE reports, fuses these reports with business context data using the assigned business event from the company's business metadata to serve as guide and accordingly prepares EPC-IS compliant events. The latter events are submitted to the EPC-IS Repository, based on an EPC-IS capture interface and related bindings. The specification of the BEG is a valuable addition over existing RFID middleware architectures and platforms.

Information Sharing Repository: At the heart of the architecture is the EPC-IS repository. The ASPIRE Information Sharing repository is responsible for receiving application-agnostic RFID data from the filtering & collection middleware through the Business Event Generation (BEG) application and to store the translated RFID data in corresponding business events. These events carry the business context and make business events and master data available and accessible to other upstream applications through the query interface.

Generally, the ASPIRE information sharing repository is dealing with two kinds of data:

- RFID event data i.e. data arising in the course of carrying out business processes. These data change very frequently at the time scales where business processes are carried out.
- Master/company data i.e. additional data that provides the necessary context for interpreting the event data. These are data items associated with the company, its business locations, its read points, as well as with the business steps comprising the business processes that this company carries out.

At a glance Information Services of the ASPIRE Information Sharing middleware itself consists of three parts, a capture interface that provides web services for storing data, a repository that provides persistence, and query interface that provides web services that retrieves the business events/master data from the repository.

Connector Application: RFID middleware components described in the previous paragraphs provide a foundation for translating raw RFID streams to meaningful business events comprising business context such as where a tag was seen, at what time and in the scope of which process. Enterprises can then leverage these business events through their legacy IT systems, which are used to support their business processes. To this end, there is a clear need for interfacing these legacy systems with the information sharing repositories, established and populated as part of the RFID deployment. Interfacing between IT systems and the information sharing repository, as well as other middleware blocks of the RFID deployment is realized through specialized middleware components that are called “connectors”.

The main purpose of connector components is to abstract the interface between the ASPIRE information sharing repository and enterprise information systems. Hence, connectors offer APIs that enable proprietary enterprise information systems to exchange business information with the ASPIRE RFID middleware system.

Connectors therefore provide:

- *Support for services and events*: Composite applications can call out to existing functionality as a set of services, and to be notified when a particular event type (for example, “purchase order inserted,” “employee hired”) occurs within an application.
- *Service abstraction*: All services have some common properties, including error handling, syntax, and calling mechanisms. They also have common access mechanisms such as JCA (Java Connector Architecture), JDBC, ODBC (Object Database Connectivity), and Web services, ideally spanning different platforms. This makes the services more reusable, while also allowing them to share communications, load balancing, and other non-service-specific capabilities.
- *Functionality abstraction*: Individual services are driven by metadata about the transactions that the business needs to execute.
- *Process management*: Services embed processes, and process management tools call services. Hence, connectors support the grouping of several service invocations to processes.

Management: The architecture specifies also the implementation of end-to-end management functionality based on JMX (Java Management Extension) technology. To this end, a JMX wrapper is specified for each middleware and hardware component. JMX wrappers interface to underlying readers based on the Simple Network Management Protocol (SNMP) and the Reader Management (RM) protocol, while they interface to middleware components using MBeans, which access their low-level control properties. Based on these JMX wrappers composite, sophisticated management applications can be implemented. Management applications can be used to interface and control actuators as well. Based on JMX, actuator control commands can be issued upon the occurrence of certain events at any middleware layer.

Actuators: The actuator control framework defines interfaces and connectors that third party applications will be able to utilize in order to successfully interact with analogue or digital devices, based on sensor events. These sensors may either be RFID or other ASPIRE supported physical sensors. Applications will be able to register an event handler that will, for example, interact with a flashlight when a specific group of tags pass through a RFID aggregation gate.

Integrated Development Environment: As far as ease of development and deployment is concerned, the architecture specifies the existence of an IDE enabling the visual management of all configuration files and meta-data that are required for the operation of an RFID solution.

2.2 ASPIRE Middleware features

ASPIRE solutions will be open source and royalty free, which will bring an important reduction of the Total Cost of Ownership, and at the same time programmable and lightweight in order to be backwards compatible with current IT SME infrastructure. Additionally, ASPIRE will be designed as privacy friendly, which means that future privacy features related to RFID can be easily adopted by the platform. Finally, ASPIRE will act as a main vehicle for realizing the proposed swift in the current RFID deployment paradigm. Portions (i.e. specific libraries) of the ASPIRE middleware will be hosted and run on low-cost RFID-enabled microelectronic systems, in order to further lower the TCO in mobility scenarios (i.e. mobile warehouses, trucks). Hence, the ASPIRE middleware platform will be combined with innovative European developments in the area of ubiquitous RFID-based sensing towards enabling novel business cases that ensure improved business results.

ASPIRE Innovative filtering solution

As observed in previous subsections, filtering has a prominent position in the RFID middleware blocks. Legacy middleware products concentrate on

- Low-level filtering (Tags, Tag Data)
- Aggregation of readings
- Provision of basic low-level application events

Advancing on this legacy features, ASPIRE introduces a new approach to RFID middleware through a two-tier filtering:

- Conventional filtering (e.g., EPC-ALE paradigm)
  - Open Source Tools (Stored/Save, Edit, Delete Filters) compliant to ALE specifications
- Filtering of business events (i.e. based on the paradigm of BEG module)
  - Combination of filtered data with business metadata according to declared/configured processes
  - Specifications for mapping sensor reading events into business events
- Filtering of many types of sensors other than RFID, like ZigBee (IEEE 802.15) and HF sensors.

The ASPIRE FML (Filtering Markup Language)

The filtering functionality in an RFID platform is not only used to get rid of extra information that is not relevant for upper layers, but it represents the connection between the low level RFID world, and the business and application level semantics, therefore being a critical point for middleware integrators and developers. To provide a clear consensus for open source contributors around this important interface, a straightforward solution is to use a high level programming language oriented to describe business semantics and to isolate them from the low level details of RFID platforms. Among such languages, one that has received special interest due to its flexibility and great acceptance between Internet and application developers is the extensible markup language (XML). XML is a set of rules for encoding documents electronically. It is defined in the XML 1.0 Specification produced by the W3C (world wide web consortium) and several other related specifications; all are fee-free open standards. As the name suggests, by using a set of markups, the language is able to be adapted to a variety of purposes, including the filtering functionality of an RFID system as described in this document. The filtering markup language proposed by ASPIRE not only helps in the programmability of the tool but it also provides modularity and the possibility of reusing filtering rules. In this way future developers can start building up new and interesting filtering policies from previously tested and mature solutions. Code reusability has been widely used in the software world, for example in the context of compilers for object oriented languages, and in the open source community itself. Reuse of filters with business meaning will allow SMEs and untrained persons on RFID to deploy new applications in short periods of time and at low cost.

Integration of Low-Cost reader within the ASPIRE Architecture

This hardware platform will enhance the ASPIRE middleware programmable architecture by providing capabilities for flexibly handling physical quantities data (e.g. temperature, pressure, humidity). The ASPIRE reader will come into facets (which can be considered as two distinct readers) in particular:

- A classical fixed reader
- A portable low-cost reader

The ASPIRE architecture includes an interface to the low-cost readers. In connection to, a hardware abstraction layer (HAL) implementation for the low-cost readers will be provided. This HAL implementation will enable ASPIRE applications, as well as ASPIRE management and development tools to use the low-cost reader exactly in the same way with other readers (e.g., using the EPC-RP, EPC-LLRP or RM protocols). As a result of this interface, in the scope of the ASPIRE trials, as well as other deliverable of the project, system architects will be able to conveniently choose between the low-cost reader and other commercial readers (e.g., based on end-user requirements and trial objectives).

3 Hydra

The first objective of the Hydra project is to develop middleware based on a service-oriented architecture, to which the underlying communication layer is transparent. The middleware will include support for distributed as well as centralised architectures, security and trust, self-management and model-driven development of applications.

The Hydra middleware will be deployable on both new and existing networks of distributed wireless and wired devices, which operate with limited resources in terms of computing power, energy and memory usage. It will allow for secure, trustworthy, and fault tolerant applications. The embedded and mobile service-oriented architecture will provide interoperable access to data, information and knowledge across heterogeneous platforms supporting true ambient intelligence for ubiquitous networked devices.

The second objective of the Hydra project is to produce tools that will simplify the development process based on the Hydra middleware: software and a device development kit (SDK and DDK) to be used by developers.

3.1 General Architecture

The Hydra middleware is an intelligent software layer placed between the operating system and applications. The middleware contains a number of software components - or managers - designed to handle the various tasks needed to support a cost-effective development of intelligent applications for networked embedded systems (see Figure 4.8-3). The middleware distinguishes between application elements and device elements, where the main differentiation is the resources required to run the manager.

Application elements are components, which are usually running on powerful machines intended to serve as managing instance inside, e.g. a home automation environment. Device elements are deployed in machines, which are restricted in computing power or battery lifetime.

The middleware can be incorporated in both new and existing networks of distributed devices. It provides easy-to-use web service interfaces for controlling different types of physical devices irrespective of their network interface technology. It is based on a semantic model-driven architecture (MDA) for easy programming and also incorporates means for device and service discovery, peer-to-peer communication and diagnostics. Hydra-enabled devices offer the potential for secure and trustworthy communication through distributed security and social trust components of the middleware.

The Hydra middleware specifically facilitates the realisation of context-aware behaviour and management of data persistence on resource-constrained devices. Context-aware services can ubiquitously sense the user's environment and obtain information about the circumstances under which they are able to operate and thus adapt their behaviour based on rules defined in the application or set directly by the user.

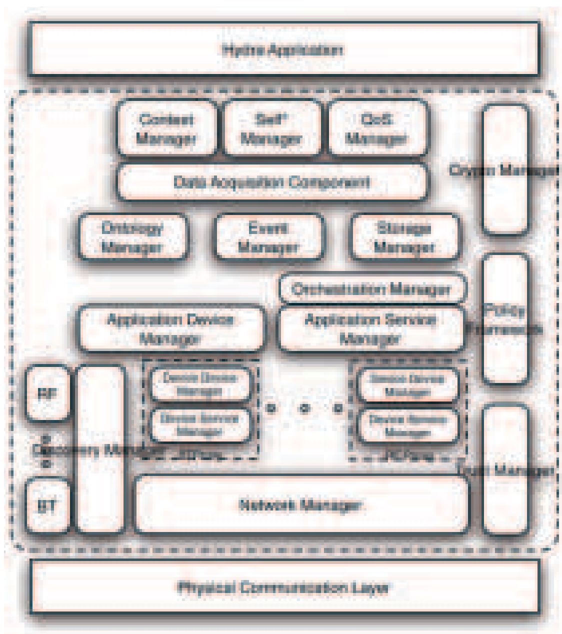


Figure 4.8-3: Hydra Architecture.

3.2 Semantic Device Discovery and Ontologies

Semantic Device Discovery: The basic idea behind the Hydra semantic model-driven architecture (MDA) is to differentiate between the physical devices and the application's view of the device. A Hydra device is the software representation of a physical device. This representation is either implemented by a Hydra software proxy running on a gateway device or by embedded Hydra software on the actual device. A Hydra device is said to Hydra-enable a physical device.

The concept of semantic devices, which is based on Hydra devices, supports static as well as dynamic mappings to physical devices. Mappings can be both 1-to-1 from a semantic device to a Hydra device or compositions of multiple devices into an aggregate. An example of a 1-to-1 mapping would be a "semantic pump" that is exposed with all its services to the programmer, whereas a "semantic heating system" is a composition of three different underlying Hydra devices – a pump, a thermometer and a digital lamp [1]. Hydra supports the semantic MDA approach from two perspectives:

- At design-time through the use of the Hydra Device Ontology, whereby it supports both device developers as well as application developers. When a new device type is needed, the adequate concept in the device classification ontology can be further sub-classed by more specialised concepts and the new properties can be added. Specific device models are created as instances of device ontology concepts and serve as templates for run-time instances of physical devices.
- At run-time, whereby Hydra applications can use knowledge provided by various device management services (e.g. discovery and updates). In the device discovery process, the discovery information is resolved using the ontology and the most suitable template is identified. The identified template is cloned and a new unique run-time instance representing the specific device is created.

These device descriptions can be defined at a fairly general level, e.g. the application may only be interested in a "Hydra SMS Service" and any device entering the network that fits this general category will be presented to the application. This means that an application need only know the types of devices and services. The application may use a device that may have been designed and built after the application was defined, as long as it can be classified through the device ontology as being of a device type or using a service that is requested by the application.

The Hydra SDK is available in an object-oriented language environment providing class libraries developers can use to program with existing devices, and to generate new ones. Specific tools exist for accessing and maintaining the Device ontology.

Device Discovery Architecture: The Hydra MDA includes a three-layer discovery architecture. The discovery process operates both locally and remotely so that devices that are discovered in a local Hydra network can also be discovered in a Hydra network over the P2P protocol implemented by the Hydra Network Manager.

The lowest discovery layer implements the protocol-specific discovery of physical devices. This is performed by a set of specialized discovery managers listening for new devices at gateways in a Hydra network. The second layer uses UPnP/DLNA technology to announce discovered physical devices in the local network and to peer networks. At the top most layer the device type is resolved against the device ontology and is mapped to one or more Hydra device types.

Hydra Device Ontology: The Hydra Device Ontology is expressed in OWL-DL [5,7] and is structured in several modules connected to the core ontology concepts, describing device capabilities like hardware and software properties, services, device malfunctions, QoS-properties, energy profiles, and device security properties [1]. The Hydra device ontology was. as illustrated in Figure 4.8-4, initially based on the FIPA Device Ontology, which specifies a frame-based structure to describe devices [3]. The initial device taxonomy has been extended based on the AMIGO project vocabularies for device descriptions [2] and has been further extended with additional subsets for specific device capabilities.

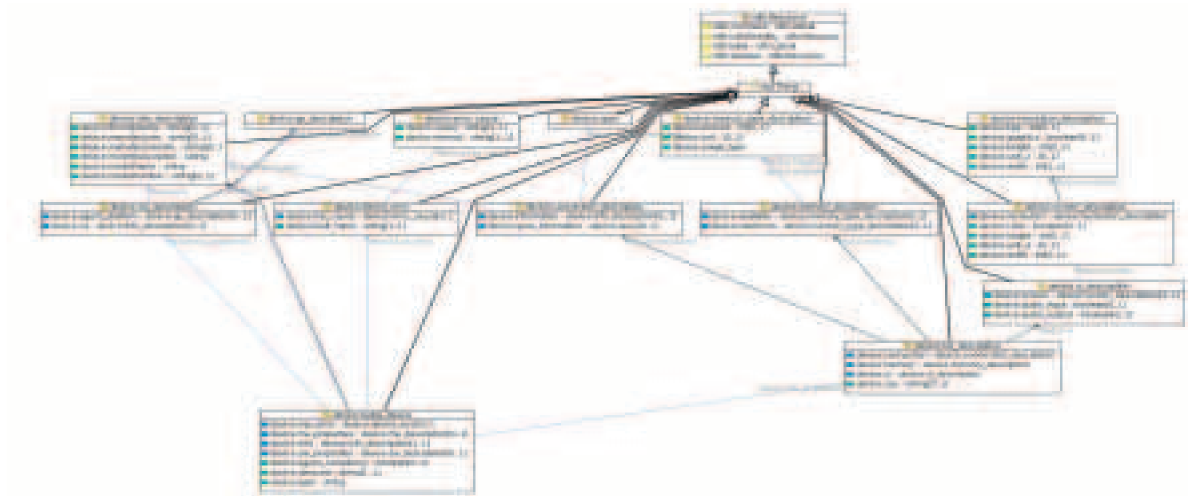


Figure 4.8-4: Hydra Device Ontology.

3.3 Security

There are many security challenges in a homogeneous environment, but are even larger when we move to enable interoperability across heterogeneous platforms and protocols, which otherwise are incompatible. It is expedient that users inside ambient environments should be able to simply specify their security, privacy and trust requirements as policies.

The Hydra security framework deploys a policy enforcement framework comprising of a policy administration component, a policy decision component, a policy enforcement component, a policy conflict resolution component and the core Hydra policy language. The confluence of these components ensures that security decisions made by the individual user are enforced as and when necessary [11].

A further concern in ambient intelligence is that of context-awareness and securing context information. Context information can be shared in a “push” or “pull” approach. Context managers, the components within the Hydra middleware responsible for context acquisition and sharing, can assign security policies to context data, which in general identify Hydra principals who are authorised to access context data. For the “pull” approach, the enforcement is straightforward, as context consumers make themselves known and the distribution can be dealt with on a case-by-case basis. For the “push” approach to context sharing, a blackboard has been realised. Whenever data is published onto the blackboard, it is accompanied by a security policy, which will be used for the authorisation decision about who can subscribe to the published data.

A third paradigm, originating from MobiPets, is virtualisation [10]. Hydra applies virtualisation mechanisms to different entities: virtual devices or proxies act as logical representations of devices to protect the actual device from possible attacks by adding another protection layer. By defining a proxy for a physical device, it is possible to integrate non-Hydra-enabled devices into a Hydra-enabled network and to enable further high-level concepts, such as semantic description of device capabilities or resolution of security. In addition, physical devices can be assigned to specific virtual device classes in a way that best serves their control within an application context – e.g. it is possible to define a “virtual” global light-switch that controls all lights within a building.

3.4 Service oriented Architectures and Hydra

The term Service-Oriented Architecture, i.e., describes an architectural style in which units of functionality are exposed by ‘service providers’ in a network-accessible and loosely coupled way as ‘services’ used by ‘service consumers’, is used both inside the Hydra middleware and encouraged in applications built using the Hydra middleware on top of it. As an example in the agriculture scenario, the robotic radio transmitter and the irrigation system itself could be exposed and interact through services. Inside Hydra, the managers of the middleware expose their functionality as services and interact through services. Outside Hydra, applications may use Hydra managers through services and the Hydra SDK/DDK contains tools to service-enable elements of applications.

Concretely, Hydra uses web services in the form of SOAP [SOAP] over HTTP for communication. The 'Limbo' tool [LIMBO] creates service stubs for service providers and consumers to be deployed on embedded devices. Based on a description of the service (through a WSDL interface description [WSDL]) and the device do deploy on (through the Hydra Device Ontology), a service- and device-specific service stub is generated. Devices are described by a static profile (through, e.g., a hardware description) and a dynamic profile (through a state machine describing device runtime states). Artefacts generated from the dynamic profile allow Hydra services to tie into the self-management functionality of Hydra (through the 'Flamenco' service), which includes self-protection and self-adaptation functionality realized using semantic Web technology [SeMaPs].

4 Summary and Future Steps

RFID and Sensor technology has advanced significantly over the past few decades. Rapid developments of low cost microelectronics and radio frequency transceivers have considerably reduced size and costs of high frequency and ultra-high frequency RFID transceivers/sensor nodes allowing longer reading ranges and faster reading rates than before. The technology is now viable to newer novel applications with higher mobility and large number of tagged items. However, unlike conventional scenarios, these new applications require a more robust and complex middleware platform in order to cover issues at different layers of the communication architecture, from different business contexts. This complexity has left several open research issues in middleware design that still pose a high entry cost for RFID/Sensor technology adopters, mainly SMEs.

The research carried out in ASPIRE and HYDRA will provide a radical change in the current RFID/WSNs deployment paradigm through distributed as well as centralised architectures, security and trust, self-management and model-driven development of applications innovative, programmable, royalty-free, lightweight and privacy friendly middleware.

The ASPIRE solutions will be open source and royalty free, which will bring an important reduction of the Total Cost of Ownership (TCO), and at the same time programmable and lightweight in order to be backwards compatible with current IT SME infrastructure. Additionally, ASPIRE will be designed as privacy friendly which means that future privacy features related to RFID can be easily adopted by the platform. Finally, ASPIRE will act as a main vehicle for realizing the proposed swift in the current RFID deployment paradigm. Portions (i.e. specific libraries) of the ASPIRE middleware will be hosted and run on low-cost RFID-enabled microelectronic systems, in order to further lower the TCO in mobility scenarios (i.e. mobile warehouses, trucks). Hence, the ASPIRE middleware platform will be combined with innovative European developments in the area of ubiquitous RFID-based sensing (e.g., physical quantities sensing (temperature, humidity, pressure, acceleration), mobile, low-cost); towards enabling novel business cases that ensure improved business results.

The HYDRA middleware will be deployable on both new and existing networks of distributed wireless and wired devices, which operate with limited resources in terms of computing power, energy and memory usage. It will allow for secure, trustworthy, and fault tolerant applications through the use of distributed security and social trust components. The embedded and mobile Service-oriented Architecture will provide interoperable access to data, information and knowledge across heterogeneous platforms, including web services, and support true ambient intelligence for ubiquitous networked devices.

The new middleware paradigm will be particular beneficial to European SMEs, which are experience significant cost barriers to RFID deployment. In-line with its open-source nature this platform aims at offering immense flexibility and maximum freedom to potential developers and deployers to incorporate heterogeneous physical devices into their applications by offering easy-to-use web service interfaces for controlling any type of physical device irrespective of its network technology such as Bluetooth, RFID, ZigBee, RFID, WiFi, etc.. This versatility includes the freedom of choice associated with the hardware.

5 Acknowledgment

This work has been performed in the framework of ASPIRE and HYDRA, ICT Projects partly funded by the European Commission. The Authors would like to acknowledge the contribution of their colleagues from the ASPIRE and HYDRA Consortium.

6 References

[1] Kostelnik P, Ahlsen M, Axling M, Sarnovsky M, Rosengren P, Hreno J, Kool P, Semantic Devices for Ambient Environment Middleware, proceedings of the TrustAMI 2008, Sophia Antipolis September 2008

[2] Amigo middleware core: Prototype implementation and documentation, Deliverable 3.2. Technical report, Amigo Project, IST2004004182, 2006.

[3] FIPA Device Ontology Specification, Foundation for intelligent physical agents, 2002.

[4] HYDRA: Networked Embedded System middleware for Heterogeneous physical devices in a distributed architecture", Project Proposal, September 2005.

[5] D.L. McGuinness, F. van Harmelen, OWL Web Ontology Language Overview, W3C Recommendation, 2004.

[6] Naval Research Lab. Nrl security ontology, http://chacs.nrl.navy.mil/projects/4SEA/ontology.html, 2007.

[7] OWLS: Semantic Markup for Web Services, 2004.

[8] Ian Horrocks, et. al., SWRL: A Semantic Web Rule Language. W3C Member Submission, 2004.

[9] Delivery Context Ontology. W3C Working Draft 2007

[10] Badii A, Hoffman M, Heider J, MobiPETS: Context-aware mobile service provisioning framework deploying enhanced Personalisation, Privacy and Security Technologies (.PETS), the Proceedings of 1st International Conference on COMmunication System softWAre and MiddlewaRE (COMSWARE).

[11] Badii A, Adetoye A O, Thiemert D, Hoffman M, Hydra Semantic Security Resolution Framework, Proceedings of DIComAe 2009, Paderborn, September 2009

[SOAP] W3C (2000) Simple Object Access Protocol (SOAP) Version 1.1. http://www.w3.org/TR/soap/

[Limbo] Hansen, K. M., Zhang, W., and Fernandes, J. (2008a). Flexible Generation of Pervasive Web Services using OSGi Declarative Services and OWL Ontologies. In Proceedings of the 15th Asia-Pacific Software Engineering Conference, pages 135–142, Beijing, China

[WSDL] W3C (2001) Web Services Description Language (WSDL) 1.1. http://www.w3.org/TR/wsdl

[SeMaPs] Zhang, W., Hansen, K.M., Kunz, T. (2009). Enhancing intelligence and dependability of a product line enabled pervasive middleware. Elsevier Pervasive and Mobile Computing, doi:10.1016/j.pmcj.2009.07.002, in press.

[EPC] Application Level Events 1.1(ALE 1.1) Overview, Filtering & Collection WG, EPCglobal, March 5, 2008 , available at: http://www.epcglobalinc.org/standards/ale

[FLOER] C. Floerkemeier and S. Sarma, "An Overview of RFID System Interfaces and Reader Protocols", 2008 IEEE International Conference on RFID, The Venetian, Las Vegas, Nevada, USA, April 16-17, 2008.

[AS43b] ASPIRE D4.3b Programmable Filters – FML Specification

4.9 Usage of RFID in the Forest & Wood Industry and Contribution to Environmental Protection

Indisputable Key Project

Janne Häkli; Kaarle Jaakkola; Kaj Nummila / Åsa Nilsson / Ville Puntanen; Antti Sirkka

VTT, Finland / IVL, Sweden / Tieto, Finland

Abstract: Novel RFID technology and solutions for the wood products industry have been developed in the Indisputable Key project: pulping compatible biodegradable UHF transponders and robust RFID readers for use in the forest in the harvesters and at saw mills. The new technology allows tracing of individual logs from the tree felling to the sawing of the logs at the saw mill. Introduction of traceability in the forestry and wood sector facilitates maximization of the raw material yield, and optimisation and monitoring of environmental impact, by linking the relevant information to the traced objects. By implementing and extending the EPCIS standard the new solution allows the environmental efficiency of a product to be computed accurately at item level, because information regarding processes at each stage of the distributed supply chain can be tracked, analyzed and allocated to the product. Special Key Performance Indicators (KPI) have been established that give easily accessible information on the environmental performance of the product. The environmental KPIs are calculated using the life cycle assessment (LCA) methodology outlined in the ISO 14040 standard. The industrial benefits of monitoring environmental KPIs are e.g. awareness of the current environmental performance of the production, detection of potential new products with a competitive edge and enhanced environmental management. Furthermore, traceability in the wood sector is a way to guarantee that a particular product is made of wood coming from certified forests.

1 Introduction

The Indisputable key project (10/2006-03/2010) develops tools and knowledge to enable a significant increase in raw material yield and in utilisation of production resources in the forest and wood industry, thus decreasing the environmental impact. The main means to achieve these benefits is utilisation of traceability at item level, i.e. at log and board level. This traceability requires novel technology solutions to be developed. The results are also applicable to other biological raw materials at large extent, thus opening up opportunities for a wider use. The project consortium includes 29 partners from 5 countries: Estonia, Finland, France, Norway, and Sweden.

The novel technology development focuses on marking technology for logs and boards and on Traceability Services (TS) software – the repository for item level traceability data and process level data, and services to access and utilise this information by using selected parts of EPCIS interfaces. For log marking, passive EPC C1G2 compatible UHF transponders and readers were developed. Inexpensive printed ink marking methods are used in the board marking.

The Indisputable key systems are implemented at different nodes of the forestry-wood production chain: at harvesting of logs in the forest, at log to board conversion in the saw mill and at the product refinement of the secondary manufacturer. The traceability at item level – logs and boards, allows monitoring and optimisation of the environmental impact by linking the relevant information to the individual logs and boards for calculation of environmental key performance indicators (KPIs). In addition to these, economical KPIs are used to study and optimise the production chain for increased profitability.

The developed technology and the benefits of its use are to be demonstrated in Sweden in 2010 in a case covering the complete wood supply chain – from the tree felling in the forest to a secondary manufacturer using the boards. Parts of the system are also demonstrated in France and used to study and develop the manufacturing processes in Finland and Norway.

2 Traceability in the forest and wood industry

Making information available at different stages along the forestry-wood production chain requires automatic traceability systems. The developed systems are based on the Individual Associated Data (IAD) concept; the measurement and processing data are related to the individual logs or boards so that the traceability includes the data associated with the items. For complete traceability, the items have to be automatically identified at all processing steps and all the associated data has to be stored and be retrievable.

Automatic and reliable identification of each item requires a highly readable unique ID-code for each log or board. The forestry and wood products industry set additional requirements on the item marking technologies: operation in harsh outdoor conditions and industrial environments, suitability for the processing steps of the items, etc. For the logs the selected technology is EPCglobal Class 1 Generation 2 compatible passive UHF RFID-transponders that have a long reading distance and allow a globally unique ID-code for the logs with 96 or 198 bits of data with SGTIN-96 or SGTIN-198 (Serialized Global Trade Item Number). In the board marking inexpensive ink marking is used and sufficient uniqueness of the ID-code is achieved in each process step for the boards in the production chain at the saw mill.

2.1 RFID system for the log identification

The RFID system consists of the transponders, their applicator to the logs, RFID readers and the middleware. The following requirements are set to the transponder used for log marking:

- High readability for reliable and automatic log identification
- Pulping compatibility; the transponder materials need to be harmless in the pulp and subsequent paper making
- Automatic applicability, i.e. fast and reliable attachment of the transponder onto the logs
- Low price

The transponders are attached to the logs automatically by the harvester during the log cutting after the tree felling, the logs are identified using an RFID reader and data collected by the harvester are associated with them. RFID readers are also used in two locations at the saw mill; in the log sorting and in the saw intake. The special requirements for the harvester reader include the following:

- Tolerance to four-season Nordic weather conditions in the forest
- Tolerance to extreme shocks and vibration in the operating harvester during tree felling and log cutting
- Tolerance to liquids, dirt and impacts
- Operation in proximity of large metallic bodies in the harvester.

The readers at saw mills are subject to industrial conditions including outdoor temperatures, dust, dirt, vibration, shocks and impacts.

The requirements for the RFID systems are such that no satisfactory commercial solutions for log tracing existed prior to the project and therefore novel technology was developed.

2.1.1 Transponders

High readability of automatic log identification requires a long reading distance in excess of 1 metre. In addition to the long reading distance, high transponder survivability is needed as only functioning transponders can be read. To achieve high readability the UHF technology was selected. For improved survivability, the transponder is inserted into the log so that it is protected by the surrounding wood during the log handling (transporting on conveyors and with forklifts and cranes) at different processing steps. Wood as a natural material is a challenging environment for the transponder; its electrical properties are strongly affected by the varying moisture content. For automatic application into the wood, the transponder size and shape need to be optimised for penetration into the wood. High electromagnetic losses in moist wood with large variation as well as variations in the permittivity in and between the logs make the transponder antenna design challenging. The main challenge was to achieve a sufficiently long and consistent reading distance also in the worst reading conditions, with a transponder that can be easily automatically inserted into a log.

Wood chippings, made from the parts of the logs that are not sawn into boards, are used as raw material at pulp mills that supply the raw material to the paper mills. In principle, the material to be pulped is not allowed to contain any plastics, metal or coal. The commercial transponders usually contain plastic, which is forbidden to end up in the pulp and in the subsequent paper making. Transponders made of pulping compatible materials with only a minimal amount of less harmful plastics than the commonly used transponder materials were developed. The transponder materials need to have low electrical losses to allow a good transponder reading range and to be mechanically durable for the transponder insertion into the logs. The materials also have to be inexpensive and suitable for mass production of the transponders to keep the transponder price low. The casing of the transponder developed for log marking is made of durable artificial wood material that is suitable for the pulping processes, has reasonably low electrical losses and is relatively inexpensive.

A novel transponder (patents pending) encased in artificial wood material was developed to meet the requirements on transponders for automatic marking of logs. The developed transponder is an approximately 80 mm long wedge that is inserted into the log end by the harvester. The transponder is shown in Figure 4.9-1. The reading range of the transponder was measured to be over 2.5 m inside a fresh moist log at the European UHF RFID frequencies.

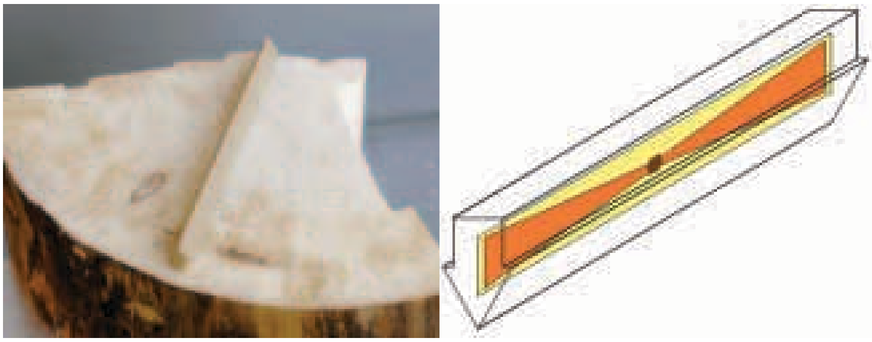


Figure 4.9-1: Developed UHF transponder for marking logs.

2.1.2 Transponder applicator

The transponders are inserted into the logs using an applicator – a manual insertion tool or an automatic device on the harvester machine. Both manual and automatic applicators were developed. Manual marking of logs with the transponders is shown in Figure 4.9-2. An experienced applicator user has a success rate exceeding 95 % in the application attempts. The automatic application is expected to be more reliable and repeatable than the manual application.

Figure 4.9-2: Manual application of the transponder into the log end.

2.1.3 RFID readers

The logs are marked and identified when the tree is cut into logs by the harvester. A robust RFID reader with a patented adaptive RF front-end that compensates the effects of metal in the vicinity of the reader antenna was developed for installation in the harvester head. The reader was tested to survive the outdoor temperatures and to operate under vibrations and shocks at the levels specified in ISO 15003 (2 G vibration at 10–2000 Hz, 50 G shocks), which specifies the environmental resistance testing for electronic devices for agricultural machines. The reader is enclosed into a robust IP67 casing. The reader prototype is shown in Figure 4.9-3 together with a reader set-up at a saw mill.

The RFID reader is controlled over a CAN-bus in the harvester using EPCglobal's Reader Protocol. For implementing the Reader Protocol over the CAN-bus a new Messaging/Transport Binding (MTB) was developed.

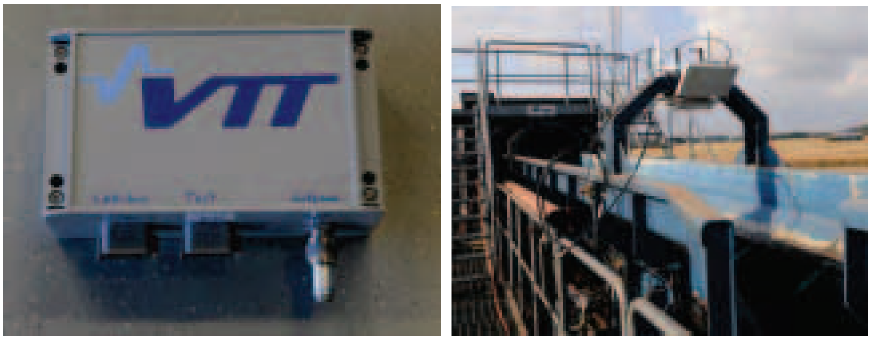


Figure 4.9-3: Developed RFID reader for the harvester and a test reader set-up at a saw mill.

At the saw mill, commercial RFID readers (Sirit IN510) were used with specially developed software for log identification and singulation. The readers were placed into robust aluminium casings to protect them from possible impacts, dirt and dust. Robust metal antennas (Intermec IA33D Antenna Cell) were integrated to the reader casings. The integrated reader set-ups were positioned over the conveyor at the log sorting, where the logs are received at the saw mill, and at the saw intake, before the logs are sawn into boards, at two saw mills; one in Sweden and another one in Finland. The reader position over the conveyor allows the reader installation at the saw mills with minimal changes to the existing conveyors. A read rate of approximately 100 % was achieved for operating transponders inside the log ends in the tests at saw mills. The read rate is affected by the survival of the transponders in the logs, which depends on the success of the application into the log end. Transponders that are not fully inserted are vulnerable to damage during the handling of the logs.

2.2 Traceability services

Indisputable Key project's view of traceability is more than just knowing the location of an object. In addition to location information, the information related to the production/processing throughout the supply chain is gathered, e.g. processing conditions and wood quality parameters.

Traceability Services (TS) enables traceability and visibility of products in the distributed supply chain. By rolling out Traceability Services the organisation can monitor and analyse the efficiency of its processes and value chain in real time.

Traceability Services

- Connects the steps of the supply chain together
- Provides a common data model for the whole supply chain
- Enables statistical and logical analysis of large sets of transaction data which can be used in Enterprise Resource Planning
- Provides the metrics to monitor and analyse the performance of a company.

By combining the process information of the supply chain and the traceability data about products travelling through the supply chain Traceability Services enables new methods for analyzing the performance of the organisation. The modules of Traceability Services have the capability for receiving and processing environmental product and process properties.

The performance of products can be compared and analyzed between different steps; e.g. how the environmental performance of products is affected by the use of different transport processes having varying environmental properties (diesel vs. biodiesel as the energy source). Another possibility is to analyze how a certain product property affects another product property. For example, how the area of origin of the log affects the board quality.

The purpose of Traceability Services is to act as a repository for item level trace¬ability data and process level data and to provide services based on this information. This is realised by utilizing the extension point provided by EPCIS Standard [1].

The solution connects the steps of the supply chain together and provides a common data model for the whole supply chain. The solution offers services for monitoring environmental, economic and social performance of an organisation.

2.2.1 Traceability Data Repository

The Traceability Data Repository is a set of databases and data warehouses designed for storing traceability data and master data from the supply chain. Data warehouses enable detailed analysis of data and the calculation of the economic and environmental KPIs.

TS KPI Calculations are a set of configured formulas that are used to calculate economical, environmental and quality key performance indicators. Different kind of formulas for KPI calculations can be fed to the calculation engine and presented in TS Reports and TS Analytics. The Environmental KPIs used in the Indisputable Key are presented in Chapter 3.

2.2.2 Visualisation and Analysis of the traceability information

Traceability Services consists of a set of different business intelligence tools to visualise and analyse the traceability information.

TS Reports offers KPI visualization and different reporting possibilities, including export of the reported data for local use by the researcher. TS Reports is implemented on Performance Point Server and Microsoft Office Sharepoint Server 2007. By using TS Reports the user can monitor the performance of the organisation.

TS Analytics provides a user interface through Pro Clarity tool to advanced users for detailed analysis of the collected data exploiting the data from TS Repository database and data warehouses. ProClarity Analytics provides a powerful yet simple to-use analysis tools to cover everything ranging from ad-hoc querying to sophisticated analytic modelling. In Figure 4.9-4 there is an example where the user compares log diameter measurements in the forest and in the saw mill. Based on this information a company can calibrate its measurement devices automatically.

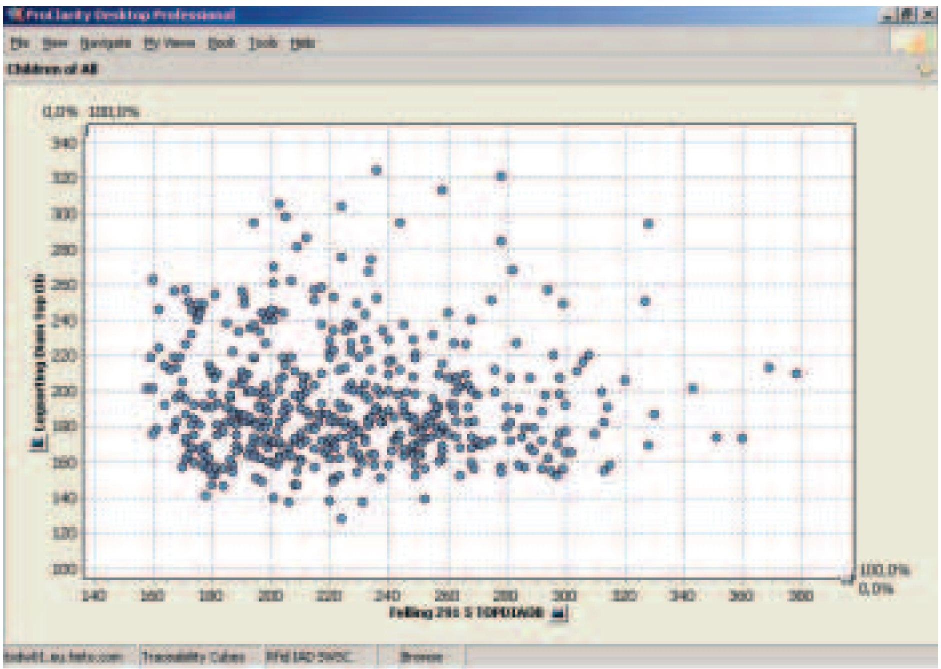


Figure 4.9-4: Analysing in TS Analytics.

2.2.3 Integration to source systems

The integration to source systems is realized with adapters to acquire and share the traceability data together with the process data. Traceability Services allows integrating EPC compliant readers into the system by supporting the Reader Protocol [RP 1.1] standard [2]. The new interfaces introduced in the Indisputable Key project support integration of non EPC standard readers to Traceability Services.

TS Visibility offers comprehensive visibility of products in the distributed supply chain by implementing selected parts of the EPCIS Query and Capture interface.

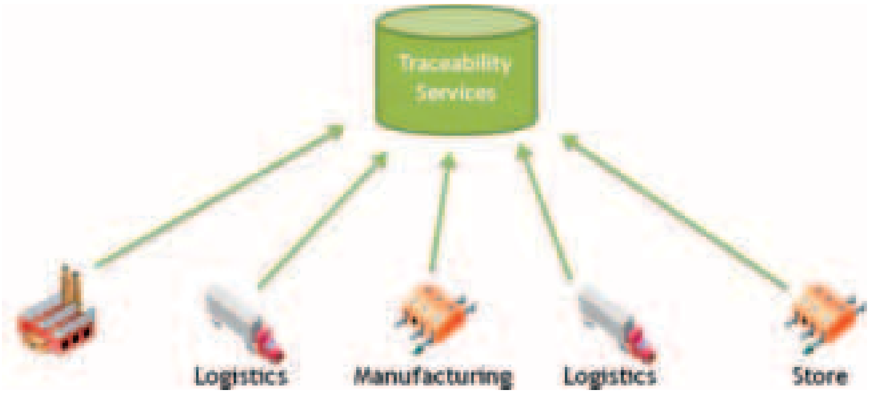


Figure 4.9-5: Visibility throughout the supply chain.

The IK extension to EPCGlobal interfaces enables Traceability Services to connect product traceability data to process information which provides means to monitor and analyse the performance of a company in real time.

3 Monitoring environmental performance

Continuous monitoring and control of processing conditions and product quality is normal procedure in most of today's industrial production. Introduction of the necessary tools for a similar follow-up on the environmental performance of the production processes and the generated products gives the industry the opportunity to be more actively involved in the environmental protection. This is part of the traceability system developed in Indisputable Key, where it is applied and tested in the wood products industry. The impact on the environment is registered in the traceability system and easily accessible to the user.

On-line monitoring of the environmental performance brings the potential to detect appropriate improvements in the process to limit the environmental impact caused by the production. The methodology can be used either for the entire wood supply chain or for a separate process in the supply chain. On-line monitoring of environmental performance is not restricted to the wood products industry. The same methodology can be applied in any production chain or process. A similar application was developed and applied at a municipal wastewater treatment plant in the EU FP6 project HIPCON [3].

The conventional approach for analyzing the environmental impact of product manufacturing is to calculate the yearly average impact based on annual information. Compared to that approach the more detailed information recorded in the traceability system, collected from different parts of the supply chain and related to an individual product or a product batch, provides a much more effective base for proactive environmental management in the industry.

3.1 Key Performance Indicators

In order to keep the information presented to the industrial user at a comprehensible level, whilst still meeting the project objective to create a tool that includes environmental impact from a life-cycle perspective, a set of environmental Key Performance Indicators (KPI) for use in the wood industry were defined. The majority of the proposed KPIs were established in line with the international LCA standard (ISO 14040 and ISO 14044) with some additions of specific KPIs of particular interest for the wood products industry. 11 indicators are used in the project:

1. Climate change
2. Acidification
3. Eutrophication
4. Stratospheric ozone depletion
5. Ground level photochemical ozone
6. Depletion of non-renewable resources
7. Human and ecological toxicity
8. Biodiversity
9. Resource use
10. Generated waste
11. Water emissions

An overview of the LCA procedure, creating the base for these KPIs, is presented in the White Paper - How to gain from measuring environmental impact from wood products [4].

The indicators are calculated and presented in Traceability Services (TS). The TS allows the environmental impact from production of a product to be computed at item level, because information regarding processes at each stage of production is tracked and used as input to the calculation of the KPIs. Typical information which is needed in the KPI calculation is direct emissions to air (e.g. CO2 and particles), raw material use, resource consumption, energy use, generation of waste, production volumes and the ratio of different products. An initial inventory of the current situation is required for correct configuration of the KPIs in TS. When inputs are not measured on-line, and thus not available for automatic tracking in TS, results of the inventory can be used as default values. The more detailed information that is gathered in TS from each stage of production the higher the specificity of the KPI and the higher the potential benefits for the users.

The KPIs reflect the environmental impact of production. Thus the aim for an industrial user is to keep the values of the KPI as low as possible. The front page of the environmental interface of the system developed in Indisputable Key can be configured according to user preferences, with information on e.g. values of the most interesting KPIs and contribution to a KPI from the different processing stages, see Figure 4.9-6.

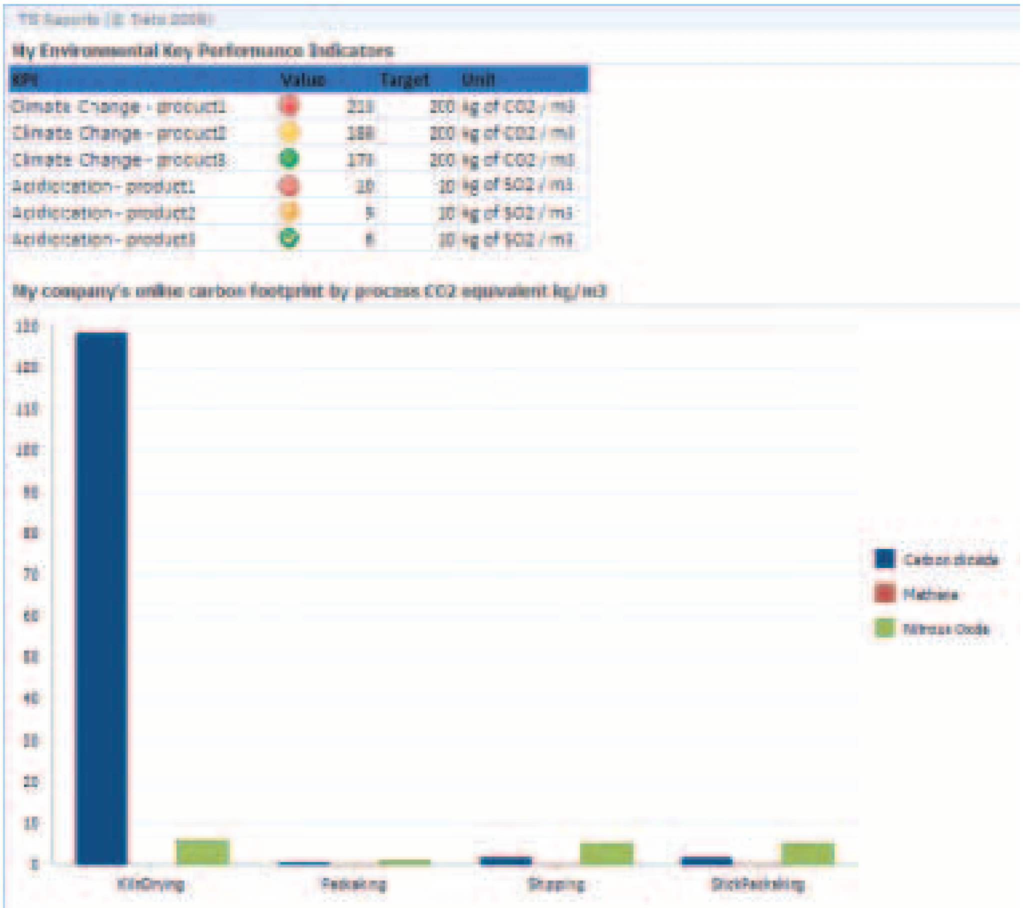


Figure 4.9-6: Front page of the environmental interface provides the industrial user with his preferred information. The example shows information on KPI values, colour indicator on KPI level compared to defined limits and the contribution to the KPI Climate Change from the different production stages.

The user can view the result with different levels of detail. The most aggregated level is to present the accumulated KPI value for all the stages of the entire production chain. From that it is possible to drill down and get information on the contribution from separate stages (e.g. harvesting, transport and saw mill) and different processes within a production stage (e.g. log sorting, sawing and green sorting in the saw mill). It is also possible to analyse which of the used resources has the largest contribution to the selected KPI. The impact from resources stems from their production and the transport to the location where they are used (i.e. impact is based on LCA results for the resources). Direct emissions occurring in the supply chain are also presented.

3.2 Environmental benefits

The environmental KPIs should be viewed as a tool for the industrial user to enhance the company's environmental management and thus taking an active part in contributing to environmental protection. As such, the tool brings great potential benefits. The actual magnitude of the environmental benefits for an industrial user depends on the involvement and interest of the personnel. Company policies can play an important role. A company with a clearly stated policy for environmental management, with the goal to reduce its impact on the environment, has already the necessary incentive to motivate the personnel into active use of the KPIs.

In order for a company to take actions towards a more environmental friendly production, the first step is to assess the current environmental impact of the product. When this is known, potential improvements can be identified and actions can be taken. The current status of environmental impact is documented in the initial inventory that precedes the configuration of KPIs in Traceability Services. The industrial user can then follow-up on the KPIs in the TS and benchmark against the inventory results, aiming for improved production compared to the annual averages that were the outcome of the initial inventory. The important extra benefit from a more detailed follow up on the environmental performance is the possibility to study and take action on variation over time. Allocation of KPIs to individual items, such as logs and boards, which is the novel idea developed in Indisputable Key adds an extra dimension to the production control and refinement. The information collected in the traceability system enables a continuous improvement and fine-tuning of the production stages.

The methodology developed in Indisputable Key, which introduces traceability in the wood supply chain and a tool for calculating environmental KPIs, has a major advantage in preventing the risk of sub-optimisation caused by overlooking effects in other parts of the supply chain. Traceability enables the complete view of the entire supply chain, as exemplified in Figure 4.9-7. With this kind of information available, the industry can easily identify which parts of the supply chain are the "hot spots" with respect to the environmental impacts monitored by the KPIs. Collaborative action can then be taken by the actors in the supply chain to reduce the impact, starting with the most critical stages.

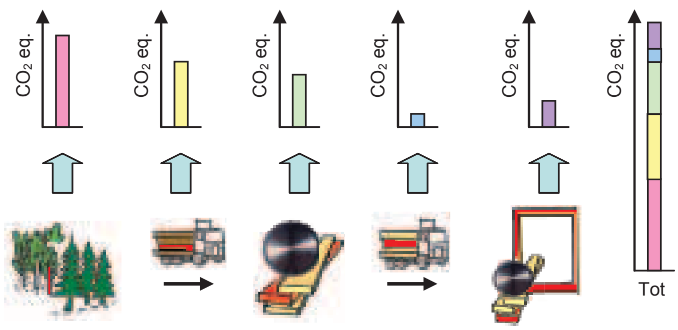


Figure 4.9-7: Information about direct emissions contributing to the KPI Climate Change (in the unit CO2 equivalents) from production of a window frame is collected from the different stages in the supply chain. The tracked item is illustrated with the colour red. The total value for the window frame consists of the contribution from harvesting, transport from the forest to the saw mill, production of boards at the saw mill, transport from the saw mill to the secondary manufacturer and finally production of a window frame.

The system architecture developed in Indisputable Key creates a link between the final product and its origin. This makes it possible to trace information up-streams in the supply chain all the way to the harvesting of the tree. In other words, the origin of a wood product (e.g. when and where the tree was cut) is possible to read from the traceability system. This feature can help prevent illegal cutting and it can provide the information needed to guarantee that a product is made from wood coming from certified forests.

The environmental KPIs harmonize with the required content of an Environmental Product Declaration (EPD), thus facilitating the creation of EPDs for the products of the industrial user. EPDs describe the environmental characteristics of a product or a service from a life cycle perspective. The overall goal is to provide relevant, verified and comparable information to meet the customer and market needs. An EPD can be used for benchmarking the product against other products that could serve the same purpose. In a time with increasing environmental awareness, the fact that a product or service is “green” creates added values amongst the customers.

Active monitoring and control of the environmental impact of production has the additional advantage that it can raise attention to process improvements that might otherwise be overlooked. The fact that the KPIs take into account the environmental burden from manufacturing of resources used by the wood products industry (e.g. electricity, diesel and glue) makes it possible to detect excessive use of external resources. Limiting the use of resources has a positive effect on the environment as well as the economy of production, which is sometimes of higher priority for the industrial user.

4 Conclusion

Novel technology for traceability in the forest and wood industry was developed; pulping compatible UHF transponders for log marking, robust RFID readers for harvesters and saw mills and Traceability Services software. Traceability Services connects the steps of the supply chain together and allows new methods to analyze the performance of the whole chain and any process, service and or product within. The traceability system and its benefits are to be demonstrated in 2010 in a complete forest supply chain in Sweden.

Indisputable Key has provided the tools necessary for the wood industry to become more proactive with respect to environmental protection. Monitoring of environmental KPIs makes it possible to achieve the following advantages for the industrial user:

- Status of environmental performance
- Detection of potential improvements
- Basis for optimisation of environmental impact
- On-line monitoring and control of environmental impact
- Environmental benchmarking
- Environmental management
- Marketing purposes such as EPDs or support for eco-labelling

The magnitude of the achieved benefits are very much dependant on the industrial users engagement and interest in making use of the developed technology.

5 References

[1] EPCglobal, “EPC Information Services (EPCIS) Version 1.0.1 Specification,” EPCglobal Ratified Standard, September 2007,http://www.epcglobalinc.org/standards/epcis/epcis_1_0_1-standard-20070921.pdf.

[2] EPCglobal, “EPCglobal Reader Protocol Standard, Version 1.1,” EPCglobal Ratified Standard, June 2006, http://www.epcglobalinc.org/standards/rp/rp_1_1-standard- 20060621.pdf.

[3] Holistic Integrated Process Control (HIPCON), EU FP6 project, NMP STRP 505467-1, http://www.hipcon.org.

[4] Erlandsson M, Nilsson S, Nilsson Å (2008): White paper - How to gain from measuring environmental impact from wood products, available at http://www.indisputablekey.com.

4.10 RACE networkRFID – Stimulating the take-up of RFID in Europe

Ian G. Smith

Chairman RACE network-RFID Management Board, President of AIM UK

Abstract: The RACE networkRFID project has been developed to raise awareness of Radio Frequency Identification across Europe through the establishment of a federating platform for all key European stakeholders in the development and use of RFID technology and applications.
The global RFID market is forecast to grow from $5.3 billion today to $27 billion by 2018. Whilst the USA and China are currently the biggest RFID spenders it is confidently anticipated that the European market will show significant growth over the next 10 years.
For precisely these reasons RACE has been structured as a truly international network or forum, open to partners across the Community. This is essential for the optimum exchange of ideas on best practices in RFID and for continued international progress on standards and applications.

1 Introduction

The three-year RACE networkRFID project was launched in March 2009 and in its first year of operation the partners have made good progress. Membership will double in this first year. Direct contact has been made with SME organisations across Europe who represent millions of small businesses – a major target of the project. A comprehensive new website is under construction which will be launched at the March 2010 General Assembly providing a comprehensive guide to Radio Frequency Identification that should be of interest to end users and educators as well as suppliers and integrators. It will link with a very comprehensive database of "applications and deployments" allowing companies to share with the network their RFID projects and "know how." The database will also give the general public a tool to access RFID case studies from around Europe.

One of the early deliverables has seen the production of an RFID Market Analysis Report which summarises information from 20 published reports highlighting current state of the art in both technology and market conditions.

Partners are working energetically on a number of key European initiatives including the development of Europe's Privacy Impact Assessment, developing a harmonized RFID sign, and defining common terminology. The key goal in 2010 is to engage with the appropriate Government Department's of all Members States and ensure the widest possible dissemination of the benefits of RFID to the widest possible audience.

1.1 Project description and objectives

The objectives for RACE networkRFID have been developed from the needs identified by the ICT PSP for a thematic network for RFID, namely:

1. Creating a federating platform to the benefit of all European Stakeholders in the development, adoption and usage of RFID.
2. Positioning the European Union as a world leader in RFID excellence.
3. Establishing the market position for RFID in Europe, defining the roadmap and addressing the barriers to adoption and deployment as well as fragmentation in the market.
4. Promoting best practices, case studies, reports, guidelines, events and services to increase awareness at European and national level.

5. Involving a large number of Member States' authorities dealing with public RFID issues, including involvement of major industry (automotive, aerospace, etc...), civil society, RFID advocacy groups and research agencies where relevant.

In addition RACE networkRFID will include the following key objectives:

6. Providing a structure for initiating, developing, and sustaining a large variety of support measures to promote the take-up of RFID with appropriate attention to associated automatic identification, data capture and communication technologies and their potential within application designs.
7. Focusing attention upon the SME business communities and the potential that exists within these communities for product, process and services innovation.
8. Addressing the requirements of policy-makers and the general public to ensure that both businesses and consumers benefit from RFID with a specific focus on consumer trust and acceptance, innovation and enterprise.

The objectives are seen as being mutually inclusive and tempered by the need to accommodate consideration for sustainability, change management in relation to market needs, concept and technological developments and thought leadership for positioning Europe as a world leader in RFID and associated technologies. The concept on how to fulfil the vision of a central platform will be developed and should be approved by a general assembly of interested stakeholders over the period of the project.

A logical approach to achieving a self-sustaining federated network structure, offering both collaboration and independence of contributory stakeholders, is to provide a framework and a set of deliverables for creating member-state-funded national centres for RFID and object connected technologies.

The founding Management Board of RACE networkRFID propose to link this framework to what they are calling a supporting central platform that can accommodate, on an on-going basis, key objectives which will help achieve a coherent and effective platform for informing and involving Member States of key European and international issues concerning RFID. This will accommodate new developments, concepts, research outcomes and event services (seminars, enterprise events and conferences), building upon and extending the European Commission's RFID Expert Group activities in a new form for strengthening Europe's involvement, understanding and exploitation of RFID.

The RACE networkRFID consortium recognises the need to consider and accommodate a number of specific issues of direct significance in seeking to achieve the aims and objectives of a European thematic network for RFID. These issues include:

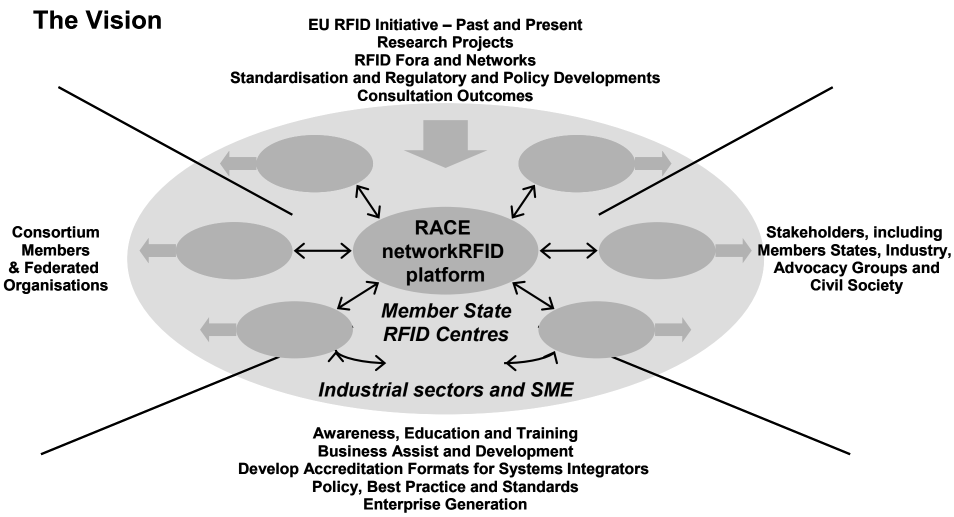
- Lack of awareness and understanding of the technology dimensions, attributes and foundations for selection both within the prospective end-user community and a percentage of the vendor and support communities
- Take-up requires greater attention to SME and end-user needs and business development and assist initiatives supported by accredited advisors and appropriate follow-through support
- Enterprise awareness and follow-through initiatives are required to assist SMEs exploit the potential on offer through RFID and the 'Internet of Things', using existing SME application examples of enterprise and innovation
- RFID requires positioning with respect to other automatic identification and data carrier technologies – more appropriately object-connected technologies and real world awareness (RWA)
- Consumer trust and security, as well as "privacy friendly development" aspects
- Positioning is also considered important with respect to the emerging concept of the 'Internet of Things' and the associated developments in the Internet (Web 2.0 and semantic web)
- Greater attention to integration capabilities is required with respect to other identification (including natural feature identification), location, security, sensory and local communication technologies
- The RACE network RFID consortium will collaborate with the relevant EU projects relating to all standardisation issues
- Attention to design, risk assessment socio-economic issues and application principles

- Implementation practicalities, coexistence and layered interfacing and networking issues.

In paying collective attention to the ICT PSP aims and objectives and these additional issues the prospect is seen for a network, orchestrated through a central platform that will provide the necessary transformational conduit linking the current EU investment outcomes with a user community receptive to the potential and the opportunities for innovation and enterprise and the need to establish and maintain competitive advantage. The proposed central platform would also be seen as a vehicle for sharing knowledge and expertise arising from member states and as a point of promotion and roll-out for thematic initiatives, such as business development programmes that will have relevance across member states.

RACE networkRFID is also seen as a platform for sharing knowledge and expertise arising from Member States and as a point of promotion and roll-out for thematic initiatives, such as business development and assist programmes that will have relevance across member states.

2 The Vision



The collective vision for the federated network is to provide a network of excellence for raising the wealth creating and competitive status of European member states in the area of RFID usage, thought leadership and development, and positioning within mainstream information and communications technology (ICT). The network will draw upon expertise of Member States and the evolving RFID community to create a dynamic, change-responsive capability that not only aligns with the initial Information and Communication Technologies Policy Support Programme (ICT PSP) objectives, but extends that capability to accommodate emergent and future needs.

The proposed central platform will provide the conduit for deriving user-facing potential from EU RFID initiatives and outcomes, together with structured support services, and convey them effectively to the European Community, initially through a network of members, but ultimately through a network of member state centres. With some member states government representatives and national administrations already supporting such centres, a move towards growing the network and federating these facilities is both logical and possible.

The full set of RACE networkRFID objectives map into a framework of work packages which will meet the intrinsic requirements, identified in the ICT PSP objectives for 2008, for actions aimed at mobilizing stakeholders to:

- Share experiences
- Build consensus around common approaches
- Prepare roadmaps for facilitating the uptake of innovative ICT RFID based solutions

The work will further develop and promote the platform aims of the European concerted effort on RFID and will:

- Foster on-going RFID consultations
- Federate existing local/national initiatives into a co-ordinated European initiative on RFID

- Maintain a roadmap of the relevant technologies, their applications and how to deal with the potential privacy and security issues
- Create an environment for progress in related European standardisation and critical governance infrastructure issues.
- Monitor and, where appropriate, link to RFID policy initiatives in other regions of the world
- Identify best practices to achieve progress towards a single market for RFID applications by raising awareness and removing barriers to its effective, secure and privacy-friendly deployment
- Support the EU/US transatlantic "lighthouse priority project" on RFID

2.1 Policy background and EU dimension

Policy decisions are extremely critical as they constitute a fundamental pillar in assisting the development of an environment that is favourable to the adoption of RFID applications. Policies at EU and national level can play an important role in lifting non technical barriers to the adoption of RFID, by giving an appropriate level of certainty to the market actors and confidence to consumers and citizens in general.

These are indispensable prerequisites to the firm take up of RFID technology in Europe. For this reason, RACE networkRFID has gathered together international participants from the industry, standards organizations and consumer groups from diverse origin, interest, size and points of view but each have in common the desire for a stable successful take up of the technology, for the benefit of the society in general.

2.2 Towards an EU internal market of RFID and its applications with a focus on SMEs

Any approach taken by a particular area of public policy in the EU is then executed at national level, so it is important to assure coordination of national initiatives and policy measures in order to guarantee **an internal market for the technology and the multiple applications it serves**. In this sense, RACE networkRFID has foreseen a specific Work package on "Harmonization of Related Projects" (WP 4), which intends to identify collaboration possibilities and liaise with existing projects and organizations.

In addition work packages dedicated to "Dissemination" and "Awareness" will also facilitate the task of contributing towards an internal market, as the dissemination and awareness aim to happen across multiple member states.

2.3 Enhancing the competitiveness of the European industry in a global world

The analysis of current policies, their impact on RFID applications implementation on the one hand, and the identification of policies that contribute to enhancing the competitiveness of industry sectors and Small and Medium enterprises on the other, will be an integral part of RACE networkRFID throughout all its Work Packages. This multifaceted approach will result in a more enriching view and contribution to policy makers, based on practical experience and gaining from the synergies created by the work within the RACE networkRFID.

In addition, the linkage between different policies that converge in the use of RFID technologies cannot be seen in an isolated manner either geographically or by sector. This is why RACE networkRFID will not only connect with major European industry sectors, but also with SMEs and their customers as they will play an essential role in the adoption and usage of RFID. Furthermore, RACE networkRFID will address competitiveness not only from a European perspective but also in the context of policy developments in other parts of the world, principally Asia and the United States, so underlining the fact that the advancement of RFID applications and standards is truly global phenomenon.

2.4 i2010 Consumer confidence in the information society era

In determining the focus on policies that are relevant for RFID adoption, the activities of RACE networkRFID will also be informed by the i2010 EU Strategy- a European information Society Framework for Growth and Employment, which promotes the positive contribution that ICT technologies can make to the economy, society and personal quality of life, and with special attention to consumer confidence, privacy and security of RFID applications as well as awareness about the benefits that these bring to the European society at large. It will also be essential for the network to contribute to enhancing consumer confidence in RFID by addressing underlying ethical, trust and security concerns, in particular by considering potential privacy - friendly development aspects.

3 Impact

3.1 Expected outcomes

There are four principal outcomes to be expected from the work and activities of the thematic network. These outcomes will address each of the three policy implementation themes identified in the ICT PSP Work Programme.

1. Extended platform for developing and promoting policy for RFID in line with the objectives of ICT PSP, and embodying the principle of consultation as a basis for deriving policy.
2. European–wide awareness and adoption of RFID and associated technologies concentrating upon awareness, business assist, business development, innovation and enterprise and the collective goal of wealth creation and competitive advantage for Europe – growing the market 'cake' and enjoying a greater slice of it.
3. Empowering of the greater SME community in exploiting the potential of RFID, associated technologies and the realistic potential arising from radical concepts such as the 'Internet of Things.'
4. A Thematic Network able to grow into a central platform providing an infrastructure for promoting a consistent, coherent European-wide message and policy with regard to RFID.

3.2 Expected impacts

RACE networkRFID expects to achieve significant impact across Europe in the take-up and exploitation of RFID and associated technologies by SMEs, larger organisations and the Public Sector.

To foster RFID deployment and increase awareness across a wide array of relevant communities, the RACE networkRFID consortium relies on the broad range and expertise of its partners.

Engaging appropriately with the vast SME community provides a concrete opportunity for exploiting the revolutionary and radical potential of RFID. It is revolutionary because of its relevance to virtually every sector of industry, commerce and services; and radical in the potential it provides for improving and realising new processes, services and products. Therefore, one of the partners in the RACE networkRFID project is UEAPME, the European SME umbrella organisation which incorporates 87 member organisations across Europe. They consist of national cross-sectoral SME federations, European branch federations and other associate members which support the SME community. UEAPME represents more than 12 million enterprises which employ more than 55 million people across Europe.

By engaging with larger organisations and by closely linking with activities promoting existing and generating new standards, the network is expecting to have a direct impact on the remaining bottlenecks that hinder RFID deployment. In particular, by addressing application standards, significant impact can be expected in open systems and supply chain applications.

In 2010 the key project objectives are to create greater awareness of the benefits and potential of RFID among SMEs across Europe; engage with appropriate Government departments across the 27 Member States; and significantly increase the number of project partners.

4 Members

The RACE networkRFID community involves both Contractual Members and Associate Members. The Contractual Members are signatory to the contract with the European Commission, and Associate Members are partner organisations joining the network after its contractual start.

Contractual Members:

- ERCIM (France)
- GS1 (Europe)
- FHG IML (Germany)
- FILRFID/CNRFID (France)
- ETSI (Europe)
- IF RFID (Germany)
- IBERLOG (Portugal)
- AIM (UK)
- AIDC (UK)
- RFID PLATFORM (Netherlands)
- AUEB (Greece)
- RFIDSEC (Denmark)
- ISMB (Italy)
- UNIMAN (UK)
- ARDACO (Slovakia)
- ITT (Ireland)
- ROBOTIKER (Spain)
- VTT (Finland)
- TREVI (Italy)
- RAND Europe (UK)
- SINTEF (Norway)
- RFID NORDIC (Sweden)
- UEAPME (Europe)
- BIBA (Germany)
- INTERNET VECI (Czech Republic)

Associate Members:

- CNIPA (Italy)
- Institute of Shipping Economics and Logistics (Germany)
- Mondi AG (Austria)
- Link (Portugal)
- CYCLOPS (Turkey)
- Aston University (UK)
- VDEB (Germany)
- CEDT (Portugal)
- CATTID (Italy)
- Pepperl+Fuchs GmbH (Germany)
- Consejo General de Colegios Oficiales de Farmacéuticos de España (Spain)
- Research Group RI-ComET at HTW des Saarlandes (Germany)
- Friendly Technologies (United Kingdom)
- Georgia Tech Ireland (Ireland)
- University of Craiova (Romania)
- Fraunhofer Institute for Integrated Circuits (Germany)
- AIM-D e.V. (Germany, Austria, Switzerland)
- CLECAT (Belgium)
- K.U. Leuven Association (Belgium)
- National AIDC Centre for Wales (UK)
- Cheshire Henbury (UK)
- METRO Group (Germany)
- BITKOM e.V. (Germany)
- Intel GmbH (Germany)
- Not Innovated Here (Finland)
- Trinity Systems (Greece)
- CISC Semiconductor Design+Consulting GmbH (Austria)
- Picosoft Solutions (Ireland)
- AIDC Global (UK)

4.11 Outlook on Future IoT Applications

EPoSS – European Technology Platform

Ovidiu Vermesan

SINTEF, Norway, ETP EPoSS

Abstract: Internet of Things technology opens the way towards multi dimensional, context aware, and smart environments. The technology is bridging the real, virtual and digital worlds by using wireless connectivity for energy efficient and environmentally friendly applications and services and by respecting the security and privacy of individuals and organisations.

1 Introduction

Tackling the challenges that European society and the world will face in developing the "Future Internet" will require a multidisciplinary approach and coordinated efforts.

Today, there are 36 European Technology Platforms (ETPs), and five Joint Technological Initiatives (JTIs) originated directly from ETPs, covering the most important technological areas. They connect thousands of European companies, knowledge institutes and policy makers and have facilitated the development of a common vision and research agenda for each of the 36 technology fields they represent.

In the context of "Future Internet" there are 10 ETPs that have become important interlocutors for the European Commission for the development of strategic research agendas defining the technologies required for implementing the future internet.

Figure 4.11-1: European Technology Platforms – IoT technology research and development.

EPoSS has close links with other ETPs addressing the IoT technology. Coordination meetings have been held with the other Platforms, facilitated by the fact that several industrial partners were members of these Platforms. An agreement was reached on the different core competencies, but care was taken to insure a smooth integration among different activities, to avoid missing to cover critical elements for the full integration of planned applications.

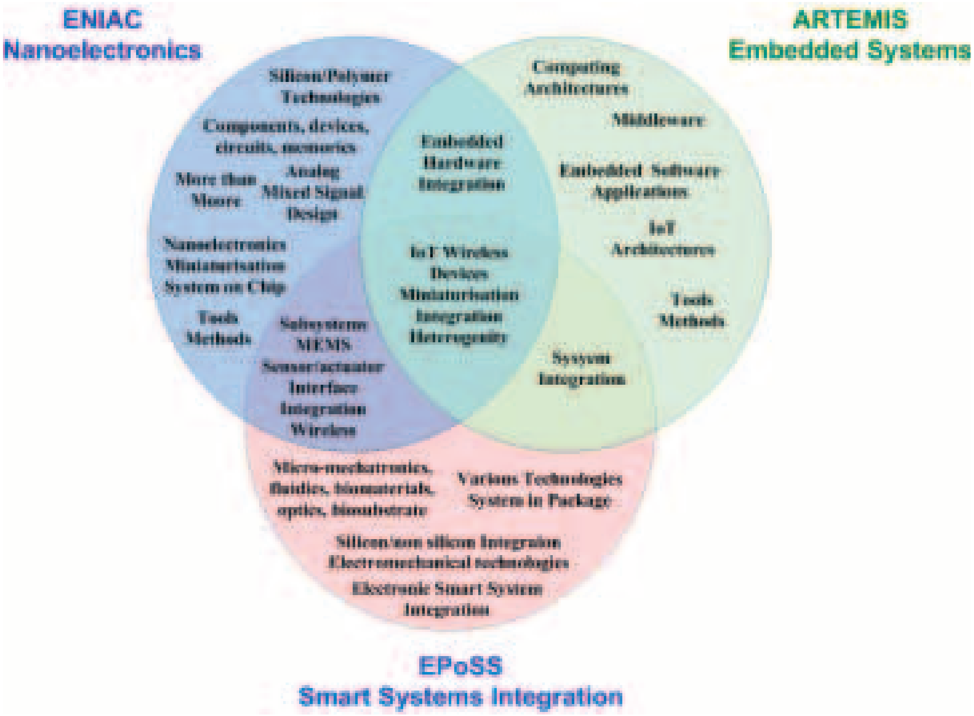


Figure 4.11-2: Core competences for IoT provided by ARTEMIS, ENIAC and EPoSS ETPs.

The three ETPs (ARTEMIS, ENIAC and EPoSS) have cooperated in the definition of the Strategic Research Agendas and (for ENIAC and ARTEMIS) of the content of the JTI.

These technology platforms are organized by final applications, but they target different layers as presented in Figure 4.11-2:

- ENIAC focus is on the development of the Nanoelectronics components, and related equipment, materials and design tools; development of nanoelectronics technologies, devices, circuits architectures and modules
- ARTEMIS focus is on system architecture, system design tools and methodologies and software development;
- EPOSS, which is closer to the final application, focuses on the full integration of the electronic smart system, which combines components developed by ENIAC, software and architecture designed by ARTEMIS, with additional electromechanical technologies.

This paper will focus on the activities of EPOSS, which is the European Technology Platforms that is active in the field of Internet of Things and smart systems integration.

The Internet of the Future, or as it's commonly called, the "Future Internet", will result from the synergic merging of today's computer networks with the Internet of Media (IoM), the Internet of Services (IoS) and Internet of Things (IoT) into a common global IT platform. Complete definitions of these terms have been provided by the Strategic Research Agenda of the CERP-IoT SRA 2009 that is included in this book.

While the current Internet is a collection of rather uniform devices, albeit heterogeneous in some capabilities but very similar for what concerns purpose and properties, the future IoT will exhibit a much higher level of heterogeneity, as totally different objects, in terms of functionality, technology and application fields will belong to the same communication environment.

The IoT as a concept describes a wireless network between objects that would include addressable objects that could be anything from home appliances, food, flowers and pot plants that become connected to the Internet. Some of the things, which are very sensitive to the environment in which they travel, will have sensors attached. This will allow participants to monitor conditions and climate during the entire journey. Under this vision, objects will be able to transport themselves, implement fully automated processes and thus optimise logistics; they will be able to harvest the energy they need; they will configure themselves when exposed to a new environment, and show an “intelligent” behaviour when faced with other objects and deal seamlessly with unforeseen circumstances. Finally, at the end of their lifecycle, they will manage their own disposal or recycling/remanufacturing, helping to preserve the environment.

In this context the technologies such as nanoelectronics, communications, sensors, smart phones, embedded systems and software together with smart wireless identifiable devices will form the backbone of “Internet of Things” infrastructure allowing new services and enabling new applications.

Those smart wireless identifiable devices will provide the means for the fusion of the real, virtual and digital worlds, creating a map of the physical world within the virtual space by using a high temporal and spatial resolution and combining the characteristics of ubiquitous sensor networks and other wireless identifiable devices, while reacting autonomously to the real world and influencing it by running processes that trigger actions, without direct human intervention.

1.1 ID

As their basic functionality, simple tags/devices provide an ID number wirelessly. The devices require no line-of-sight and can be read as long as the tagged item is within range of the reader. The tags are simple, low cost, disposable, and implemented using polymers, SAW (Surface Acoustic Wave), or low cost silicon technologies. Radio-frequency tags are used to identify animals, track goods within the logistics chain and replace printed bar codes at retailers. RFID tags include a chip that typically stores a static number (ID) and an antenna that enables the chip to transmit the stored number to a reader via electromagnetic waves. When the tag comes within range of the appropriate RF reader, the tag is powered by the reader's RF field and transmits its ID to the reader. RFID middleware provides the interface for communication between the interrogator and existing company databases and information management systems.

1.2 Beyond ID

The development of smart systems implies new devices that go beyond wireless identification and include processing capabilities, sensing/monitoring, larger non-volatile memories and combining multiple standards and multiple communication protocols (NFC, RFID, UWB, Rubee, Zigbee, Wi-Fi, or others) to interconnect with other ubiquitous sensor networks and to implement Real Time Location Systems (RTLS). Applications of wireless identifiable smart systems will go beyond mere identification in many areas such as:

- Ambient Intelligence and ubiquitous computing
- Hybrid wireless sensor networks that are characterised by modularity, reliability, flexibility, robustness and scalability.
- Systems using different communication protocols
  - RFID, NFC
  - ZigBee
  - 6LowPAN
  - WirelessHART
  - ISA100.11a
  - UWB
  - Rubee
  - Ultra low power Bluetooth
  - Wi-Fi
  - Wi-Max
- Wireless monitoring of different ambient parameters (video, audio, temperature, light, humidity, smoke, air quality, radiation, energy, etc)
- Mobile robotic sensor networks.

These developments will enable the development of new context and situation based personalised applications and services:

- User context identification
  - Biometrics
  - Privacy mode
  - Attention
  - Gesture
  - Posture

- Social context
  - Surrounding people and/or objects/things
  - Type of group
  - Link to people and/or objects/things
  - Net link - Internet of Things
- Environmental context
  - Location, position
  - Time
  - Condition
  - Physical data

1.3 Beyond RF

The devices used in the future IoT will employ wireless communications using the frequency spectrum beyond the radio frequency range. The table below present the mapping between the frequency spectrum and the existing standards and protocols that are used for implementing wireless identifiable devices.

Table 4.11-1: Summary of standards used for IoT applications.

Range		Frequency Range	Wavelength	Frequency	Standard
LF	Low Frequency	30kHz to 300kHz	10km to 1km	30-50kHz 125/134kHz[1] 131/450kHz	USID ISO/IEC 18000-2 IEEE P1902.1/ RuBee ETSI EN 300 330
MF	Medium Fre-quency	300kHz to 3MHz	1km to 100m		ETSI EN 300 330
HF	High Frequency	3MHz to 30MHz	100m to 10m	6.78MHz[2] 7.4-8.8MHz 13.56MHz 27MHz	ISO/IEC 18000-3 ISO/IEC 15693 ISO/IEC 14443 ISO/IEC 18092/NFC ISO/IEC 10536 EPCglobal EPC HF C1G2 ETSI EN 300 330
VHF	Very High Fre-quency	30MHz to 300MHz	10m to 1m	125MHz	
UHF	Ultra High Fre-quency	300MHz to 3GHz	1m to 10cm	433MHz 840-956MHz 2.45GHz	ISO/IEC 18000-7 ISO/IEC 18000-6 Types A, B. C, D EPCglobal EPC UHF C1G2 IEEE 802.11 ISO/IEC 18000-4 IEEE 802.15 WPAN IEEE 802.15 WPAN Low Rate IEEE 802.15 RFID ETSI EN 300 220 ETSI EN 300 440 ETSI EN 302 208
SHF	Super High Fre-quency	3GHz to 30GHz	10cm to 1cm	3.1-10,6GHz 5.8GHz 24.125GHz	IEEE 802.15.4a WPAN UWB ETSI EN 300 440
EHF	Extremely High Frequency	30GHz to 300GHz	1cm to 1mm		MMID ETSI EN 300 440

1, 2 According to Annex 9 of the ERC Rec 70-03, inductive RFID Reader systems primarily operate either below 135 kHz or at 6.78 or 13.56 MHz.

The correlated transponder (TRP) data return frequencies reside in the following ranges:

LF Range Transponder Frequencies: fC = < 135 kHz, f TRP = 135 to 148.5 kHz

HF Range Transponder Frequencies: fC = 6.78 MHz f TRP = 4.78 to 8.78 MHz

fC = 13.56 MHz f TRP = 11.56 to 15.56 MHz.

2 Technology

The technological developments that are offering the technology basis for IoT are the exponential increase of the processing and storage power of the devices, miniaturisation, ubiquitous connectivity and autonomous behaviour and the ability of devices to connect and to sense i.e. the ability to be intelligent. From the technological point of view, in order to realise the vision of the IoT, several technological advances must be carried out by the research community

The social impact of these three technological trends is the key driver to the Internet of Things.

2.1 Energy

Energy in all its phases of harvesting, conservation and consumption is a key issue in the future. There is a need to research and develop solutions in this area, having as an ultimate objective a level of entropy as close as possible to zero. Current technology development is inadequate 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 etc; 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.

2.2 Intelligence

The **Intelligence** of devices, in particular as regards context awareness and inter-machine communication, is considered a high priority for the IoT. This context awareness is strongly related to information received via sensors, corresponding sensor networks and the capabilities of localisation, as well as the possibilities to influence via appropriate actuators. Besides this, environmental context identification can also be user related or social. Communication capabilities will have to include multi-standard as well as multi-protocol compatibility.

Furthermore, the development of ultra low power designs for mobile IoT devices and a new class of simple and affordable IoT-centric smart systems will be an enabling factor. In that context the terminology of ultra low power design is a broad one - from high efficiency front-ends, ultra low power processors/microcontroller cores, ultra low power signal processing capabilities, ultra low power sensors to low power base stations. however the intelligence of local IoT nodes will be heavily restricted by size, cost and need to mass-produce in high speed, roll-to-roll manufacturing processes, thus keeping the distributed intelligence on a rather low level and accordingly specific. Processing of accumulated information will take place separately.

2.3 Communication

Communication, in terms of physical wave transmission and protocols, will be the cornerstone of the novel IoT architecture. Integration of smart devices into the products themselves will allow significant cost savings and increase the eco-friendliness of products. In the future, application- specific antennae will need to be developed, in order to allow the smooth functioning of applications and services; those antennae will eventually evolve into smart devices themselves, able to reconfigure themselves, and to adapt to the specific application needs and to their surrounding environment.

2.4 Integration

The integration of chips and antennae into non-standard substrates like textiles and paper, even metal laminates and the development of new substrates, conducting paths and bonding materials adapted to harsh environments and for environmentally friendly disposal will become mainstream technologies. RFID inlays with a strap coupling structure 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 antennae will avoid galvanic interconnection and thus increase reliability and allow even faster production processes. The target must 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. This will require ultra-thin structures (< 10 µm) as well as printed electronics, which are both robust and flexible.

2.5 Interoperability

It is common knowledge that two different devices might not be interoperable, even if they are using the same standard. We define interoperability as the capability of two or more networks, systems, devices, applications, or components to exchange information between them and to use the information so exchanged. Future tags and interrogators/readers must integrate different communication standards and protocols that operate at different frequencies and allow different architectures, centralised or distributed, and be able to communicate with other networks unless and until global, well defined standards emerge. The interoperability issues have to be differentiated at different levels like physical, syntactical, services, devices, functions, the communication layers, radio protocols, frequencies, application and semantics and a holistic approach is required in addressing and solving the interoperability of IoT devices and services at one or several layers.

2.6 Trust and Security

There is a need to have a technically sound solution to guarantee privacy and the security of the customers in order to have a widespread adoption of any object identification system. While in many cases the security has been done as an add-on feature, it seems that the public acceptance for the IoT will happen only when strong security solutions are in place. Long term security protection is a necessity, one which takes into account the product lifecycle.

3 Applications

Under the current vision, the IoT will have an even more fundamental impact on our society than the impact of the Internet & mobile technologies or even today's acclaimed "Information Era". The future ubiquitous IoT will make it possible for virtually any object around us to exchange information and work in synergy with each other in order to dramatically increase the quality of our lives.

We will be wearing smart clothes, made of smart fabrics, which will interact with the Climate Control of our cars and homes, selecting the most suitable temperature and humidity levels for the person concerned; smart books of the future will interact with the entertainment system, such as a multi-dimensional, multi-media Hypertext bringing up on the TV screen additional information on the topic we are reading in real time; and so on.

Many application areas are foreseen for the future IoT and they range from automatic meter reading, home automation, industrial monitoring, military, automotive, aeronautics, consumers (Personal Area Networks), retail, logistics (shipping tracking storing, managing supply chain), food traceability, agriculture, environment and energy monitoring to healthcare with pharmaceutical or public and private safety and security.

Initially, RFID technology was studied in order to replace the bar code in retail. While currently tested in a variety of pilot projects, the adoption of RFID has been slowed down by several factors, such as the much higher cost of an RFID tag over bar code labels, necessary technological improvements to overcome attenuation by metals and liquid items, and privacy concerns. The electronic tags offer multiple benefits over the bar code for both retailers and consumers. The retailers will have item identification which is integrated from the producer, through to the storage, the shop floor, cashier and check out levels. RFID tags will also ensure enhanced theft protection. The shelves will be able to issue refill orders automatically, and the history of any item from production to the shelf can be stored offering increased quality management along the supply chain. For the consumers this offers the possibility to avoid long check-out queues, and having the product history available will improve food safety and protect consumer rights in case of faulty or tainted products. RFID tags will also prove a great tool to fighting counterfeit goods.

Another important application field is logistics. Today, RFID technology is mainly being used for identification purposes. In the future, using the autonomous routing of data packets in today's internet as a model, the next evolution step will be an integrated automation and individualization of material flows. For that purpose, logistics objects will be equipped with RFID tags which contain not only identification attributes but also information regarding the destination, routing, priority, and processing steps of the object. The logistics environment will be composed of standardized modules (e.g., conveyors, junctions) with an integrated intelligence based on powerful microcontrollers. This will allow for intelligent communication between logistics objects and other modules; via this set up, actions of the different modules and the logistics objects can be negotiated between themselves. A complex central material flow computer therefore becomes obsolete.

As a result, this allows for a completely decentralized material flow. Changes in topology, routing order, etc, will not require costly adaptation work – the system recognizes them on its own. This increases not only efficiency, flexibility and robustness of material flow systems but also decreases costs and energy needs through the better usage of existing capacities. In the end, logistics objects will find their way through the production site, to the customer and back to recycling facilities independently – just like the data packets in today's internet.

Advanced RFID technologies will also reshape pharmaceutical and medical applications. Electronic tags will carry information related to drug use making it easier for the customer to be acquainted with adverse effects and optimal dosage. RFID enhanced pharmaceutical packaging can carry not just all related information, but also control medical compliance. Finally, smart biodegradable dust embedded inside pills can interact with the intelligent tag on the box allowing the latter to monitor the use and abuse of medicine and inform the pharmacist when a new supply is needed. The smart dust in pills could also detect incompatible drug mixtures, and in case a dangerous mix is detected the medicament carrier could refuse to activate or release the active substances. The combination of sensors, RFID and NFC (near field communication) will allow a significantly improved measurement and monitoring methods of vital functions (blood pressure, blood glucose etc). The enormous advantages are to be seen on the one hand side in prevention and easy monitoring (and having therefore an essential impact on our social system) and on the other side in case of accidents and ad hoc diagnosis. Especially passive RFID could act as communication as well as power interface for medical implants.

Implantable wireless identifiable devices could be used to store health records that could save a patient's life in emergency situations especially for people with diabetes, cancer, coronary heart disease, stroke, chronic obstructive pulmonary disease, cognitive impairments, seizure disorders and Alzheimer's, and people with complex medical device implants, such as pacemakers, stents, joint replacements and organ transplants and have particular use in an emergency room when the patient is, unconscious and unable to communicate. Edible, biodegradable chips that can be introduced into the body and used for guided action. Paraplegic persons could have muscular stimuli delivered via an implanted radio-controlled electrical simulation system in order to restore movement functions.

In this context security, privacy and safety by design will be a first priority for the implantable wireless identifiable devices development and use.

RFID and wireless identifiable systems will benefit the aeronautics industry, helping it to optimise its existing processes, improve reliability, offer new services and realise the advantages of rationalisation.

Dynamic monitoring systems will employ RFID and wireless identifiable sensing devices to provide input during the life-cycle phases of production, operation and disposal of aircraft and components. This will require robust RFID and sensor technologies. These will need to have in-service lives of 25-30 years, and be able to operate in harsh environments (for example, with large variations in temperature, humidity, material use, and corrosion).

The wireless identifiable devices attached to the aircraft components and parts can be updated with warranty and repair information to provide a virtual pedigree on each device, and these devices can help ensure that manufacturers comply with regulatory mandates for disposal of toxic substances (products that contain lead, mercury and other hazardous substances - Restriction on Hazardous Substances - RoHS directive). This will result in the development of a complete systematic scheme to assess the environmental impact of the products throughout their entire life cycle, targeting design, procurement, manufacturing, transport, in-service operations, including maintenance, aircraft end of life and recycling (from cradle to grave).

Wireless identifiable systems will be developed using RFID tags correlated with luggage in containers, RFID tags for tracking passengers/luggage/cargo, RFID tags and sensors on conveyors.

Applications in the automotive industry include the use of RFID devices to monitor and report everything from pressure in tyres to proximity of other vehicles. RFID technology is used to streamline vehicle production, improve logistics, increase quality control and improve customer service. The devices attached to parts contain information related to the name of the manufacturer and when and where the product was made, its serial number, type, product code, and precise location in the facility at that moment. RFID technology provides real-time data in the manufacturing process and maintenance and offers a new way of managing recalls more effectively.

The use of wireless identifiable devices helps factory workers to gain insights into where everything is so that it is possible to speed assembly processes and locate cars or components in a fraction of the time. RFID technology is ideal in enabling real-time locating systems (RTLS), improving vehicle tracking and management and supporting automotive manufacturers better manage the process of testing and verifying vehicles coming off the assembly line while tracking them as they go through quality control, containment and shipping zones. The future IoT will enable car-to-car communication based on ad hoc dynamically composed local data networks. Cars will inform each other about their current position, speed, direction etc and about threats such as a wet road surface around the corner.

The idea of IoT involving the utilization of "the naturally embedded (biological) sensors of plants and animals" into Internet world is very attractive. Many animals have a "sixth sense" that can be used for life-saving services: for instance, snakes can sense earthquakes, fire and other calamities, while even plants are able to send some signals about threats, like potatoes when attacked by the "Colorado beetle". As much as it sounds science fiction, it is reasonable to think that if we can sense animals' signal we can give them the required support, and prevent natural catastrophes. A much easier application could be linked to plants, in order to give them the right amount of water, and to animals, to prevent illnesses and optimize group behaviour. Wireless sensors are already part of current home applications, in systems like air-conditioning or security. They cooperate in a strictly defined system to fulfil a precisely defined task. Normally, those systems are closed and can't exchange any kind of information.

The future IoT will increase the prevalence of the development of self-managed smart homes which will be "embedded into the Earth eco-system". We can only imagine a few of the services and application that will be enabled by the IoT: for instance, the personal RFID body temperature sensors (embedded into the fabric of our clothes) will communicate with air-conditioning system that will decide upon the most comfortable temperature and humidity considering the users general preferences, its health condition, the outside temperature and short and long term weather forecasts delivered by Internet.

4 Research Priorities

The research priorities are built on the five pillars that will form the basis for developing smart wireless identifiable systems:

- ***Multidisciplinary***: different disciplines are involved spanning from micro/nano to communication protocols and integration
- ***Convergence***: the convergence of different technologies like nano/micro, sensor, flat batteries/printed, printed antennae, silicon/polymer,
- ***Heterogeneity***: heterogeneous communication protocols, sensor technologies, and combinations of different antennae, batteries, power generation and displays.
- ***Multifunctionality***: multi functional miniaturised and smart RFID devices and readers operating at different frequencies and protocols, that have improved quality, performance and cost effectiveness, security/privacy friendliness, are world-wide compatible and transparent for the user. Flexible and adaptable RFID devices (passive/active) that incorporate sensing and actuating devices in a wide range of materials depending on the application requirements.
- ***Integration***: very high levels of miniaturization and integration, small size, low power and low cost requirements that implies high integration using a combination of system on chip (SoC) and system in package (SiP) implementation

In this context key research priorities for the next few years are presented in the following sections.

4.1 Intelligent systems

Intelligence of the systems will be central to the development of IoT and the focus will be on context-awareness and inter-machine information exchange. In the coming period, there is therefore the need to study a global architecture for the IoT, where peer-to-peer communication models, the shift of already existing bio-inspired approaches from a centralized view to a distributed one, in which intelligence is pushed towards the edge of the system, and the development of autonomous devices able to generate automatic code and behaviours, will play a central role.

The research priorities will focus on increasing and adapting the intelligence at the device level by the integration of sensors and actuators, new power efficient hardware/software security architectures, high efficiency, multi-standard and adaptive communication sub-systems, adaptable antennae (smart beam steer able phased array antennae, multi frequency band antennae, on chip antennae (OCA), coil on chip, printed antennae, embedded antennae and multiple antenna using different substrates and 3D structures).

4.2 Energy sustainability

A strong emphasis will be put on energy efficient and self-sustainable systems. Novel ways to harvest energy from the environment must be explored and developed, in order to create systems that require little external energy, if any. Efficiency in processing and in communication must also be achieved through novel programming paradigms and the further development of energy efficient protocols and smart antennae.

Research efforts will focus on multimodal identifiable sensing systems enabling complex applications such as implants monitoring vital signs inside the body and drug delivery using RFID and harvesting the energy from different sources.

Research on printed batteries manufactured with sensors, thin film solar (thermal) cells for energy harvesting, vibration and piezoceramic devices for energy harvesting, (or even micro fuel cells for long term power generation) wireless power supply to sensors and thin batteries with a life of 10 years.

4.3 Privacy and Security

Many of today's concerns about the wide adoption of the IoT lie in the popular belief that both privacy and security will be at risk. In order to reverse this belief, sound technological solutions must be developed, together with legislators at national and supra-national level. Extensive dissemination of the results of these discussions must also be undertaken by all IoT actors.

The research will focus on RFID with privacy control and energy efficient cryptography algorithms and using non-linkable digital transfers for disguising digital transactions. Combining different identification technologies to increase the security and privacy by using private, revocable ID to enable users to be the sole owners of an object's identity.

4.4 Harsh Environments and Integration into Materials

Current trends show that the research process from application specific antenna design to smart antennae, suitable in different applications and materials, will finally lead to the integration of devices into non standard substrates. These substrates, and their operational fields, might have very specific requirements, and the resilience of these smart electronic components must therefore be extremely high.

Research will focus on RFID devices with sensing capabilities that are embedded in composite parts, by using antennae, integrated electronics, micro sensors, materials and special assembly techniques for operation in harsh environments (large temperature, pressure variations, etc) or implanted, requiring biocompatible functionality.

5 Future outlook

The Internet of Things will change our society, and will bring seamless 'anytime, anywhere' business, entertainment and social networking over fast reliable and secure networks. This means the end of the divide between digital, virtual and physical worlds.

In this new context technical architecture that addresses point of control issues for tracking objects across networks, companies and business processes will become essential. Simple, distributed, architectures to enable multiple identifier authorities supporting the interests of local, regional and national business, policymakers, and individuals and addresses concerns over security and privacy will be the answer.

Today, the web services are standard and widely adopted technology for the Internet. The future Internet will bring new challenges where the wireless identifiable embedded systems at the edge of the network need to have and utilise similar functionalities.

Wireless identifiable devices and embedded distributed systems will implement service oriented architectures to solve the complexity of distributed embedded applications and propagate web services as a cross domain technology.

Wireless sensor networks and ubiquitous networks, where the sensors will be connected to and controlled by embedded systems will use this approach, where services encapsulate the functionality and provide unified access to the functionality of the system through a middleware layer.

The middleware solutions for these systems will need to provide, monitor, and manage quality of service aspects, such as response time, resource consumption, throughput, availability, reliability and security. This will determine the encapsulation of access to the system resources that will increases reliability of the overall communication network.

In the vision of Internet of Things, intelligent/smart wireless identifiable devices and embedded devices will offer their functionality as a web service, and will be able to discover and cooperate with other devices and services in a peer to peer manner.

Discovery processes distributing knowledge about the availability of services, capability descriptions and publish/subscribe mechanisms will give full control to the stakeholder for managing complex work processes.

Chapter 5 Projects in the Cluster

AmI-4-SME

Ambient Intelligence Technology for Systemic Innovation in Manufacturing SMEs

The AmI-4-SME project is addressing Ambient Intelligence (AMI) technology, oriented to surround people with electronic environments, sensitive and responsive to their desires.

The AMI-4-SME Project

It was searched for process innovation potentials for manufacturing industry based on a revolutionary next step in systemic innovation. Based on manufacturing SME business cases, the research and IT partners clearly identified, that AmI is facilitating the collaboration between humans themselves and with their ambience such as machines on the shop floor or existing IT systems (e.g. ERP, PPC, MRP). On top of that, feedback from prototype testing in the SME environments indicated SMEs' urgent need for highly tailored turn-key solutions, when aiming at the exploitation of AmI enabled innovation potentials, required to guarantee the realisation of business benefits and competitive advantage.

Project Results

For effectively serving SME needs concerning turn-key solutions in a suitable price range as well as to empower suppliers of AmI based solutions to serve those needs, the AMI-4-SME project elaborated three Building Blocks for realising innovative AmI as well as human centred solutions:

- RFID based sensor system, mobile readers & middleware, highly compatible for integration with SME infrastructures.
- Speech recognition system, for implementing configurable natural human interaction on mobile devices; easy to generate & maintain; using standard interfaces.
- AmI system adaptor for mobile device, service & system integration. Enabling a flexible, secure & efficient configuration, mapping & interfacing of legacy systems, AmI services as well as mobile devices.

Moreover, the AMI-4-SME Software Platform was realised to easily set-up the required runtime environment as well as software infrastructure to provide a cost and time efficient realisation of a human centric turn-key solution.

To guide the innovation approach of both the manufacturing SME and the IT provider, the AMI-4-SME Methodology was developed. It provides clear instructions, guidelines and templates for realising the successful utilisation of new AmI technologies. It is based on a traceable improvement process, driven by the company staff, enabling informed decisions of the management.

AmI-4-SME was completed in September 2008. The consortium is continuing its work in their fields of expertise and is providing the following consultancy and products: AmI turn-key solutions, AmI software services & hardware easy to be integrated in SMEs infrastructures as well as Consultancy, based on the AMI-4-SME Methodology.

Further information:

Partners: ATB, Brüggen, CARSA, DERi, EuroCoach, OAS, PRO DV, Sidheán, Softrónica, Telefónica, TNS, TRIMEK

Contact: Harald Sundmaeker;
ATB Institute for Applied Systems Technology Bremen GmbH
Wiener Str. 1; D-28359 Bremen
Germany
Tel.: +49-421-220920
E-mail: Sundmaeker@atb-bremen.de
Internet: www.ami4sme.org
Duration: 01.10.05 – 30.09.08 - 36 Months

ASPIRE

Advanced Sensors and lightweight Programmable middleware for Innovative RFID Enterprise applications

The ASPIRE project is addressing RFID deployment paradigm, by introducing and boosting a shift towards lightweight, royalty-free programmable, privacy friendly, standards-compliant, scalable, integrated and intelligent RFID middleware. The ASPIRE middleware is being placed at heart of RFID infrastructures. This will be freely offered to end-users (particularly SMEs).

The ASPIRE Project

ASPIRE is developing an innovative royalty free middleware platform. This middleware platform is a primary target of the open source "AspireRFID", which has been established in the scope of the OW2 community. The open nature of the "AspireRFID", requires versatility of the hardware and tools that will support the RFID solutions being built based on the ASPIRE middleware platform. The ASPIRE middleware is vendor- and frequency independent. The ASPIRE middleware can also support different tag formats. Also, it is able to be programmed and configured so as to "bring it closer" to RFID systems "illiterate".

This freedom of choice is perfectly in line with both the "open" nature of the middleware and the requirements of Small Medium Enterprise (SMEs). Avoiding vendor and technology lock-in and the reconfiguration ability is a major requirement from the SME community with respect to RFID solutions.

Project Results

For effectively serving SME needs concerning turn-key solutions in a suitable price range as well as to empower suppliers of RFID-based solutions to serve those needs, the ASPIRE project elaborated three parts for realising innovative SME oriented solution:

- ASPIRE Middleware Architecture and solution (http://forge.ow2.org/project/show files.php?group_id=324): ASPIRE introduces a new approach to RFID middleware through a two-tier filtering:
  - Conventional filtering (e.g., EPC-ALE paradigm): Open Source Tools (Stored/Save, Edit, Delete Filters) compliant to ALE specifications
  - Filtering of business events (i.e. based on the paradigm of BEG module):
    - Combination of filtered data with business metadata according to declared/configured processes
    - Specifications for mapping sensor reading events into business events
  - Filtering of many types of sensors other than RFID, like ZigBee (IEEE 802.15) and HF sensors.
- ASPIRE Low-cost hardware and Tools
- ASPIRE Trails: The trails are being performed in the areas of Logistics, Textiles-Apparel, Cold Chain Management, Process Management and Retail to lower SME entry cost barrier and Total Cost of Ownership (TCO) for RFID technology solutions Provide efficient inventory and smart services.

Moreover, the ASPIRE Middleware Platform will be user-friendly especially focusing on SME demands. To guide the innovation approach of both the manufacturing SME and the IT provider, the ASPIRE Methodology was developed. It provides clear instructions, guidelines and templates for realising the successful utilisation of RFID technologies and ASPIRE Middleware.

Further information:

Partners: AAU, AIT, INRIA, UJF, Melexsis, OSI, UEAPME, SENSAP, PV and IT.

Contact: Prof. Neeli R. Prasad;
Center for Teleinfrastruktur (CTIF)
Aalborg University
Niels Jernes Vej 12;
DK-9220 Aalborg
Denmark

Tel.: +45-994-09835
E-mail: np@es.aau.dk
Internet: www.fp7-aspire.eu

Duration: 01.01.08 – 31.12.10 - 36 Months

BRIDGE

Building Radio Frequency Identification Solutions for the Global Environment

BRIDGE (Building Radio frequency IDentification solutions for the Global Environment) is a European Union funded 3-year Integrated Project addressing ways to resolve the barriers to the implementation of RFID in Europe, based upon GS1 EPCglobal standards. The project consisted of a series of business, nical development and horizontal tivities. It started in July 2006 and ended in August 2009.

Project Objectives

The implementation of RFID and EPCglobal standard solutions is hindered by a number of technical, social and educational challenges. The objective of the BRIDGE project was to research, develop and implement tools to enable the deployment of EPCglobal applications in Europe.

Project Activities

The project included an important research and development programme in various aspects of RFID hardware, software, network and security.

Seven Business work packages were set up to identify the opportunities, establish the business cases and perform trials and implementations in various sectors including anti-counterfeiting, pharmaceuticals, textile, manufacturing, re-usable assets, products in service and retail non-food items.

A series of horizontal activities provided training and dissemination services, enabling the adoption of the technology on a large scale in Europe for the sectors addressed by BRIDGE and beyond. BRIDGE involved 31 partners and was coordinated by GS1.

Project Achievements

The project delivered truly innovative hardware and software products. It also issued several important contributions to standard bodies in the areas of sensors, security and Discovery services. The lessons learned from the multiple pilot implementations will be inspiring for many companies in various sectors. Finally, a considerable set of education material has been made publicly available.

This project has been a great opportunity for Europe to build on a standardised RFID technology for use in global supply chains. The BRIDGE project has clearly contributed to the development of new solutions for all businesses, from small to large. Improving skills and expertise on RFID technology and network information sharing is leading to enhanced competitiveness of European companies and to benefits to customers and citizens.

Further information:

Partners: GS1 organisations: Global Office (Coordinator), France, UK, Germany, Spain, Poland, China;

Universities: Cambridge, ETH Zurich, Fudan, UPC Barcelona, TUG Graz; Users: Carrefour, Bénédicta, Kaufhof, Gardeur, Nestlé UK, Sony, El Corte Inglés, Northland, COVAP;

Solution Providers: BT, SAP, AIDA, Caen, Confidex, AT4wireless, UPM Raflatac, Verisign UK, Melior, Domino, JJ Associates.

Contact: GS1
Avenue Louise 326 – Bte10
B-1050 Brussels ; Belgium
Tel.: +32-278-87800
E-mail: info@bridge-project.eu
Internet: www.bridge-project.eu

Duration: 01.07.2006–31.08.2009 - 38 Months

CASAGRAS

Coordination and Support Action (CSA) for Global RFID-related Activities and Standardisation

CASAGRAS aim to provide an incisive framework of foundation studies that can assist the European Commission and EU member states in influencing and accommodating international issues and developments concerning radio frequency identification (RFID) and the emerging "Internet of Things".

The CASAGRAS Project

CASAGRAS Work Packages:

1. Standards and Procedures for International Standardisation in relation to RFID, including applications and conformance standards.
2. Regulatory issues in respect of RFID standards
3. Global coding systems in relation to RFID standards
4. RFID in relation to Ubiquitous Computing and Networks
5. Functional, including sensory, developments in RFID and Associated Standards
6. Areas of Application, existing and future, and associated Standards.
7. Socio-economic components of RFID usage

Project objectives

To Provide:

- A Platform for international collaboration on all aspects of standards and regulations relating to RFID
- A framework and supporting documentation for incisive and analytical review of international RFID standards
- Recommendations with respect to international standardisation and regulatory developments for RFID
- Recommendations with respect to applications methodologies and positioning
- Recommendations for future research and development and international collaboration
- Recommendations to encourage participation of SMEs
- An ongoing collaborative research platform for RFID

Field of Application

The framework studies will draw particular attention to Objective ICT-2007-1.3: ICT in support of the networked enterprise and the call within that objective for a Support Action (SA) for global RFID-related standardisation activities involving in particular organisations from China, Japan, Korea and the USA.

Further information:

Partners: AIM UK Ltd; YRP Ubiquitous Networking Laboratory; Hong Kong Science Parks Corporation; AIDC UK Ltd; Electronics and Telecommunication Research Institute; FEIG Electronic; ETSI; QED Systems

Contact: Ian Smith; AIM UK Ltd

The Elsie Whiteley Innovation Centre

Hopwood Lane, Halifax, West Yorkshire, HX1 5ER, UK

Tel.: +44 1422 399 499

E-mail: ian@aimuk.org

Internet: www.rfidglobal.eu

Duration: 01.01.08 – 30.06.09 - 18 Months

CASCADAS

Component-ware for Automatic Aware Situations Communications for a Dynamic and Adaptable Service

Today's Internet is rapidly evolving towards a highly distributed and communication-intensive collection of services. In the future, these services would be expected to detect automatically data and to self-configure, in order to meet the needs of various Users, in diverse situations, without requiring explicit human intervention.

To achieve this, a re-thinking is needed of the current way of developing and deploying distributed systems and applications. One approach consists in developing an "open ecosystem", which can prosper and thrive. This vision is attractive: it provides new and better services to Users.

CASCADAS goal is to provide an automatic component-based framework that can support the deployment of a novel set of services, via distributed applications, which can cope with dynamic and uncertain environments, i.e. having Self-Configuration, Self-Healing; Self-Optimization; Self-Protection (self-CHOP) capabilities.

Technical and innovation approach

CASCADAS is a robust modular framework and acts as a high-level reference model for a new generation of programmable elements, which can be reused at different stack levels. Such a model, is the core of the fundamental software Autonomic Communication Elements (ACE).

Target users and benefits

CASCADAS proposes a do-it-yourself innovative services and knowledge management, which will allow real People to be the target Users. CASCADAS has identified the following main areas of benefits and industrial exploitation of results:

- Introduction of innovative SAC "services" (and new business models)
- Future Internet development;
- Optimization of Telco-ICT Service Frameworks (Capex savings);
- Simplification of Management (Opex savings) of above Frameworks.

CASCADAS framework, called the Toolkit, provides a running-time environment capable of supporting ACEs in all their features.

CASCADAS Toolkit

ACE Toolkit is available for download at: http://sourceforge.net/projects/acetoolkit/

Project deliverables are available at: http://www.cascadas-project.org

Toolkit has been successfully used to build a prototype system to suit a potentially industrial future scenario, called Behavioural Pervasive Advertisement, which takes a crowded venue, with many public screens. The advertising screens display information independent of the context. Smart services could then gather publicly information on Users and advertise their particular interests. This would transform the effectiveness of advertising service! Hence, the level of business investments would be higher, in buying and allocating advertising time slots, by "auctioning" these advertising time slots. CASCADAS has an auction paradigm whereby advertisers can acquire the rights of advertising, on a specific screen, at a specific time.

Further information:

Partners: Telecom Italia, BT, Budapest University, Fraunhofer, Imperial College London, Eurecom, Politecnico di Milano, Uni Kassel, Uni di Modena e Reggio Emilia, Uni Trento, Uni Ulster, MIP School of Management, Uni Athens, Uni Libre de Bruxelles

Contact: Antonio Manzalini; Telecom Italia
Via Reiss Romoli 274;
IT-10148 Torino; Italy

Tel.: +39-011-2285817

E-mail: Antonio.manzalini@telecomitalia.it

Internet: www.cascadas-project.org

Duration: 01.01.06 – 31.12.08 - 36 Months

CE RFID

Coordinating European Efforts for Promoting the European RFID Value Chain

Within the Coordination Action "CE RFID" European stakeholders discussed and lysed all major issues concerning RFID: technology, R&D, standards, guidelines and regulation.

The CE RFID Project

From 2006 to 2008 European RFID users and vendors cooperated within the initiative CE RFID ("Coordinating European Efforts for Promoting the European RFID Value Chain") in order to improve the market conditions and development of RFID technology in Europe and to reinforce the political environment of RFID at European level.

Project Results

The activities of CE RFID centred around five main topics:

- RFID application and technology roadmap,
- European RFID research & development policy,
- RFID standards and radio regulations,
- RFID application and implementation guidelines, and
- Regulatory framework for RFID.

For each topic an in-depth analysis of the state-of-the-art was conducted and detailed recommendations for European RFID stakeholders and decision makers from policy, economy, and society were provided.

About 200European experts from different stakeholder groups contributed to the work of CE RFID by participating in workshops or by reviewing reports, thus ensuring that the detailed recommendations for a supportive European policy on RFID are based on a broad societal basis.

The main recommendations of CE RFID were:

- There should be an active sponsorship and funding for RFID-specific cooperative research which covers all activities from applied research to those close to market innovation.
- Generic, interoperable and easily applicable standards are needed and a close cooperation between the existing international standardisation organisations should be established.
- Users need application-specific guidelines to implement RFID.
- The principle of technology neutrality needs to be preserved in the regulatory approach.

A continued dialogue between all relevant stakeholders should be ensured.

Additionally, the partners elaborated the "RFID Reference Model" which clusters more than 100 examples of RFID use cases into eight RFID application fields with 41 subcategories.

All reports of CE RFID and the presentations given at the closing conference "Towards a European Policy on RFID" are published on the project website: www.rfid-in-action.eu. The partners summarised their findings also in the book:

Gerd Wolfram, Birgit Gampl, Peter Gabriel (Eds.): The RFID Roadmap: The Next Steps for Europe. Berlin/Heidelberg: Springer 2008

Further information:

Partners: MGI METRO Group Information Technology, Deutsche Post, FEIG Electronic, Siemens, NXP, VDI/VDE-IT, RF-iT, EADS, AIDA, ADT, UPM Raflatac, Pleon

Contact: Matthias Robeck
METRO AG, CIO-Office
IT Strategy and Innovation
Postbox 23 03 61;
D-40089 Duesseldorf; Germany

Tel.: +49-221-9694-224
E-mail: Matthias.robeck@metro.de
Internet: www.rfid-in-action.eu

Duration: 01.04.06 – 30.09.08 - 30 Months

CoBIs

Collaborative Business Items

The CoBIs project developed a radically new approach to business processes involving physical entities such as goods and tools in terprise environments, integrating wireless sensor networks with enterprise systems using a service-oriented architecture.

The CoBIs Project

Wireless Sensor Networks are seen as one of the most promising technologies that will bridge the physical and virtual worlds, enabling them to interact. Expectations go beyond the research visions, towards their deployment in real-world applications that would empower business processes and future business cases.

Advances in networked embedded systems were applied to embed business logic in the physical entities to create so-called Collaborative Business Items. These items enable to relate more closely the state of an enterprise as represented in a business process with what is actually happening in the real world. Thereby, business processes can be extended to the "point of action" rather than via a centralized back-end system.

Project Results

The central concept of the CoBIs project was to use a common service paradigm throughout all layers, from the enterprise application down to the logic executed on sensor nodes. Solutions especially concern, the integration of sensors and actuators with enterprise systems as well as the management, monitoring and administration of a system with highly distributed logic. The main results can be summarized as follows:

- A middleware based on a service-oriented architecture (SOA). The middleware allows the deployment of business logic in the form of services to the edge of the network. CoBIs provided the basic SOA framework as well as the tools to monitor and manage the network.
- A new service description language called CoBIL (CoBIs Language) to describe services for wireless sensor networks, their interface, their composition and dependencies as well as technical constraints regarding their deployment.
- A set of reusable collaborative services that were applied in a set of demonstrators and application trials.
- Hardware adaptation and integration of three different sensor network platforms, namely Particles, μNodes and Sindrion, through a common abstraction layer.

Application trials were conducted to show how the technology developed can be applied to a real-world setting. In the first one, a self-configuring RFID smart shelf was developed for the clothing industry, increasing stock visibility. The second one was conducted at a chemical plant of BP in the UK, showing how the technology can be applied to monitor storage regulations for hazardous chemicals and thus reinforce storage and workers' safety regulations in the domain of the oil and gas industry.

Further information:

Partners: SAP AG, Ambient Systems, BP International Ltd., Infineon Technologies Austria AG, Lancaster University, University of Karlsruhe, University of Twente

Contact: Stephan Haller;
SAP (Schweiz) AG
SAP Research

Kreuzplatz 20; CH-8008 Zurich
Switzerland

Tel.: +41-58-8717845

E-mail: Stephan.haller@sap.com

Internet: www.cobis-online.de

Duration: 1.8.2004 – 31.1.2007 - 30 Months

CONFIDENCE

Ubiquitous Care System to Support Independent Living

Confidence: Innovative care system. The main objective of this project is the development and integration of innovative technologies to build a care system for the detection of abnormal events (such as falls) or unexpected behaviours that may be related to a health problem in elderly people.

The Confidence Project

Nowadays, most of the care systems in the market are limited to detect falls. The innovation of the system developed in the Confidence project is that it will not only detect falls, but also identify short and long term unexpected behaviours that could indicate health problems.

Confidence will be a cost effective, non-intrusive and reliable system that will increase the quality of life and security of the elderly and their families and caregivers.

Features of the system

- Reliable
  – Low false alarm rates
- Non intrusive
- The system will adapt itself to the user
  – Learn the user behaviour
- Small and low cost changes in the user's home
- Easy to setup and to use
  – No limit to the user's daily activity
- Customized alarm protocol
- Portable
  – Operates both outdoors and indoors

Target Group

- Elderly over 65 years
- Cared or not by some kind of home assistance provided by Public Administration
- Mobility independent and with no particular difficulty with activities of daily living
- With fear of falls
- At risk of social exclusion

Technical Approach

The result of this multidisciplinary research will be a working prototype. The end-users will be involved in the RTD activities by co-defining the specifications, monitoring and testing the project. This early user involvement will contribute to meet the user's requirements and will increase the acceptability of the final system.

Impact

ICT in combination with other technologies can play a major role in prolonging the personal autonomy and active participation in society of elderly people. In this respect, Confidence has the potential to enhance the independence of elderly people.

Confidence's goals are twofold:

There is the social advantage of a better quality of life for elderly people who live alone and their relatives. The elderly will prolong their active participation in the society, and their relatives will be less concerned.

The economic advantage has to be taken into account. As elderly people will be able to live longer on their own, with a higher quality of life and not in care institutions, there will be a cost reduction for the welfare state.

Further information:

Partners: Fraunhofer, Jozef Stefan Institute, Ikerlan, COOSS Marche, University of Jyväskylä, Umeå Municipality, eDevice, CUP2000 S.p.A/Ltd, ZENON S.A.

Contact: Igone Vélez;
Centro de Estudios e Investigaciones Técnicas de Gipuzkoa
Pº. de Manuel Lardizabal,15, 20.018, San Sebastián (Spain)

Tel.: +34-943-212800

E-mail: coordinator@confidence-eu.org

Internet: www.confidence-eu.org

Duration: 01.02.08 – 31.01.11 - 36 Months

CuteLoop

Customer in the Loop: Using Networked Devices enabled Intelligence for Proactive Customer Integration as Drivers of Integrated Enterprises

CuteLoop has the strategic objective of exploring how Intelligent Networked Devices such as enhanced RFID-based systems and Global Navigation Satellite Systems can be used to effectively "integrate customers within an Integrated Enterprise" and with this to provide an important step towards 'real' Integrated, Real Time Enterprise.

Scope

Such real time enterprises shall be supported to realise highly flexible and dynamic business interconnections for agile coordination in business networks and supply chains, having customers as key drivers. Moreover, the project will address just-in-time interaction of actors and exchange of knowledge/experience among Large Enterprises (LEs), SMEs and customers.

Project Description

CuteLoop intends to explore how to radically improve the interaction of diverse actors in the integrated enterprise. Specifically including the customer dimension as an integral part of these complex relationships, while focusing on the usage of "Network Devices Enabled Intelligence" to realise distributed and autonomous control of business processes. CuteLoop is aiming at realisation of a holistic approach on:

- An innovative architecture by integration of event-driven and SOA based principles,
- Intelligent and agile agents combined with an event-driven architecture,
- Decentralised approach for assuring security and trust as well as supporting a customer oriented privacy of data and
- New interaction models and patterns for the real time enterprise.

Context

CuteLoop intends to address these problems in an SME driven integrated enterprise scenario, which is, due to its high complexity and requested flexibility, the most critical scenario from both technical and organisational/ business points of view. CuteLoop is focusing on SME in two sectors: construction and food industry.

Field of Application

The Field of Application ranges from logistical Tracking and Tracing, over Production Maintenance and Product Safety, to Quality and Information. Including, but not limited to, Peer-to-Peer Networking, Distributed and Asynchronous Interaction, Ad-hoc interaction of anonymous actors; decentralised coordination of activities and enabling a coordinated extension of existing networks.

CuteLoop includes two application scenarios (food and construction industry) for technological as well as organisational proof of concept for the new approach to be realised. On top of that CuteLoop will realise generic services for supporting typical, while still generic Interaction Models, being cross sectorial.

Further information:

Partners: ATB, CAPEB, ETSI, ETS, EuroPool, TraceTracker, TheOpenGroup, UniBonn, UNINOVA

Contact: Harald Sundmaeker;
ATB Institute for Applied Systems Technology Bremen GmbH
Wiener Str. 1; D-28359 Bremen
Germany

Tel.: +49-421-220920

E-mail: Sundmaeker@atb-bremen.de

Internet: www.cuteloop.eu

Duration: 01.02.08 – 31.01.11 - 36 Months

DACAR

DACAR

Data Capture and Auto Identification Reference Project

The aim of this collaborative research is to develop, implement, validate, disseminate and commercialise a novel, highly secure, "in-the-cloud" infrastructure for capture, transmission, storage and viewing of data within a health care domain.

The DACAR Project

This aim will include novel patented technology recently developed for digital forensic applications at Edinburgh Napier University. At present an in-the-cloud solution supports much greater levels of resilience, and reduces complexity, but often suffers from a lack of auditability, compliance and integrated security. This project overcomes this by using a novel domain-based approach, with role definitions within each domain, of which roles exposed across domains, and then the access to data is controlled by a strict interdomain security policy. The system will be implemented in a major London teaching hospital, which will enable the project to study novel risk assessment and management strategies to support a novel pervasive adaptation feature to enhance security.

Aims and Objectives

This project thus has the potential to provide an alternative strategy for real time data integration in health care. The objectives include:

1. Develop novel distributed and secure infrastructure based on role and interdomain security polices;
2. Smart device and system integration platform based on novel digital forensic security technology (DDNA);
3. In-the-cloud connectivity to improve resilience;
4. Integration of existing international codes and standards including HL7 and GS1 RFID standards;
5. Generic risk assessment strategy for smart device and system integration; and
6. Clinical evaluation, dissemination, and commercialisation.

Further information:

Partners: Edinburgh Napier University; Chelsea and Westminster NHS Foundation Trust; Imperial College London, Department for Acute Medicine; Kodit Database Ltd; GS1 UK Ltd; CipherLab UK Ltd

Contact: Dr. Christoph Thuemmler, Chelsea and Westminster NHS Foundation Trust London, UK

E-mail: c.thuemmler@rfidworksuk.com

Internet: www.dacar.org.uk

Duration: 1.10.2009 – 31.09.2011 - 24 Months

DiYSE

Do-it-Yourself Smart Experiences project

The DiY Smart Experiences project will enable people to direct their everyday 'smart' environment – together with the objects, devices and media involved – into a highly personalised meaningful communications and interaction experience that can span the home and urban domains. The project aims to create a sustainable marketplace for user-generated applications and components for an 'Internet-of-Things' world, in which non-technically-skilled people can participate – creating and sharing their own smart, interactive applications.

Increased mobility and the drive towards efficiency in modern life are a premise for the growth of technologies and services that enable intelligent and seamless interaction with a smarter environment. DiYSE is conceiving, designing and creating viable technologies, applications and business models based on smart objects, middleware and application-creation environments – promoting growth in an area of significant strategic importance to Europe for an increasingly connected world.

DiYSE aims to create a sustainable marketplace for user-generated applications for non-technically-skilled people. The proposed do-it-yourself (DiY) approach in which non-professional users get the tools and the support to create and share their own smart experiences is supported and motivated by visions of an open society in which citizens are empowered to form and share their own view of reality.

Modern technology has a key role to play in realising this vision of an open society. Considering the impact of web blogs, grassroots journalism and the low barrier to create personal websites on the Internet as well the effects of mobile phone communications and text messaging, it is clear that 21st century citizens are significantly more empowered to create such a new society.

Supporting a Web of Things

The ITEA 2 project will contribute substantially to the open Internet-of-Things world and the transition to Web 3.0. This is the so-called 'semantic' intelligent web, where the meaning of information and services is defined, making it possible for the web to understand and satisfy the requests of people and machines to use web content, and with this project also connected objects, in a meaningful way.

DiYSE will enable people to direct their everyday environment into a highly personalised meaningful communications and interaction experience. Driven by a user-centred design methodology and concrete proof-of-concept demonstrators, the project envisions innovating on new valuable interactive user experiences based on intelligent, privacy-respecting, self-aware services and objects, sensors, actuators and collaborative media devices.

The approach proposed in the project is supported and motivated by visions of an open society, the continuing trends towards globalisation and localisation, the anticipated long-tail marketplace for user generated Internet-of-Things applications, the rapid urbanisation of the world's population and the quantifiable emergence of new functional elements that can be part of the smart space experience.

Fostering innovation through shared knowledge

This project involves a particularly large consortium of European technology and applications developers and equipment manufacturers, each making use of their own specific expertise to deliver end-user focused solutions based on qualified business models. Representation from all stages in the value chain is encouraging the development of end-to-end solutions, whilst fostering innovation through shared knowledge and know-how.

The main objectives of DiYSE are to:

- Allow people to control their smart environment at home and in the urban area as part of an open Internet-of-Things world. DiY tools, services and application templates together with an Internet-of-Things application-creation environment will lower the barrier to application creation and distribution for non-technical people;
- Create an interoperable cross-domain substrate on which these smart experiences can flourish and co-exist;

Creating a pool of European expertise

The ITEA project will create a pool of expertise, providing unprecedented common ground for consortium partners – ranging from SMEs to multinational companies – to share knowledge and experience across Europe. The level of interoperability demanded by the concepts developed will be underpinned by a unified service infrastructure and standards.

A wide range of application domains is envisioned for the DiYSE creation methodology

- Conceive a layer on the smart elements in the environment, so that interaction with these elements can be carried out on a semantically-meaningful level, with the urban area defined as an open platform for innovations – sharing data, mutualising resources and making resources interoperable;
- Create a sustainable marketplace for these user-created applications;
- Evolve from unconnected to networked and finally ambient service blocks – both hardware and software; and
- Integrate the project results into demonstrators of the DiY toolkit and user cases.

Major visible results will include: a DiY smart application creation environment for non-professional users; demonstrators of concrete Internet-of-Things services and applications based on cross-media and multi-device user experiences; an advanced service infrastructure that offers cross-domain interoperability, service exposure awareness and concurrency, fitting the requirements set by the DiY approach selected; and physical building blocks for smart spaces interaction with the environment.

European-centred involvement at this fundamental stage of development of an open Internet-of-Things will promote adoption of shared communications principles and infrastructure to enhance the mass-market appeal of the concept and its commercial viability.

The resulting interactive environment will empower users to create, deploy and control their smart surroundings that promise to become a pervasive feature of everyday life. The consortium of European organisations developing this concept will drive the success of its component companies on an individual level, and place Europe at the forefront of this major new initiative.

Further information:

Partners: Alcatel-Lucent coordinates the DiYSE project; for a complete list of project partners please visit the project website

Contact: Marc Roelands;
Bell Labs, Alcatel-Lucent

Copernicuslaan 50, B-2018 Antwerp
Belgium

Tel.: +32-324-041-44

E-mail: Marc.roelands@alcatel-lucent.com

Internet: www.dyse.org

Duration: March 2009 – December 2011
22 Months

DYNAMITE

Dynamic Decisions in Maintenance

The project objectives of DYNAMITE (Dynamic Decisions in Maintenance) are to produce an infrastructure for global e-maintenance to allow mobile monitoring of machinery and processes. It includes hardware and software as well as mobile devices for access to and reporting from the e-maintenance infrastructure. Further tools and methods are developed for cost-effective applications of maintenance technologies for continuous enhancement of companies' profitability and competitiveness.

What is DYNAMITE?

DYNAMITE is a European joint research and development project running 2005-2009 within the European Union 6th Framework Programme.

DYNAMITE has created new technological solutions to meet the future challenges.

DYNAMITE is the project that created DynaWeb.

DYNAMITE created, developed and demonstrated in industrial use the DynaWeb platform including 28 novel hardware and software components as an advanced e-maintenance solution.

DYNAMITE includes new solutions for smart tags (RFID), MEMS maintenance sensor platform, on-line lubricant monitoring, mobile handheld maintenance computer (PDA), wireless communication, condition monitoring, diagnostics, prognostics, cost effectiveness decision support, web services - all integrated to DynaWeb utilising same basic machinery condition data.

DYNAMITE offers a vision to the future - an advanced e-maintenance solution for industry and transportation.

Project description

The maintenance of machinery is a huge cost to European industry. Studies over the last 20 years have indicated that around Europe, the direct cost of maintenance is equivalent to between 4 percent and 8 percent of the total sales turnover. The monitoring of machines and processes for predictive maintenance and control is crucial for a sustainable and competitive industry in Europe. Distributed, autonomous monitoring is fundamental to the penetration of e-maintenance to the cutting edge of a high capital and highly productive plant. DYNAMITE will create an infrastructure for mobile monitoring technology and create new devices which will make major advances in capability for decision systems incorporating sensors and algorithms. The key features include wireless telemetry, intelligent local history in smart tags, and online instrumentation.

Further information:

Partners: VTT Technical Research Centre of Finland coordinates the DYNAMITE project; for a complete list of project partners please visit the project website

Contact: Kenneth Holmberg, VTT Technical Research Centre of Finland

VTT / MK6, P.O.Box 1000, 02044 VTT, Finland

Tel.: +358-20-5442285

E-mail: kenneth.holmberg@vtt.fi

Internet: dynamite.vtt.fi

Duration: 01.09.2005 - 28.2.2009 , 42 months

EPoSS

Implementing the European Research Area for Smart Systems Integration

European industry is the world leader in microsystems and related advanced technologies. The further enhancement of product capabilities and services through evolving complexity, integration and interconnectivity will help to ensure Europe's competitiveness. The key heading for these developments is Smart Systems Integration.

Smart Systems are miniaturised devices which are able to describe and diagnose a situation. They are able to decide or help to decide in critical conditions and to identify and address each other. They also may be energy autonomous and networked.

In this light a group of major industrial companies based in Europe decided to coordinate their R&D activities and to set-up EPoSS, the European

Technology Platform on Smart Systems Integration, which was launched in July 2006.

Priorities

The research priorities of EPoSS were defined while establishing the Strategic Research Agenda. They represent the core fields of interest of the members of the technology platform:

- Miniaturized and integrated smart systems with advanced functionality and performance
- Autonomously operating, power efficient and networked smart systems
- Robust systems, compatible and adaptive to environment and lifetime requirements

Bridging the gap between research and product development EPoSS is addressing technology issues from a strict application point of view.

Objectives

EPoSS is a major, transnational, pan-European, mission-oriented initiative aiming at strengthening Europe's capacity to organise and to deliver innovation in the area of smart systems technologies and integration. EPoSS embraces all key players, public and private, in the value chain so as to

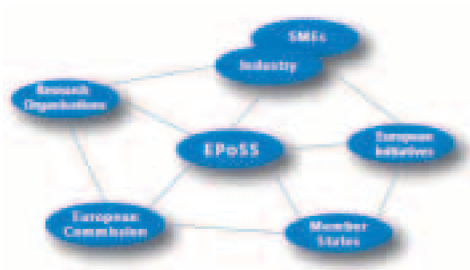
- provide a common European approach on innovative Smart Systems Integration
- formulate a commonly agreed roadmap
- and provide a continuously updated strategic R&D agenda
- define an action and implementation plan mobilising public and private human, infrastructural and financial resources
- develop options for Public Private Partnerships
- promote Smart Systems applications in sectors of high economic relevance
- strengthen global competitiveness of European industry & SMEs

The EPoSS Network

The EPoSS Networks consists of

- industry representatives including SMEs,
- public & private research organisations,
- representatives of the European Commission,

- representatives of the Member States,
- other European initiatives and key actors in the area of smart systems technologies, micro systems, and/or nanotechnologies or in a related applications area.



Organisational Structure

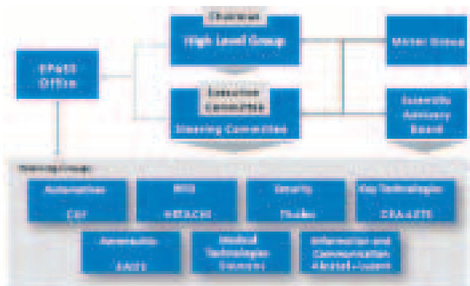
The High Level Group guides the overall strategic development of the Technology Platform and sets the frame for future priorities of EPoSS. The High Level Group is chaired by a senior industry representative.

The Steering Committee deals with cross-sectional issues related to framework conditions for research targets and directions. This group provides an operational link to the European Commission, other public authorities and to the EPoSS working groups.

The Executive Group as the central management unit of EPoSS consists of a subset of Steering Group members.

The Working Groups – structured according to application areas - are chaired by a representative from industry. The working groups involve representatives from industry, private & public research organisations, universities, public authorities and scientific, industrial and public associations.

The work of the platform is supported by the EPoSS Office.



EPoSS services offer a series of advantages

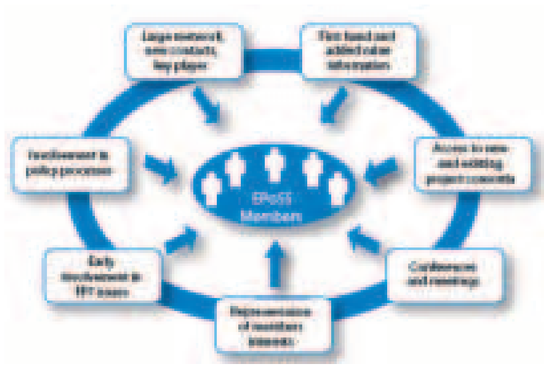
Being an EPoSS member means to improve your position in the EU policy context and to obtain an efficient forum for networking and interest representation. Furthermore, a number of services will be provided that will allow you:

- to access the internal area of the EPoSS web portal and fully participate in the EPoSS information flow
- to have unlimited access to the EPoSS working groups and to receive first hand information on newest developments and on Commission decisions
- to receive the EPoSS electronic newsletter
- to participate in EPoSS meetings such as the annual general assembly or expert workshops organised by EPoSS
- to obtain special conditions for other smart systems events connected to EPoSS.

How to benefit from EPoSS

You will become eligible for the EPoSS services by contributing to the financing of the EPoSS Office. This financial contribution per year amounts to (+VAT):

- € 4.000 for large companies
- € 2.000 for SMEs or public research organisations
- € 1.500 for universities.



Further information:

Partners: VDI/VDE Innovation + Technik GmbH coordinates the EPoSS project; for a complete list of project partners please visit the project website

Contact: Wolfgang Gessner, Sebastian Lange; VDI/VDE Innovation + Technik GmbH

Steinplatz 1, D-10623 Berlin
Germany

Tel.: +49-30-310-078 (-173) / (-299)

E-mail: contact@smart-systems-integration.org

Internet: www. smart-systems-integration.org

EURIDICE

European Inter-Disciplinary Research on Intelligent Cargo for Efficient, safe and environment-friendly logistics

Euridice is an Integrated Project funded by EU's Seventh Framework Programme ICT for Transport Area. The basic concept of Euridice is to build an information vices platform centred on the individual cargo item and on its interaction with the surrounding environment and the user.

Objectives

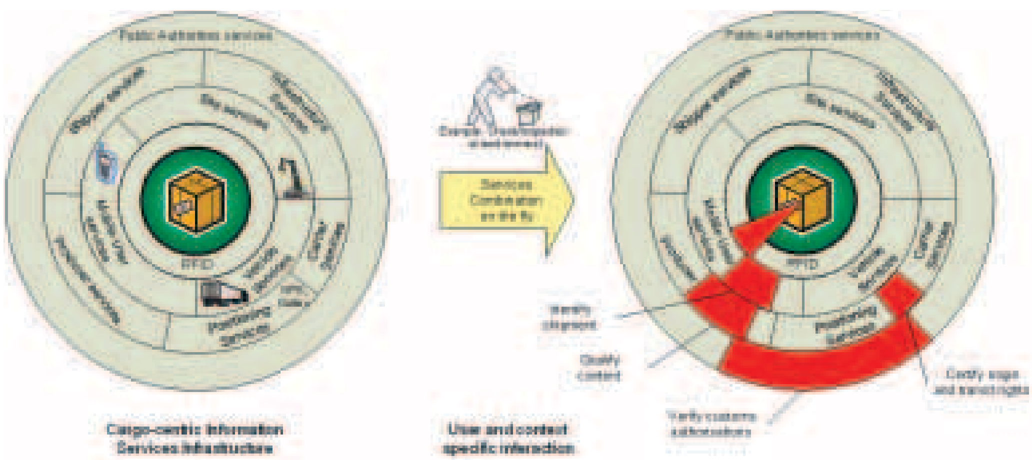
The EURIDICE project has the following main objectives:

- Supporting the interaction of individual cargo items with the surrounding environment and users on the field.
- Improving logistic performances through application of the intelligent cargo concept and technologies in the working practices of operators and industrial users.
- Developing collaborative business models to sustain, promote and develop an intelligent cargo infrastructure.
- Realizing more secure and environment friendly transport chains through the adoption of intelligent cargo to support modal shift and door-to-door intermodal services.

EURIDICE Service Platform

The Euridice Platform will allow to address simultaneously the logistics, business and public policy aspects of freight transportation, by dynamically combining services at different levels of cargo interaction:

- immediate proximity services, for direct interaction with cargo items on the field, like individual shipments or packages: RFID-based identification services, mobile user services, vehicle services, site services supporting freight interaction with fixed structures such as terminals, warehouses and intermodal facilities;
- supply chain services for interaction with the actors responsible of shipping, carrying and handling the goods, as well as producers and consignees of the goods themselves;
- freight corridor services managed by authorities and operators in charge of infrastructures efficient operation, security and safety control, such as land and port terminals, railways and motorways for resources allocation and traffic control, customs agencies and other entities in charge of safety and security checks on the goods.



Approach

The EURIDICE platform will consist of a fixed and mobile web services infrastructure supporting "on the fly" combination of services to address ad hoc user-cargo-context interactions. To this purpose the project will integrate and further develop several technological components and approaches:

- Adapting and integrating state-of-the-art identification, communication and networking technology (i.e. RFID tags readers/writers; GPRS localization systems; mobile devices; software defined radio technologies) into an Intelligent Cargo Integration Framework (ICIF).
- Realizing Cargo Intelligence applications for distributed and centralized data gathering, anomaly detection, analysis and prediction, based on approaches like semantic web and domain ontologies, advanced context technologies and distributed intelligent agents.

- Implementing interoperability standards and service oriented architectures for public and private stakeholders to access and use the services they need on a cargo item at any point along its route across European corridors, connecting the cargo with back-office users and consumers.

Activities

The EURIDICE integrated project has duration of three years and an estimated effort of approximately 1600 person months, subdivided into three main typologies of activities:

- S/T Research, pursuing the required innovations into the four main areas of cargo connectivity and communication, service oriented architectures, cargo information management and decisions support.
- Pilot applications, providing requirements and trial scenarios for test and assessment of the S/T results. Pilots will be designed and implemented taking into account of two dimensions: the supply chain/sector dimension, to assess impact from an industry viewpoint, and the stakeholder dimension, considering the different perspective of the main public and private actors involved in freight logistics.
- Impact creation, including knowledge sharing, dissemination and training activities directed to target scientific and business communities to ensure proper diffusion of the project concepts and results. To maximize impact, business modelling activities are carried out throughout the duration of the project, involving industrial partners in the Consortium as well as key players in the field participating in the EURIDICE Business Forum.

Partnership

The project is undertaken by a Consortium, coordinated by Insiel (Italy), bringing together 22 partners from 9 countries. The EURIDICE Consortium has been assembled to support a multi-disciplinary approach, involving leading industries and research organizations in complementary domains: mobile and wireless technology, RFID, application software, business consultancy and logistics. The key stakeholders are sented in the Consortium by leading trial companies from different sectors, logistic operators, public authorities and infrastructures.

Further information:

Partners: Akarport, Assindustria Belluno, Autorità Portuale Di Trieste, BIBA, CAEN RFID, CeTim, Enicma, FHV, Gebrüder Weiss, Insiel, JSI, LogicaCMG, Omega, Oracle, Proodos Kuehne Nagel, SDAG, Searail, Singular Logic, Telit, TREDIT, VIU, VTT

Contact: Paolo Paganelli;
Organisation: Insiel
Via Cesare Battisti 27;
IT-40123 Bologna; Italy

Tel.: +39-040-3737-001
E-mail: Paolo.paganelli@insiel.it
Internet: www.euridice-project.eu
Duration: 01.02.2008 – 01.02.2011 - 36 Months

GRIFS

GRIFS

Global RFID Interoperability Forum for Standards

The Global RFID Interoperability Forum for Standards (GRIFS) is a Support Action Project funded by the European Commission's FP7 Programme with the aim to improve collaboration and thereby to maximise the global interoperability of RFID standards. This two year project started in January 2008 and is run by GS1 (project coordinator), CEN and ETSI.

Project objectives

A world of global supply chains requires that RFID tags and associated sensors can operate, can be seen and can be interrogated anywhere. For maximum competitiveness and greatest efficiency this requires standards that are global in definition and in application.

The GRIFS project aims at initiating a forum that will continue to work constructively and grow after the end of the project through a Memorandum of Understanding between key global standard organisations active in RFID. This Forum should improve the collaboration between standards organisations and increase interoperability of standards.

Project activities

GRIFS is undertaking the following work to achieve its objective:

- Analyse the national, regional and global RFID standardisation activities. The team has built up an online database listing more than 160 RFID standards.
- Several workshops and other actions have been organised at regional level to raise awareness and to identify areas where standard development coordination might be required. Those workshops have helped to prepare the creation of the GRIFS forum.
- A GRIFS forum has been launched and four forum meetings are being organised in the regions of Asia, America and Europe. The final forum meeting in Europe will aim to cement the Memorandum of Understanding and ensure that the GRIFS forum will be viable and will be able to continue to operate beyond the end of this support action.

This support action is focusing on the use of RFID in supply chain and related activities. These activities primarily encompass the tracking and tracing of physical items as they move through supply chains in many different businesses, both in the public and private sector.

The forum will continue to enable exchanges of views on all aspects of RFID interoperability from the perspective of standardisation, thus facilitating a coherent and consistent global RFID standardisation policy.

Further information:

Partners: GS1, CEN, ETSI

Contact: GS1
Avenue Louise 326 – Bte 10;
B-1050 Brussels ;
Belgium

Tel.: +32-278-87800

E-mail: info@grifs-project.eu

Internet: www.grifs-project.eu

Duration: 01.01.2008 – 31.12.2009 - 24 Months

Hydra

Networked Embedded System Middleware for Heterogeneous Physical Devices in a Distributed Architecture

The first objective of the Hydra project is to develop middleware based on a Service-oriented chitecture, to which the underlying communication layer is transparent. The middleware will include support for distributed as well as centralised architectures, security and trust, flective properties and model-driven development of applications.

The HYDRA middleware will be deployable on both new and existing networks of distributed wireless and wired devices, which operate with limited resources in terms of computing power, energy and memory usage. It will allow for secure, trustworthy, and fault tolerant applications. The embedded and mobile Service-oriented Architecture will provide interoperable access to data, information and knowledge across heterogeneous platforms supporting true ambient intelligence for ubiquitous networked devices.

The second objective of the Hydra project will produce two tools that will simplify the development process based on the Hydra middleware, a software- and a device development kit (SDK/DDK) to be used by developers.

Project description

Embedded Systems denotes invisible modular systems that are combined to form complex higher-order systems and are used, e.g., in motor vehicles, airplanes, "intelligent" buildings or home multimedia systems. Advanced applications in these fields require to network growing numbers of devices, typically from more than just a few manufacturers.

Given the plethora of heterogeneous devices, sensors and actuators in the field, the large number of manufacturers and the differences in their speed of innovation, there is an urgent need for technologies and tools that make it easier to reap the benefits of networked systems. And the complexity to build such technologies and tools grows exponentially with the number of devices, manufacturers and protocols involved.

For this situation Hydra develops a middleware that will help manufacturers and systems integrators to build devices that can be networked easily and flexibly to create cost-effective high performance solutions. The results will reduce design complexity by providing well-defined open interfaces between types of devices.

The Hydra middleware will have a transparent communication layer, equally supporting centralized and distributed architectures. The Hydra middleware takes security and trust into account and will allow building model-guided web services. It will run on wired or wireless networks of distributed devices with limited resources. The embedded and mobile service-oriented architecture will provide fully compatible data access across heterogeneous platforms, allowing to create true ambient intelligence for ubiquitous networked devices.

Further information:

Partners: Aarhus Universitet, CNET SVENSKA, Fraunhofer SIT, In-JET, Innova, Siemens, T-Connect, Technicka Univerzita Kosiciach, Telefonica I&D, University of Paderborn, University of Reading

Contact: Dr. Markus Eisenhauer; Fraunhofer FIT
Schloss Birlinghoven;
D-53754 Sankt Augustin
Germany

Tel.: +49-224-1142 859

E-mail: Markus.eisenhauer@fit.fraunhofer.de

Internet: www.hydramiddleware.eu

Duration: 01.06.2006 – 31.10.2010 - 52 Months

IFM Project

Interoperable Fare Management Project

The project is expected to significantly lower the barriers to mobility and encourage the use of public rather than private transport, contributing to a reduction of carbon emissions and a reduction or elimination of paper tickets, thus further enhancing the impact of smart media on environment and on the efficiency of public transport. It will be possible to tailor the media to assist specific groups (e.g. existing concessionary travellers, benefit recipients or part-time workers) thereby supporting the EU's Social Inclusion Agenda.

The IFM Project

The project is based on delivering an ICT environment that supports nomadic passengers. It will be delivered through work packages covering trust modelling, privacy modelling, common applications and interoperable media, model of IFM organisations and supporting back office ICT system interfaces. It will be managed to ensure effective and efficient consensus and dissemination of best practice among all stakeholders.
The project is designed to provide world leadership in its segment and to deliver results which can be transferred to areas outside of the transportation sector world-wide. It will allow manufacturers and suppliers to offer the end-to-end, lossless nature of the IFM platform and transactions in other fields, thereby reducing time to market and lowering the cost of implementing other comparable schemes.

General Objectives

The key stakeholders of the IFM Forum perceive the IFM Project as a well-suited framework to coordinate their experience and share it with a wider community of beneficiaries in Europe through the IFM Forum organised by the UITP.

The objective is to avoid the establishment of enduring isolated national solutions and to define route-maps leading the way toward pan-European interoperability.

The IFM Project aims to be a European wide initiative dedicated to the establishment of attractive access to public transportation with modern fare management which is safe, reliable and convenient for both users and operators. Once achieved, this may serve as a model for many further countries outside Europe faced with the need to strengthen the use of public transport.

The "IFM Project" will be the first step of the IFM initiative. The ultimate goal of the IFM Project at the end of the two-years is a European-wide agreed concept (Route Map) developing shared back-office rules for cross-border data exchange and the associated European Secure Access Module (EU-SAM). It will create a documented framework by 2010 to deliver the requirements for secure, fully-interoperable portable object for seamless mobility on public transport accessible to all European Citizens. In a second step comprising Research and Technological Development (RTD) and field operational tests, a European interoperable fare management standard will be developed and implemented by 2010.

Following the definition and information sharing phase, existing and new schemes will be able to plan convergence strategies based on experience and utilising known technologies to enable a common Interoperable Fare Management area.

The beneficiaries will be:

- Transport Customers ("users") that will be able to use their local IFM transport cards outside their home networks as well as to use a multi-application contact-less wallet of their choice to upload the transport applications they need and carry the virtual transport tickets attached to each of them.
- Transport Authorities that will be able to build new fare and distribution agreements with the support of standardised specifications.

This will produce new inputs to set objectives to complement the existing set of standards. The EU – through CEN – has been very active in developing specific standards for the data elements necessary to support electronic ticketing. Recently approved, ISO EN 24014-1 was initiated by European proposals and complements the data elements described in EN 1545.

Pilot EU-led projects such as CALYPSO and TRIANGLE have made some progress in implementing and demonstrating the concept of interoperability.

The stakeholders wish to maintain this dynamic attitude of Europe for this subject.

Overall Strategy and general description

This project is directed at making the mobility of people more efficient and environmentally sustainable by facilitating informed modal switching and the seamless accessibility of public transport. It aims at innovative, safe and reliable ticketing and fare management across Europe using interoperable smart media with the specific aim of encouraging increased usage of public transport.

The work plan and its work packages are designed to facilitate the following operational impacts:

- Greater awareness of the benefits of applying smartcard enabled ICT Solutions to Implement harmonized Interoperable Fare Management for scheme for operators, customers and government across Europe.
- The dissemination of knowledge of how to set up an Interoperable Fare Management scheme, the ICT systems, the players, their roles, and how to achieve the maximum benefits.
- The spreading of excellence through the description of best practice in meeting European standards.
- The respect of privacy through the adoption of a common privacy model compatible with the business needs.
- The enhancement of security and minimisation of fraud by the adoption of a shared trust model.

Further information:

Partners: ITSO Limited coordinates the IFM project; for a complete list of project partners please visit the project website

Contact: John Verity, Head of Compliance and Security, ITSO Limited

Quayside Tower, 252-260 Broad Street
Birmingham B1 2HF

E-mail: compliance@itso.org.uk

Internet: www.ifm-project.eu

Duration: 24 months

Indisputable Key

Intelligent Distributed Process Utilization and Blazing Environmental Key

The Indisputable Key project is developing new methods and ICT solutions to improve the use of wood and optimise forest production by utilising traceability of logs and boards through the forest-wood supply chain.

The Indisputable Key Project

Large volumes of wood are going to waste. Knowledge of log characteristics and their impact on the quality and final end-use of wood products can help in the selection of the most suitable log for a specific product while still in the forest and thus significantly reduce the amount of wood wasted. New methods and technology for traceability are needed to make it possible to mark individual logs and boards, and to trace these through the forest-wood supply chain.

Project Results

The project covers different areas such as data exchange, models and indicators of economic and environmental performance, RFID technology and other technologies for marking and reading, and software modules for integration. The industrial implementation is supported by exploitation planning, industrial demonstrations and training.

Major achievements of the project include new RFID technology for log marking; ink-based board marking and reading; an infrastructure for data exchange based upon existing standards such as papiNet, Stanford and EPCglobal; software for tracing objects and for monitoring economic and environmental key performance indicators; models for predicting wood properties and models for the simulation of supply chain scenarios.

Main novel developments include:

- Pulping compatible passive EPC C1G2 compatible UHF RFID transponders for marking logs.
- Robust RFID reader with an adaptive RF front end for use in the forest in the harvesters.
- Special Key Performance Indicators for easy access to the environmental performance of a product.
- Software for monitoring environmental and economical performance of a product on item level.

The expected benefits of the project include better yield; reduced emissions; better tools for the tracing of timber origin and the prevention of illegal logging and better tools for product and process development. The functionality and benefits will be demonstrated at locations in France and Sweden. The main demonstration is in Sweden and will involve Sveaskog, Setra Group (Malå) and Norsjö Trä (component manufacturing).

Further information:

Partners: SP, KTH, FCBA, CIRIS, IVL, VTT, Tieto, Confidex, Idesco, Tampere Univ. of Tech., Lappeenranta Univ. of Tech.,Tallinn Univ. of Tech., Oskando, Hekotek, Skog-Data, NFLI, NTI, Skogforsk, Sveaskog, Ducerf , Raunio, ESAS, Scanpole, Mauchamp, Setra, Rolpin, Rottne

Contact: Kaj Nummila;
VTT / Wireless Sensing
P.O.Box 1000; FI-02044 VTT
Finland

Tel.: +358-20-722-5773

E-mail: Kaj.nummila@vtt.fi

Internet: www.indisputablekey.com

Duration: 01.10.06 – 31.03.10 - 42 Months

IMS 2020

Supporting Global Research for 2020 Manufacturing Vision

IMS2020 strives for strengthening international co-operation under the IMS Initiative, providing effective interface ongoing European roadmapping activities and creating research synergies through the establishment of international manufacturing communities in the five Key Areas.

The IMS 2020 Project

IMS2020 is a project conducted by an international consortium of 15 core partners and a large group of supportive members from Europe, Japan, Korea, Switzerland and the USA. The project focuses on the creation of roadmaps towards Intelligent Manufacturing Systems (IMS) in the year 2020. The roadmaps highlight the main milestones of innovation activities (research and development, management and policy actions) needed to achieve the desired vision.

IMS2020 identifies relevant research topics and supporting actions to shape the future of intelligent manufacturing through international cooperation. IMS2020 is a coordination and support action for strengthening international and interregional cooperation in Intelligent Manufacturing Systems under the IMS initiative.

Scientific and technical Objectives

In particular, the project has five main scientific and technical objectives:

Objective 1: Prepare a roadmap for future manufacturing research in the five IMS Key Areas.

Objective 2: Identify new schemes & frameworks to support MS research.

Objective 3: Stimulate small and medium enterprise's participation in international cooperative research and development projects.

Objective 4: Establish international and interregional com-munities in the five IMS Key Areas.

Objective 5: Prepare the ground for new IMS proposals and manufacturing projects.

IMS2020 wants to attract interested people and organisations to have the worldwide most qualified actors in the five IMS Key Areas to discover common innovations and potential in manufacturing.

These Five Key Areas are:

- Sustainable Manufacturing
- Energy Efficient Manufacturing
- Key Technologies
- Standards
- Education

Vision

With the support of a wide Roadmapping Support Group, made of experts, coming from enterprises, research centers and universities worldwide, the project will discover new destinations for developing Intelligent Manufacturing Systems in the forth-coming decade.

Further information:

Core Partners: Politecnico Di Milano, Institute for Operations Management, Eigengenössische Technische Hochschule Zürich, Europeen Committee for Standardization, COMAU, Clemson University, Ecole Polytechnique Fédérale de Lausanne, Fatronik, Institute for Prospective Technological Studies, Keio University, KAIST, Instituto di Tecnoloie, Holcim, Norwegian University of Science and Technology, Rockwell Collins

Contact: Prof. Marco Taisch; Professor of Operations and Supply Chain Management

Tel.: +39 (02) 2399-4815

E-mail: marco.taisch@polimi.it

Internet: www.ims2020.net

iSURF

An Interoperability Framework for Collaborative Planning

iSURF Project develops knowledge-oriented inter-enterprise collaboration tools for European SMEs to enable them to be more agile, self-sustainable and responsive to the changes in the supply chain. An open smart product infrastructure is developed to collect supply chain visibility information and an interoperability service utility is provided for seamless exchange of planning documents.

The Need for Open Collaboration Framework for SMEs

Trading partners in supply chain have different competencies based on their business strategies and varying sources of information. Competitiveness of European Companies is reduced when decision making is inconsistent due to incomplete understanding of the impact of decision on the supply chain as a whole. The distributed intelligence of multiple trading partners needs to be collaboratively exploited in the planning and fulfilment of customer demand in the supply chain in order to achieve "network is the business" vision.

As a response to this need, iSURF project is providing a knowledge-oriented inter-enterprise collaboration environment for SMEs.

Project Results

iSURF project provides a Service Oriented Collaborative Supply Chain Planning Process Definition and Execution Platform based on CPFR® guidelines. This tool enables the Collaborative Supply Chain Planning Processes to be graphically customized to the needs of supply chain partners, and provides wizards to deploy the planning process to the premises of the supply chain partners as executable business processes.

iSURF project provides a Semantic Interoperability Service Utility for achieving the semantic reconciliation of the planning and forecasting business documents exchanged between the companies conforming to different standards based on UN/CEFACT Core Component Technical Specification (http://www.oasis-open.org/committees/tc_home. php?wg_abbrev=set).

In addition to this we have developed a tool, called eDoCreator which helps to design electronic business documents by using the core components in the UN/CEFACT Core Component Library (CCL) by constraining them to the defined context.

iSURF project provides an open source smart product infrastructure based on RFID technology using EPCglobal standards. Through this infrastructure, necessary tools and processes are provided to collect real-time product visibility events from massively distributed RFID devices; filter, correlate and aggregate them in order to put them into business context. On top of this, iSURF provides easy to use interfaces to use GDSN Data Pools.

The iSURF architecture will be deployed in the premises Fratelli Piacenza S.p.A., a manufacturer of noble fibres fabrics and pure cashmere clothing and accessories.

iSURF Results are available from: http://isurf.svn.sourceforge.net/viewvc/isurf/trunk/ and http://www.isurfProject.eu

Further information:

Partners: METU, SRDC Ltd. , INTEL, Fraunhofer -IPA, TXT E-Solutions, UNINOVA, Fratelli PIACENZA

Contact: Prof. Dr. Asuman Dogac;
Computer Engineering Department,
Middle East Technical University
Campus; TR-06531 Ankara
Turkey

Tel.: +90-312-2101 393

E-mail: Asuman@srdc.metu.edu.tr

Internet: www.isurfProject.eu

Duration: 01.02.08 – 31.07.10 - 30 Months

LEAPFROG

Leadership for European Apparel Production From Research along Original Guidelines

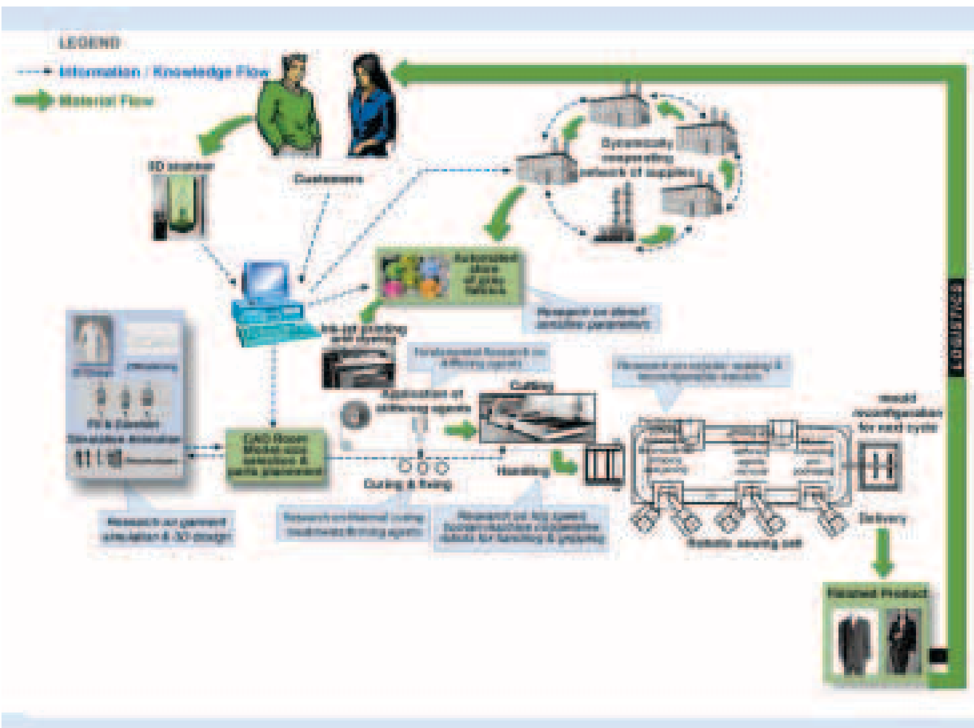
Leapfrog is a joint research and innovation initiative of the European textile and clothing industry, led by Euratex, aiming at a technology breakthrough in the clothing industry. It brings together a critical mass of European textile and clothing companies and research centres which will attempt to develop and implement new ways of optimal fabric preparation for clothing production, automated garment manufacture, virtual garment prototyping, supply chain integration and mass customisation. The ultimate goal of LEAPFROG is to achieve a step change in productivity and competitiveness of Europe's clothing sector and to decrease its dependence on the labour cost factor.

The LEAPFROG Project

The LEAPFROG Integrated Project attempts to modernise and ultimately transform the clothing sector into a demand-driven, knowledge-based, high-tech industry by exploitation of recent advances in a broad area of scientific-technological fields ranging from

- nanotechnology and polymeric material science,
- robotics and innovative joining techniques,
- 3D computer graphics and animation, to
- e-business and management research.

If LEAPFROG research and development work reaches its objectives there will be enormous innovation and new business potential across the entire spectrum of textile, clothing, machinery and service companies in Europe.



The objectives

In order to achieve the long-term industrial transformation of the Clothing Industry the LEAPFROG initiative will focus on 3 major objectives:

- A step-change in productivity, quality and cost efficiency in the garment manufacturing process.
- A radical move towards rapid customised manufacturing in one of the most demand-volatile sectors through flexibilisation and integration of cost-effective and sustainable processes from fabric processing through to customer delivery.
- A paradigm change in customer service and customer relationship management with a focus on value-adding product-services.

Results

The LEAPFROG Integrated Project was undertaken to develop concepts and technologies which would radically modernize and ultimately transform the clothing sector into a demand-driven, knowledge-based, high-tech industry.

The LEAPFROG research and development work has reached a number of its objectives to develop radically innovative technological and organisational solutions for the (textile &) clothing business of the 21st Century.
More details and extended information on the major results achieved in the project's four Research Areas, can be found on the website.
The effort undertaken through the project has reached the potential to lead to an innovation and new business development cycle involving a great number of textile, clothing, machinery and service companies in Europe over the coming years.
Several results will be available for commercial exploitation shortly after the project conclusion; others require additional research to realize their full innovation potential and to bring them as proven technology into industrial application.

Further information:

Partners: EURATEX coordinates the LEAPFROG project; for a complete list of project partners please visit the project website

Contact: Lutz Walter; EURATEX

Tel.: +32-2-2854885

E-mail: Lutz.walter@euratex.org

Internet: www.leapfrog-eu.org/LeapfrogIP/

PEARS Feasibility

Privacy-Ensuring Affordable RFID System / Feasibility

Feasibility study for an improved RFID system based on Silent Tags; providing increased vacy, security, affordability, reliability and performance.

PEARS Feasibility

Whilst it is commonly accepted that the economic, environmental and consumer benefits from the widespread adoption of passive RFID are paramount; the traditional proposal for item-level tagging is inadequate because the typical passive tag can be surreptitiously read by any compatible reader. This poses tremendous privacy issues and exposes consumers and industry to crime.

Although some have proposed solutions such as the removal or disabling of tags at the point of sale, consumer associations and privacy advocates are not convinced because these methods are unreliable, cumbersome or require extra action by consumers. In particular, it is feared that vulnerable groups such as children, the elderly or technology-unaware citizens might fail to protect themselves. The hitherto proposed solutions also prevent valuable applications such as anti-counterfeiting, domestic uses of RFID and packaging recycling. Similarly, privacy and security issues are not limited to consumers and extend to industry – e.g. misuse of tags for industrial espionage, counterfeiting or terrorist abuse. Solutions based on encryption or authentication render tags too expensive or slow for most industrial applications.

Friendly Technologies has invented a novel RFID approach that allows the item-level tagging of common objects with very affordable passive tags that pose no privacy or security issues for consumers and industry. However, the proposed system requires the development of custom-made tags, compatible readers and supporting software; none of which currently exists at commercial level.

The objective of PEARS Feasibility is to demonstrate commercial and technical feasibility of such alternative by exploring the market and developing business cases, determining the necessary technology capabilities and viable costs for high-volume applications, and researching on technical alternatives for the development of a commercial product.

Project Results

Although the project has not reached its conclusion, results to date have been very promising.

On the side of technical feasibility, several solutions have emerged, either with existing technologies. Moreover, advanced simulation software created within the project demonstrated that current technology capabilities (e.g. bandwidth) suffice to support a polling-based tracking system, even in the most complex retail environments. On the side of the commercial feasibility, the added security and privacy at a lower device cost has opened the possibility of countless applications, particularly in the fashion, library and jeweller industries.

Further information:

Partners: Friendly Technologies, TETAS, Thales, ERCIM, OSI

Contact: Humberto Moran;
Friendly Technologies Ltd
Unit 4; Aberdeen Science and Tech Park;
Scotland / UK

Tel.: +44-122-4824 322

E-mail: Hmoran@friendlytechnologies.eu

Internet: www.friendlytechnologies.com

Duration: 15.06.08 – 15.10.09 - 36 Months

PrimeLife

Privacy and Identity Management in Europe for Life

When surfing the web today, users leave digital traces without noticing. This trail of personal data puts the autonomy of the individual at risk in an unprecedented way. Unlike footprints on the beach, which are washed away by the sea, data stored online do not dissolve after time but remain available for a lifespan and even beyond. But personal information must only be carved in stone where the user is aware of this an explicitly decides to do so.

Approach

Preserving privacy over a whole lifetime, in collaborative settings and virtual communities imposes new challenges to research. The paradigm of privacy protection by data minimisation fails for use cases such as web 2.0 applications where users need or want to reveal large amounts of personal data. Here the EC-funded project PrimeLife aims to solve the challenges concerning privacy, identity and trust management. PrimeLife's vision is to counter lifelong data trails without compromising on functionality. This requires substantial progress in the underlying technologies, and subsequent adoption. To reach these aims PrimeLife is segmented into highly interacting activities.

Privacy in Life

The project is arranged around the activity "Privacy in Life" which studies how privacy can be established in real life. Demonstrators will be built to validate the research done and to show how the challenges of lifelong privacy can be met. The demonstrators build upon the requirements collected and the research done within PrimeLife's other activities.

Mechanisms

The activity "Mechanisms" researches on basic methods for privacy-enhancing identity management and trust establishment inter alia by refining existing cryptographic methods such as anonymous credentials.

Privacy Live

The dissemination activity "Privacy Live" interacts with the community and other EU projects to support the use of the developed privacy-enhancing mechanisms. To this end, PrimeLife organises workshops, contributes to standardisation bodies and provides educational material for pupils, students and the broader public.

Usability

The best privacy, identity and trust management mechanisms are useless if intuitive interfaces are missing. Users need guidance to understand privacy-enhancing identity management, trust and assurance models or privacy policies. Such interfaces are provided by the activity "Usability".

Policies

"Policies" are the central mechanism for enabling privacy, identity and trust management. In particular, policies must govern such a system from end-to-end and throughout different applications. All other activities will employ policies for practical implementations in tools or demonstrators. The goal of the policy activity is to gather the requirements and to specify the required languages.

Infrastructures

The activity "Infrastructures" addresses the question what kinds of infrastructures are needed for privacy, identity and trust management. It collects the requirements of such an infrastructure and proposes how these can be met.

Further information:

Partners: IBM, ULD, TUD, KU, UNIMI, GUF, TILT, W3C, K.U.Leuven, UNIBG, GD, CURE, EMIC, SAP, UBR

Contact: Marit Hansen; c/o Unabhängigs Landeszentrum für Datenschutz (ULD) Holstenstraße 98; DE-24159 Kiel

Tel.: +49-431-988-1200

E-mail: primelife@datenschutzzentrum.de

Internet: www.primelife.eu/

Duration: 01.03.08 – 28.02.11 - 36 Months

RACE networkRFID

Raising Awareness and Competitiveness in Europe

RFID will form the basis of better and safer healthcare, drastically improved supply chain management, low cost environmental monitoring for a cleaner, more sustainable future. We need a pro-active European approach so that we can benefit from the advantages of RFID while giving citizens, consumers and businesses choice, transparency and control. – Viviane Reding, *EU Commissioner for Information Society & Media*

A New European Union Thematic Network Project

"With founding partners from 17 countries and representatives from Europe's leading research and standards organisations, RACE networkRFID will build on the EU's already substantial investment in RFID research to increase awareness and grow the European market for these rapidly evolving, world changing technologies."

Our vision:

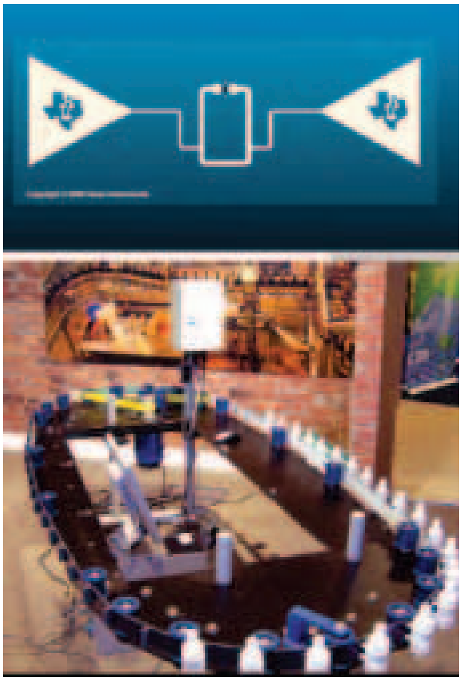
"To provide a Radio Frequency Identification (RFID) network of excellence that creates opportunities and increases the competitiveness of European Member States in the area of RFID through innovation, development and implementation. At the same time it will position RFID technology within the mainstream of information and communications technology."

The network draws upon the expertise of Member States and the evolving RFID community to create a dynamic, change-responsive capability that not only aligns with the initial Information and Communication Technologies Policy Support Programme objectives, but extends that capability to accommodate emergent and future needs.

RACE networkRFID will meet the pressing need to generate greater awareness and uptake and the exploitation of user-facing opportunities for innovation and enterprise. It will capitalise on work done by European projects and national initiatives to confirm Europe's position as a leading force in RFID.

RACE network RFID will:

- Create a federating platform to the benefit of all European stakeholders in the development, adoption and usage of RFID.
- Position the European Union as a world leader in RFID excellence.
- Establish the market position for RFID in Europe, defining the roadmap and addressing the barriers to adoption and deployment as well as fragmentation in the market.
- Promote best practices, case studies, reports, guidelines, events and services to increase awareness at European and national level.
- Involve a large number of Member State authorities dealing with public RFID issues including major industry, civil society, RFID advocacy groups and research agencies.



In addition it will:

- Provide a structure for initiating, developing and sustaining a large variety of support measures to promote the take-up of RFID with appropriate attention to associated automatic identification, Data capture and communications technologies and their potential within application designs.
- Focus attention upon SME business communities and the potential that exists within them for product, process and services innovation.
- Address the requirements of policy-makers and the public to ensure that both businesses and consumers benefit from RFID with a specific focus on consumer trust and acceptance, innovation and enterprise.

Further information:

Partners: ERCIM coordinates the RACE networkRFID project; for a complete list of project partners please visit the project website

Contact: Philippe Rohou;
ERCIM, the European Research Consortium for Informatics and Mathematics

Route des Lucioles, Sophia Antipolis
F-06410 Biot
France

Tel.: +33-497-155-306

E-mail: race-networkrfid@ercim.org

Internet: www.race-networkrfid.eu

Duration: 01.03.2009 – 31.03.2012 36 months

SMART

Intelligent Integration of Supply Chain Processes and Consumer Services based on Unique Product Identification in a Networked Business Environment

The SMART project employees RFID technology, data-stream management systems and a service-oriented architecture in order to support intelligent business networking and consumer services based on information/ knowledge sharing and collaboration among supply chain partners. The distributed service-oriented architecture of SMART can potentially support various RFID-integrated supply chain services. Special emphasis has been placed on the following two application scenarios:

- Dynamic Pricing, enabling supply chain partners to monitor back-room/ shelf inventory and expiration dates of individual product items and accordingly adjust product prices, and
- Promotion Management, enabling supply chain partners to monitor shelf availability, shelf replenishment and promotion-stand sales for products on promotion.

The two SMART services that showcase the applicability of RFID in the retail context have been analyzed, designed and then deployed in three real-life pilot sites. Specifically, the Promotion Management service has been deployed in two supermarkets in Greece and Cyprus, while the Dynamic Pricing service has been deployed in one supermarket in Ireland.

Project Results

The project's results and overall outcome include:

- Innovative in-store consumer services and new supply chain collaboration scenarios which exploit the capabilities for unique-product identification and real-time information.
- A scalable, reliable and secure infrastructure supporting information sharing, collaboration and electronic services in the above context.
- The provision of reliable and real-time end-to-end information about product quality and history to supply chain partners as well as to educated consumers through innovative electronic services.
- The assessment from a business and marketing perspective of the impact that the developed services have on consumers.
- The formulation of an integral systematic approach to analyse, design, model and evaluate alternative implementations of RFID-integrated supply chain services.

SMART was completed in June 2009. The consortium is continuing its work in their fields of expertise and is providing the following consultancy and products: SMART application platform, SMART middleware, SMART Data Stream Management System, SMART promotion stand as well as Consultancy based on the SMART methodology.

Further information:

Partners: Intrasoft International S.A., Athens University of Economics & Business (AUEB) – ELTRUN research group, WHU School of Management, Trinity College Dublin, Cambridge Auto-ID Labs, Alpha-Mega Papaellinas Super-markets, Veropoulos Super-markets, Superquinn Retailer, Rilken-Henkel S.A., Cyberce, Planning Cyprus Ltd.

Contact: Katerina Pramatari;
Athens University of Economics & Business
47A Evelpidon & 33 Lefkados Str.;
GR-11362, Athens
Greece

Tel.: +30-210-8203 663

E-mail: K.pramatari@aueb.gr

Internet: www.smart-rfid.eu

Duration: 01.11.06 – 30.06.09 - 32 Months

SMMART

System for Mobile Maintenance Accessible in Real Time

SMMART is an innovative approach of logistic and maintenance services based on ubiquitous availability of "in service" product data for air, road, rail and marine transport:

- To reduce maintenance cost
- To minimise unscheduled downtime
- To assist mobile workers wherever they operate.

SMMART key challenges

- To monitor in real-time the usage and maintenance data throughout the life-cycle of critical sub-assemblies of a vehicle.
- To optimise maintenance management through a worldwide network.
- To provide new services: advanced troubleshooting tool, global configuration control, resource planning tool.
- To remotely exchange information between all life-cycle stakeholders in a timely, secure and trusted environment.
- To provide end-to-end visibility of the logistic supply chain.
- To improve industrial and logistic traceability.
- To optimise maintenance and logistic planning.
- To further improve transportation safety.

SMMART technical approach

SMMART is the combination of:

- Smart items capable of operating and communicating wirelessly in the harsh environment of vehicles.
- Integrated ground information system providing data collection and processing to supply added value services Worldwide in a fully secured network
- Re-engineered business processes addressing technological, organisational and social aspects to support the SMMART concept implementation within the end-user community.

SMMART results

Technological breakthrough:

- RFID tag system operating in the harsh, metallic, cumbersome environment of engines
- Wireless, auto adaptive sensor networks
- RFID tag systems for track and trace in Maintenance workshops
- End to end data security and trust system
- Innovative, high added value software features as configuration control, trouble shooting, strategic forecasting and optimisation.

System Integration:

- 2 demonstrations, on truck and on helicopter engine successfully validated the end to end integration.

Further information:

Partners: Tricon Consulting, 2MoRO, 2MoRO, Commissariat a l'energie atomique, Ecole Superieure des Technologies Industrielles Avancees, Eurocopter, TDM, Thales, Thales Communication, Turbomeca, Snecma Services, CAM, Fraunhofer, Uni Stuttgart, TELETEL, Uni Degli Studi di Milano, M&M Service, Warsaw School of Economics, Robotiker, MIK S.COOP, VOLVO Technology, Avonwood Developments, Microturbo, Universal Pipe Enterprises

Contact: Jean-Louis Boucon;
Turbomeca

av Joseph Szydlowski
BP 39 ; FR-64511 Bordes Cedex, France

Tel.: +33-(0)-559-1251 10

E-mail: Jean-louis.boucon@turbomeca.fr

Internet: www.smmart.eu

Duration: 01.11.05 – 31.10.2008 - 36 Months

StoLPaN

Store Logistics and Payment with NFC

The StoLPaN project aims to define open commercial and technical frameworks for NFC-enabled services on mobile devices. These frameworks will facilitate the deployment of NFC-enabled mobile applications across a wide range of vertical markets, regardless of the phone type and the nature of the vices required.

The StoLPaN Project

The StoLPaN project intends to turn NFC (Near Field Communication) enabled mobile handsets into multifunction terminals with bi-directional interaction between the wireless NFC interface and mobile communication channels. It will show the use of this generally applicable new technology in the retail logistical value chain, and also in mobile payment, ticketing and other use cases. Mobile NFC services are developed based on their existing contactless use cases and also on the available infrastructure, but their features are enhanced through the functional capabilities of the mobile handsets and the remote application management potential.

Project Results

StoLPaN defines the Commercial and Technical Frameworks required managing multiple third party applications on NFC-enabled mobile devices. This is achieved by defining the Use Cases for the major applications and refining them with both the Service Providers, Mobile Network Operators and also with key players in the current Value Chain for the issuance and management of those products.

The resulting Use Cases are analysed to identify common set of Business Rules that define the roles and responsibilities of every player in the NFC Ecosystem. These Rules, in turn are used to define the Technical Requirements for the loading, use, maintenance and deletion of any NFC-enabled application on any mobile device.

The results are demonstrated in a Host Application developed by the project team.

The Host Application will be the physical embodiment of the Business Rules and Technical Requirements. It simultaneously supports multiple NFC services, will provide access to the phone's resources and facilitate the loading, use and maintenance of third party NFC-enabled applications through the provision of a Common API between the third party application and the mobile device's operating system.

As one of the demonstrations of the new mobile NFC platform StoLPaN specifies a smart retail environment based on item level tagging and NFC supported smart applications. The goal of this program is to create a user friendly, convenient shopping experience for the customers and to improve economics and efficiency of the retail operation.

Further information:

Partners: Motorola Ltd., SafePay Ltd., Deloitte Ltd., Budapest Tech., Auto-ID-Labs St. Gallen, BULL Ltd., Consult Hyperion, Fornax Plc., University of Technology and Economics, Banca Popolare di Vicenza, Libri Bookstores Ltd., Baker &McKenzie, Consorzio Triveneto S.P.A., SUN Microsystems Ltd., IQ-Systems Ltd., NXP Italia Spa., University of Rome, Ennova Research S.r.l, Sheffield Hallam University, NXP France, AFF Ltd.

Contact: Andras Vilmos;
SafePay Systems. Ltd.

Beg street 3-5; H-1023 Budapest
Hungary

Tel.: +36-1-2124 321

E-mail: Vilmos@stolpan.com

Internet: www.stolpan.eu

Duration: 01.07.06 – 31.12.09 - 42 Months

STOP

SToP Tampering of Products

SToP Tampering of Products (SToP) - Understanding and combating the problem of product counterfeiting with ambient intelligence based solutions.

The SToP Project

The markets for counterfeit products are growing worldwide, comprising virtually all industry sectors from spare parts and pharmaceuticals to luxury goods. Counterfeits damage the reputation of brand owners, produce economic losses, promote inferior working conditions, and put the safety and health of consumers at risk.

The SToP project takes a holistic approach at combating product counterfeiting. Drivers fuelling the recent increase in counterfeit trade, entry points of fake products into licit supply chains, and strategies of counterfeiters are analyzed to gain an in-depth understanding of the problem and its context.

Based on this analysis, the SToP project developed secure, reliable, convenient and cost effective product authentication approaches as well as anti-counterfeiting services to support activities that target the reduction of trade with illicit products. The solutions provided are based on RFID and related ambient intelligence technologies. The approaches are tailored to the specific requirements in different industries and will be used as an integral element of their anti-counterfeiting strategies.

Project Results

The project's results and overall outcome include:

- An analysis of the structure, the mechanisms, and the extent of the illicit market and the supply- and demand-side drivers of trade with counterfeit products,
- A business case framework to assist governments and companies (especially small and medium sized enterprises) to calculate the impact of illicit trade on brand name and revenue, the required financial investments to counterfeiting, and the return on investment,
- Novel product authentication approaches based on ambient intelligence technologies, in particular RFID technology and the analysis of tracking data,
- Innovative smart tagging technologies suitable for authentication,
- The product verification infrastructure, a software prototype that supports enterprises manufacturing and delivering authentic products to customers and allows consumers and supply chain participants to check the authenticity of products with a combination of various approaches,
- Integration concepts for various industries that help organisations to seamlessly integrate solutions into their products as well as their business process landscape,
- Real-world application trials that assessed the feasibility and performance of the solutions.

Further information:

Partners: SAP AG, Novartis Pharma AG, Richemont International SA, Bundesdruckerei GmbH, Airbus Deutschland GmbH, Spacecode SA, Oria Computers

Contact: Harald Vogt;
SAP AG

Vincenz-Priessnitz-Str. 1
DE-76131 Karlsruhe
Germany

Tel.: +49-622-7752-551

E-mail: Harald.vogt@sap.com

Internet: www.stop-project.eu

Duration: 01.11.06–30.06.09 – 32 Months

TraSer

Identity-Based Tracking and Web-Services for SMEs

The recently completed three-year FP6 STREP project TraSer was called to life with the primary goal of developing a free, open-source solution platform for tracking and tracing of items with unique identity. The main user group targeted by the project are small or medium-sized enterprises (SMEs) acting in production and delivery networks where flexible adaptation to varying track-and-trace systems as well as existing elements of the company's IT infrastructure is vital. With this objective, especially regarding the targeted user range, TraSer ventured beyond the state of the art, as the mainstream of today's off-the-shelf solution kits are targeting larger companies with high production volumes and sufficient financial power for large initial investment.

Aside from developing the solution platform, the TraSer project complemented the software package by case studies and tutorials. In addition to frequent industrial feedback through reference implementations, the project also explored the scientific backgrounds of phenomena related to tracking and tracing.

Project description

The project focused on the development of an industry ripe entry-level solution kit. The platform handles tracked material on the level of unique instances (as opposed to stock levels), and relies on web services for communication. Item-related data are maintained by TraSer servers communicating with each other if queries or updates are forwarded or broken down to distributed components. TraSer clients serve as interfaces "to the rest of the world", e.g., human operators, automated checkpoints or other components of the given IT infrastructure.

Aside from its focus on SMEs, TraSer is set apart from most other comparable frameworks by following key features:

- While being capable of adopting any item-level numbering scheme, TraSer uses a provider-independent internal identifier notation, making a start less burdensome for small-scale users.
- TraSer is free and open-source, and its implementation relies on open-source frameworks. Interface specifications allow easy implementation of special building blocks, or reimplementing a TraSer solution in a different development environment.
- TraSer offers useful functionalities for handling item-centric data: advanced search and aggregation support, views at historical data, or backtracking of information. These facilitate special actions, such as focused recall campaigns or locating of certain goods in the production chain.
- A special release of the TraSer platform is optimized for tracking virtual artefacts, e.g., CAD files, supporting collaborative design across company borders.
- TraSer allows a flexible definition of data models and facilitates this with its XQuery-based interfaces, which is of special importance for enterprises of high product variability.

With its versatility and flexibility, the solution platform can easily pave the way to providing services in the "Internet of Things" context.

Further information:

Partners: MTA SZTAKI; Helsinki University of Technology, University of Groningen; Innotec Magyar Kft.; Itella; TNO; ROPARDO

Contact: Dr. Elisabth Ilie-Zudor; MTA SZTAKI

Kende u. 13–17; H-1111 Budapest Hungary

Tel.: +36-12-796-195

E-mail: Ilie@sztaki.hu

Internet: www.traser-project.eu

Duration: 01.06.2006–31.05.2009; 36 months

WALTER

Specifying, testing and improving interoperability of broadband radio devices

WALTER addresses the need for broadband testbeds by overcoming the technical issues of measuring low level, high data-rate radio signals. The resulting worldwide interconnected testbeds will address the short term needs of industry and regulators but also the longer-term needs of research communities.

Main objectives

High data rate radio protocols are key developing technologies for emerging user applications. However, they raise issues of efficient radio spectrum management and interoperability within the technologies. New emerging technologies for future ubiquitous network infrastructures and architectures include high data rate technologies for Intelligent Transport Systems (ITS), delivery of services to the home ("digital home"), and pedestrian, to the general vehicular sectors, to the industrial and supporting sectors, and to the Public Protection and Disaster Relief (PPDR) organizations (national, regional and global). Ultra Wide Band (UWB) is a very promising technology for such broadband transmission of data using spectrum efficient and flexible radio techniques. Initiatives by the WiMedia Alliance have developed concepts to use UWB as a standard radio platform. This allows the transport of wireless USB (WUSB), wireless Firewire and the next generation of Bluetooth 3.0. The European Telecommunications Standards Institute (ETSI) is producing harmonised standards to foster UWB adoption in Europe.

Contributions

- Consolidation of test procedures in ETSI Harmonized Standards for broadband wireless devices in support of EU Directives.
- Assist future development of UWB Harmonized Standards including mitigation techniques and coexistence mechanisms with potential radio victim services.
- Assist interoperability between UWB devices using multi developer plug tests.

Technical Approach

The WALTER project is split into two phases:

- The first phase will standardize and validate the testbed architecture and test procedures for the first ETSI harmonized standard on UWB communication devices (ETSI EN 302 065).
- The second phase will deal with the development of test procedures for later ETSI harmonized standards, also including research activities, to cover mitigation techniques and coexistence mechanisms using Detect And Avoid protocols.

The technical work to be achieved is spread among four work packages (WP3-WP6). WP3 will identify the needs of the project in the field of existing and future broadband wireless technology requirements. This will provide input to WP4 and the development of the procedures to meet these needs. WP5 will be the crucial phase for the conception of the testbed and its validation. Finally, test services and experiments will be offered in the last WP (WP6) thanks to this new test environment.

Key Issues

The key issues to be addressed by the WALTER project are the following

- To support convergence and interoperability of broadband wireless networks.
- To support flexible and spectrum efficient radio access.
- To support the establishment of global standards while addressing complex user requirements.
- To reinforce European industrial leadership in wireless networks.

Expected Impact

WALTER is aimed at giving Europe the tools to foster its UWB development, and positioning the EU as a world leader in the domain. The project is expected to make a number of impacts at the European level.

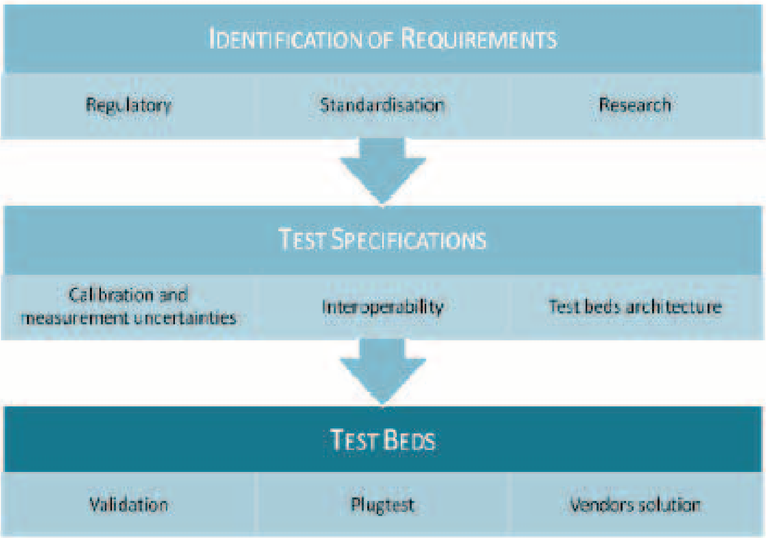
- Contribute to the establishment of a worldwide acceptance of European standards for UWB technologies.
- Give the tools aimed at ensuring that newly developed UWB technologies do not compromise persons and goods protection.
- Contribute to interoperability of UWB technologies and convergence of high capacity based services.
- Give the European industry a competitive advantage while opening the door to new innovations in the field of internet technologies based on ubiquitous networks.

Dissemination events

The main activities to be achieved for dissemination purposes are as follows:

- Coordination with international organizations to push ETSI standards forward.
- WALTER design and implementation to be made publicly available for any test facility wishing to develop a certification program.
- Website allowing access WALTER documentation and allowing public participation through an on-line forum.
- Presentation of the WALTER achievements at international level conferences.
- 2 multi-vendor plug tests.

These activities will be complemented by publication in specialised newspaper and presentation at international conferences.



Further information:

Partners: inno TSD, ETSI, Copsey Telecommunications Ltd, AT4Wireless, STMicroelectronics, JRC IPSC, Wisair, TMC

Contact: Franck Le Gall;
inno TSD

Place Joseph Bermond Ophira 1 - BP63;
F-06902 Sophia Antipolis Cedex,
France

Tel.: +33-49-238-8418

E-mail: contact@walter-uwb.eu

Internet: www.walter-uwb.eu

Duration: 01.01.2008–31.12.2009; 12 months

European Commission

Luxembourg: Publications Office of the European Union

2010 — 229 pp. — 17,6 × 25 cm

ISBN 978-92-79-15088-3
doi:10.2759/26127

HOW TO GET EU PUBLICATIONS

Free publications:

- via EU Bookshop (http://bookshop.europa.eu);
- at the European Commission's representations or delegations.
  You can obtain their contact details on the Internet (http://ec.europa.eu/) or by sending a fax to +352 2929-42758.

Priced publications:

- via EU Bookshop (http://bookshop.europa.eu).

Priced subscriptions (e.g. annual series of the *Official Journal of the European Union* and *Reports of Cases before the Court of Justice and the Court of First Instance*):

- via one of our sales agents. You can obtain their contact details on the Internet (http://publications.europa.eu/others/agents/index_en.htm).

KK-31-10-323-EN-C

European Commission
Information Society and Media

For further information:

Information Desk
European Commission - Information Society and Media DG
Office: BU25 02/59 B-1049 Brussels
Email: infso-desk@ec.europa.eu
http://europa.eu/information_society

Publications Office