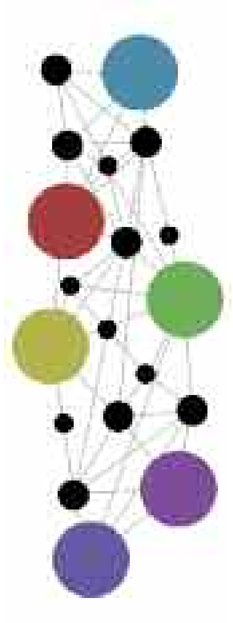


CASAGRAS

an EU Framework 7 Project

Coordination
And
Support
Action for
Global
RFID-related
Activities and
Standardisation

Final Report

RFID
and the Inclusive Model for the Internet of Things

EU Project Number 216803

CASAGRAS will 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'.

CASAGRAS

an EU Framework 7 Project

The CASAGRAS PARTNERSHIP

CASAGRAS (Grant Agreement 216803) is a Coordination and Support Action for Global RFID-related Standardisation Activities involving, in particular, organisations from China, Japan, Korea and the USA.

Ian G Smith

Prof. Dr.
Ken Sakamura

Prof. Dr.
Anthony Furness

Ricky Ma

Yong-Woon Kim

Eldor Walk

AIM UK - Ian Smith, Co-ordinator, President of AIM UK

YRP, Ubiquitous Networking Laboratory, Japan
- Professor. Dr. Ken Sakamura

AIDC, UK - Professor/Anthony Furness,Technical Co-ordinator

Supply Chain Innovation Centre, Hong Kong Science and Technology Parks Corporation, China - Ricky Ma

ETRI, Electronics and Telecommunication Institute, Korea - Yong-Woon Kim

FEIG Electronic gmbh, Germany - Eldor Walk

QED Systems, USA - Craig Harmon

Praxis Consultants - Paul Chartier

ETSI, European Telecommunications Standards Institute, France - Patrick Guillemin

RFIP Ltd - David Armstrong

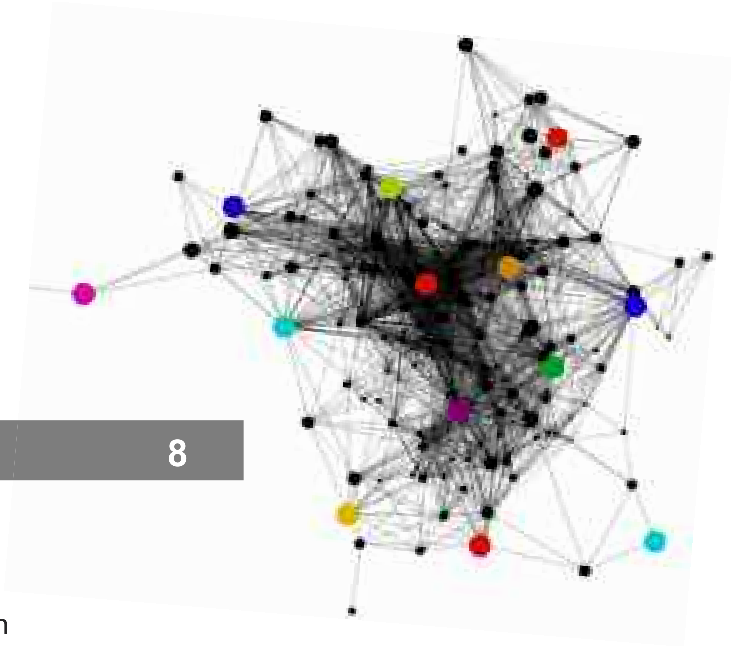
Craig Harmon

Paul Chartier

Patrick Guillemin

David Armstrong

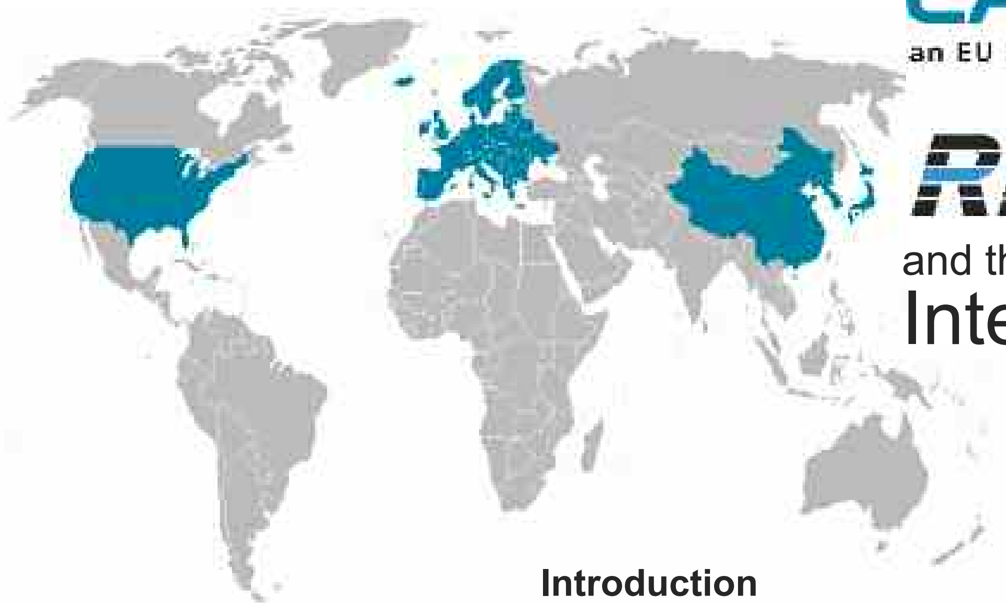
The partners extend their sincere appreciation to members of the Extended Experts Group who have advised on various aspects of the CASAGRAS Project, to our Project Officer at the EU and his colleagues, and the Project Evaluators.



Contents

CASAGRAS

an EU Framework 7 Project



Final Report

RFID and the Inclusive Model for the Internet of Things

Introduction

CASAGRAS (Coordination and Support Action for Global RFID-related Activities and Standardisation) is a European Framework 7 project. Its remit has been to consider the international dimensions concerning regulations, standardisation and other requirements for realising the concept known as the Internet of Things, and the role within it of radio frequency identification (RFID).

The 'Internet of Things' is a concept that receives considerable and significant consideration and support within the European Commission (EC) with respect to strategic developments in Europe for information and communications technology (ICT) and the Information Society. The Commissioner, Viviane Reding in her speech to the Future of the Internet initiative of the Lisbon Council [1] identified the Internet of Things (IoT) as an important driver for the Internet of the future. The IoT has been the focus of three presidential conferences addressing the subject in relation to radio frequency identification (RFID). It is seen as one of the pillars supporting the future networked society and structured on a foundation of future network infrastructure [2].

An EC communication [3] to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, entitled "Internet of Things – An Action Plan for Europe" was adopted on 18th June 2009 and reinforces the commitment to the concept and its importance for Europe, quoting in its conclusions:

> *That the "Internet of Things (IoT) is not yet a tangible reality, but rather a prospective vision of a number of technologies that, combined together, could in the coming 5 to 15 years drastically modify the way our societies function.*
>
> *By adopting a proactive approach, Europe could play a leading role in shaping how IoT works and reap the associated benefits in terms of economic growth and individual well-being, thus making the Internet of things an Internet of things for people."*

Despite the already substantial investment in EU framework projects directed to underpin the concept of the 'Internet of Things' there appears to be little awareness of the subject and its potential within the business and industrial communities, in respective member states and indeed the rest of the world. As stated in the EC communication referenced above the 'Internet of Things' is not yet a tangible reality, but technology experts believe that, given the resource and attention now being expressed through European initiatives and elsewhere around the world,

[1] Reding, V (2009), Internet of the future: Europe must be a key player, Speech to the Future of the Internet initiative of the Lisbon Council, Brussels, 2nd February 2009.

[2] Future Internet Assembly (FIA) http://www.future-internet.eu Real World Internet (Internet Of Things) cluster of FIA http://rwi.future-internet.eu/index.php/Main_Page

[3] The adopted text is available on: http://ec.europa.eu/information_society/policy/rfid/index_en.htm.

On http://eurlex.europa.eu/en/index.htm as soon as published in the official journal (1-2 days).

The press material: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/740&format=HTML&aged=0&language=EN&guiLanguage=en

it seems probable that, in one form or another, the concept will become a reality in the very near future. The challenge is to ensure that it is an effective, internationally acceptable realisation.

The IoT is now a focus for the Cluster of European Research Projects on the Internet of Things (CERP-IoT) and its remit is to prepare a strategic research agenda (CERP-IoT Research Roadmap)[4] specifically directed at the IoT. So too the European funded Real world Internet (RWI).[5] The views of both projects have been considered in relation to the CASAGRAS findings and recommendations.

The Internet of Things has been viewed as a "metaphor for the universality of communication processes, for the integration of any kind of digital data and content, for the unique identification of real or virtual objects and for architectures that provide the 'communicative glue' among these components".

RFID is seen as a means of uniquely identifying objects and via RFID in particular, the Internet of Things is being seen as the means of connecting real world items with further data and digital 'brains' and vice versa, accommodating too software systems with sensor and context information accessed by RFID tags. What constitutes 'digital brains' in this context requires qualification and will undoubtedly be viewed as a collective term for varying degrees of processing capability and intelligent functionality.

In the minimalist version of the Internet of Things these supported objects may be identified but do not 'do' anything actively, cannot communicate one with another and do not display any level of intelligence. In the strongest version, object sets can be identified that communicate with each other exploiting the potential of ubiquitous computing and ubiquitous networks. It is also being seen as a vehicle for achieving actuation and control in real world applications.

An earlier view of the Internet of Things [6], looking at the likely manifestation in 2020, provides a speculative roadmap for the future. While it draws attention to a variety of wider technology trends and enablers, together with a range of prospective applications, it lacks attention to the architectural framework for such an Internet. It also lacks an underpinning analysis of the object-connection concept to support the proposed roadmap.

With the evolving Internet seen as a support structure for the IoT some would argue that the IoT could be left to evolve naturally as applications and supporting technology develop. Such an approach would undoubtedly lead to problems of interoperability, scale and functionality, security, privacy and of course governance, to name but a few. These problems are also likely to be exacerbated by the prospective, largely autonomous nature being envisaged for the IoT, particularly where the applications involve actuation, control and sensitive data. It seems a more sensible strategy to specify a flexible framework for an IoT structure and constructively control development of that structure in order to take account of the wide ranging technical and socio-economic factors to be properly accommodated. This will require active organisation and management.

In considering the broader aspects of the framework it is also important to recognise the concept of a virtual object space. Within this concept objects are represented in electronic visual and representational media. The objects concerned may be created in this space, derived from physical object space and indeed have a mapped relationship to objects in physical space. Depending upon applications these objects may require specific aspects of identification and may indeed, in some cases, constitute part of an identification process – for example a biometric image or graphical template. Mapping and identification may also have particular significance in simulation studies, and with respect to single and multiple objects.

[4] CERP-IoT Research Roadmap, Draft version V1.9 –15 September 2009.

[5] Real world Internet, http://rwi.future internet.eu/images/c/c3/Real_World_Internet_Position_Paper_vFINAL.pdf <http://rwi.future-internet.eu/images/c/c3/Real_World_Internet_Position_Paper_vFINAL.pdf>

[6] INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems Groups in co-operation with the Working Group of the ETP EPoSS – Internet of Things in 2020, 27 May 2008.

Some would argue that the IoT is already in being, based essentially on islands of applications that relate to objects being identified and included in networked systems. Developments in sensory and actuator networks (SANs),[7] and particularly wireless and so called 'intelligent' sensory networks [8] add to this view. Unfortunately, this is only part of the IoT potential picture. There are many elements that could contribute to the realisation of an IoT concept and a bit like a jigsaw puzzle they require putting together, and in the right way to achieve a defined goal such as the realisation of cooperative services and applications. There could be significant system benefits and cost efficiency from a synergistic combination of entities that allow more to be gained from the whole than could be achieved from the component parts.

The keynote is that of flexibility combined with well formulated strategy to allow functionality and scalability to evolve with the minimum of legislative constraint on innovation and network capability, whilst maintaining appropriate governance and protection with respect to privacy, security and network functionality. In order to successfully achieve these benefits a proactive approach to provide a migration strategy is required, in order to accommodate progressive new technologies, principles, standards and legislation.

Given these wider issues concerning the IoT the CASAGRAS remit has been revised to embrace these wider considerations and to specify, if only in outline, a progressive framework for IoT realisation. Within this wider consideration the need was seen for aligning with and contributing to the on-going debates in relation to the IoT, including emergence and developments of concepts such as 'real world awareness' (RWA) and applications in the enterprise world, [9] Real World Internet [10] and the cluster manifestations arising out of the CERP-IoT activities.[11]

The CASAGRAS view identifies a fully inclusive model for the Internet of Things, and seeks to provide both a framework and migration pathway for realising such a model. Within this framework RFID and other identification and data capture (AIDC) 'edge' technologies, and associated sensory, communication, location and security technologies, are recognised in the architectures for interfacing with the physical world. The model identifies a layered approach to interfacing with the physical world through the use of object-connected or item-attendant identification and data capture technologies, linked through network structures that constitute the existing and future Internet. Intermediate layers provide for interrogator and gateway transfer devices, localised hosts, networked hosts and wider communication networks.

To identify objects in the physical world requires identification techniques of various kinds and the means of acquiring and acting upon the identification. With a range of natural feature and data carrier-based identification available, a strategy is required to include them on a progressive basis. Radio frequency identification (RFID) is seen as a very capable technology in this respect and, in combination with other technologies, may be key to the successful realisation of the IoT, but is not suitable for all objects either on the basis of cost, form factor or functionality and functional attributes of an IoT.

[7] Gluhak, A et al (2009) Towards an architecture for a Real World Internet, Towards the Future Internet (Eds; Tselentis, G et al.), IOS Press 2009.

[8] Novak, J (2007), Intelligent Sensors and Sensor Networks, Modern Sensors Handbook (Eds: Ripka, P & Tipek, A), ISTE

[9] Haller, S (2009), Potential Applications in the Enterprise World, Proceedings of the Prague Workshop Report on the Internet of Things – an early reality of the Future Internet, June 2009.

[10] Gluhak, A et al (2009) Towards an architecture for a Real World Internet, Towards the Future Internet (Eds; Tselentis, G et al.), IOS Press 2009.

[11] CERP-IoT (2009), CERP-IoT Research Roadmap (Draft version v1.9) June 2009.

To allow objects to be linked, or networked, at the object level requires processing and communications capability, either embedded or attached to the objects concerned. Because of cost and size constraints these processing and communications platforms cannot be applied to all objects. As costs and size of such platforms, reduce the population of objects so supported will increase, possibly on an exponential basis. As a consequence the populations of networked structures may similarly rise. However, identification and the capability to network are not the only factors determining the populations of networked objects that may arise. Functionality is also a factor, the ability to sense or otherwise provide data is required to give meaning to the network. A further factor of functionality is actuation and the facility to effect a control function through single interfaced devices or through suitably supported nodes in a network. Time stamping, (providing a temporal cue) and identification of location (providing a spatial cue) may also feature in such structures and contribute to application functionality.

A further facet of network requirement to support an IoT is the need for self-managing, self-monitoring, self-diagnosing and even self-repairing structures to accommodate particularly those applications involving object-to-object communications and functionality, where the presence of a sentient human agent is absent. Here the sentient component must reside within an artificially intelligent agent, the degree of so called intelligence being matched to the need. Evidence can be seen for developments and standardisation in this direction in the form of autonomic network engineering.[12]

To achieve appropriate identification and interfacing between layers or networks requires the use of harmonised or standardised identification systems and protocols. Without them the prospect is one of large scale lack of interoperability. With a wide range of numbering and identification systems in use the need is seen for some method of accommodating these legacy systems. The CASAGRAS model defines a resolver approach to solving this problem, and to the requirements for integration within the evolving Internet.

A further part of the proposed CASAGRAS IoT model provides for the development of cooperative services and applications analogous to the World Wide Web (www) – a world object web (wow), with the prospect of encouraging and supporting wide ranging product, process and service enterprise and innovation. The business case structure and viability of the wow will need considerable further attention and consideration.

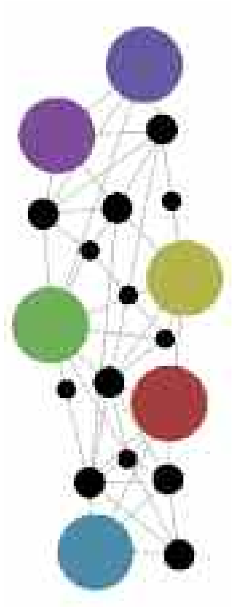
CASAGRAS

an EU Framework 7 Project

Final Report

RFID and the Inclusive Model for the Internet of Things

Still further aspects of the inclusive model address the issues of scalability, reliability, security, system integrity, autonomy and protection against network and systems attack, issues of privacy of personal data, to name but a few; and or course governance. By establishing a specific generic top-level domain (gTLD) the prospect can be seen for supporting in a controlled manner the structure, architecture and functional attributes for an IoT.



The following sections of the report present the background and outcomes of the CASAGRAS project in respect of this inclusive model and the migration route to achieving the fully inclusive structure.

[12] Chaparadza, R et al., (2009) Creating a viable evolutionary path towards self-managing future Internet via a standardizable reference model for autonomic network engineering, Towards the Future Internet (Tselentis, G et al., Editors) IOS Press, 2009.

CASAGRAS
an EU Framework 7 Project

RFID **Final Report**

and the Inclusive Model for the
Internet of Things

1 Background

The need for the CASAGRAS project is routed in the outcomes of a wide-range of framework investments and European strategy with respect to ICT that have been geared to technologies and the developing infrastructure necessary for realising an Internet of Things. Annex A (CASAGRAS, RFID and the Internet of Things) puts into context the role of the CASAGRAS project and its position in relation to other EC projects.

On a more pragmatic level CASAGRAS is seen as a coordination and support initiative directed at considering the Internet of Things as a global concept, requiring integration within the evolving Internet itself and international cooperation in realising a structure that could be of benefit to commerce and humanity across the globe. To pursue it as a competitive venture for Europe to gain competitive advantage was seen as short sighted. Through cooperation and synergy the opportunity was seen for a global advancement and a competitive, cooperative structure for global trade support and much, much more relating to human and environmental well-being.

1.1 EU Proactive Positioning

The goal set by the Lisbon Strategy for Europe was to develop "a highly competitive and dynamic knowledge-based economy". Radio frequency identification (RFID) was readily seen as an engine for growth and jobs, and a driver for realising the Lisbon strategy goal. The concept for the Internet of Things also became associated with this goal and the use of RFID within it. The European RFID Policy Outlook, working document [13] for the June 2007 conference, "RFID: Towards the Internet of Things" gave support to this view.

More recently (18th June 2009) a European Commission communication [14] to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, entitled "Internet of Things – An Action Plan for Europe" has demonstrated a commitment to the concept and its importance for Europe. The document concludes with the view that given a proactive approach Europe could play a leading role in shaping the Internet of Things and reap the associated benefits in terms of economic growth and individual well-being.

This proactive positioning and commitment within Europe has to be melded with a cooperative stance to respect other nations of the world and a cooperative move towards a global initiative that can benefit global trade and human endeavours. Failure to achieve this goal would mean

[13] European Policy Outlook RFID – Working document for the expert conference "RFID: Towards the Internet of Things, June 2007.

[14] The adopted text is available on: http://ec.europa.eu/information_society/policy/rfid/index_en.htm. On http://eur-lex.europa.eu/en/index.htm as soon as published in the official journal (1-2 days).

The press material:
http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/740&format=HTML&aged=0&language=EN&guiLanguage=en

missing an important opportunity, for Europe and the rest of the world. It is not simply about Europe achieving competitive advantage but about realising a global facility that can support competitive cooperative services and applications in the true spirit of commerce, cooperation and synergy.

As with the realisation of the Internet, the Internet of Things is a global issue, requiring international cooperation to achieve its potential. International cooperation is clearly required on a range of formative issues including:

- Identification and data transfer requirements
- Regulations in respect of communications and functional requirements such as those relating to privacy and security
- Network security and measures to ensure quality of service and autonomous network management
- Legislation in respect of network usage
- International standards and agreements in respect of IoT form, functionality and usage

Taken literally the Internet of Things (IoT) may be viewed as a network of physically connected objects, wherein embedded processing nodes with communication capability provide a means of networked functionality and communications that resemble those of the Internet. The notion of all physical objects being endowed with the capability to connect to such a network is fanciful, and in many cases without any justification for the object-to-object connections being proposed in speculative application scenarios.

The original concept for the Internet of Things was introduced through the Massachusetts Institute of Technology (MIT) using electronic product code (EPC) as a means of object identification. The concept asserted that the unique EPC-specified number contained within an objected-connected RFID data carrier could be read, using suitable readers or interrogators, and using an object naming service (ONS) directed as a pointer to information stored elsewhere. (A similar vision without the explicit use of RFID was proposed even earlier by Japan's TRON Project in the 1980's).

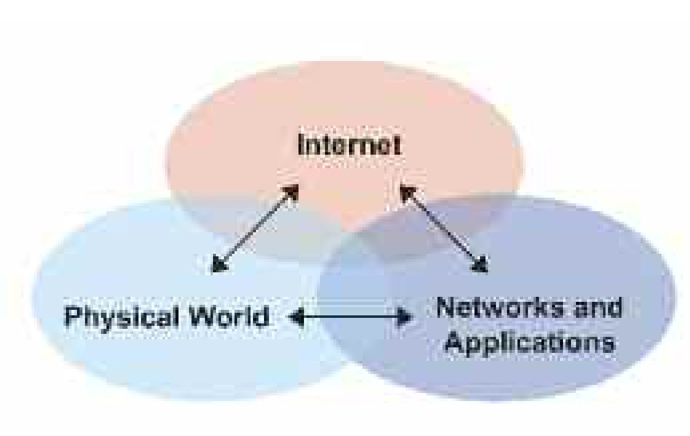
The same principle essentially relates to the use of data carriers in 'licence-plate' applications, the only difference being that the data or information is stored locally rather than within a prospectively global service support structure serving a potentially large number of service clients. In principle the stored information, for either local or a wider service support function, may be about the object concerned or information relating to the handling or processing of the object. Locally-defined functions may even be used to simply activate a process-related actuator of some kind, such as an electrically-operated barrier.

The CASAGRAS view of the Internet of Things goes beyond this EPC-based notion. The Casagras Vision is inclusive of a wide range of 'edge' technologies capable of interfacing with the physical world and also capable of accommodating numbering systems other than EPC. This is in keeping too with an IoT concept that is more formally based upon developments in ubiquitous networking and computing, and the notion of 'smart' objects. Smart objects in this context are objects with embedded, attached or accompanying support devices capable of providing a means of object identification, communication and / or processing, the level depending upon specified functionality.

In seeking to identify applications for the IoT it is clearly important to establish the nature of the development and what distinguishes it from the functionality of the existing Internet (into which it will be inevitably integrated) and other network developments, such as those between commercial organizations that are of a private or closed user-group nature (private networks). With the Internet of Things arguably in its nascent phase of development it is only possible to draw attention to the form that these applications might take and provide a precursory framework for applications and services that can be predicated upon the principles, architecture and technologies that are likely to impact on its development.

A 2005 ITU Internet Report forecasts the formation of the Internet of Things as an entirely new dynamic network-of-networks, influenced largely by the exploitation of radio frequency identification (RFID) technologies. Because of the network-of-networks nature being attributed to the Internet of Things it is of course possible to recognize network structures and applications that could fit in or migrate to an Internet of Things specification. Examples would include Sensory and ad hoc networks.

Any model for the IoT must clearly provide a link between the physical world and a virtual world, with the latter influenced significantly by the Internet itself.



The attention to ‘all things’ points to the need for defining application methodology that can assist in providing a better foundation for developing applications and services within domestic, public, industrial and other business settings. By characterizing “things” in business processes in respect of data/information, people, locations, assets, materials and utilities, principles can be derived for achieving enhanced process functionality (EPF) wherein corresponding identifiers are used to link and enhance given processes. These principles provide the keys to network-supported information and background processing that exploits an Internet of Things concept.

1.2 Defining the Internet of Things

Definitions for the Internet of Things have appeared in profusion, often structured to convey some fanciful notion of what such an Internet might provide. As a basis for considering a realistic implementation of such a network a more incisive proposition is[15] required. Despite the fact that the concept for the Internet of Things has been evolving for practically a decade it is still being defined. The European Policy Outlook, RFID working document for the June 2007 conference, “RFID: Towards the Internet of Things” makes reference to the surprising vagueness of definitions for the Internet of Things within technical trade literature.

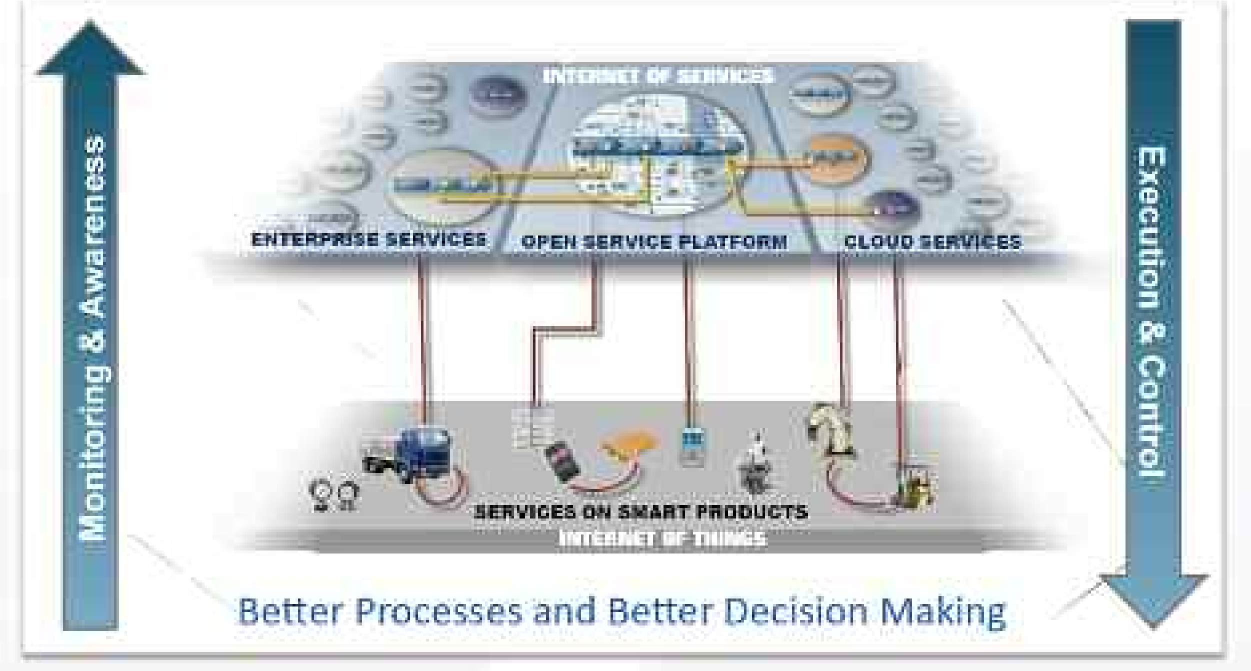
Because definitions can provide a concise, encapsulated description or statement of the nature, scope or meaning of a concept or entity they provide a quick and useful reference point in directing thoughts to such entities. CASAGRAS proposed a definition as a framework for directing the direction and content for its formative work packages. The CERP-IoT group have also been engaged in this definition deriving activity, principally it would seem, to accommodate new developments and outcomes of relevant EU Framework projects. Different definitions can provide different perspectives and lead to a consensus definition that effectively embraces the nature of the subject being defined. It is therefore instructive to consider the definitions presented through CERP-IoT and constructively compare them with that provided through CASAGRAS. In doing so it has to be noted that definitions may be derived to suit different audiences.

1.2.1 The CASAGRAS Definition

The concept of the Internet of Things, as determined within the CASAGRAS project is embraced within the following definition:

A global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and evolving Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterised by a high degree of autonomous data capture, event transfer, network connectivity and interoperability. Reference:
http://www.rfidglobal.eu/userfiles/documents/CASAGRAS26022009.pdf

[15] European Policy Outlook RFID – Working document for the expert conference “RFID: Towards the Internet of Things, June 2007.



1.2.2 SAP Definition

A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes. Services are available to interact with these 'smart objects' over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues.

Reference: http://services.future-internet.eu/images/1/16/A4_Things_Haller.pdf

Introduced through SAP AG this is a definition that aligns with the CASAGRAS definition, but introduces terms and assertions that require further qualification. The reference to ‘smart objects’ requires a definition for smart objects and while the services assertion is both interesting as a vehicle for operating upon objects to effect a change in state it is potentially one of a number of possible service provisions. The reference to physical objects becoming active participants in business processes also requires qualification as physical objects have always been associated with business processes; most businesses, irrespective of their size and function, are invariably involved with physical entities of one kind or another. What is different here is the way in which tagged or otherwise identified objects are integrated into business processes.

This critique of definition can and should be exercised with any definition including those of CASAGRAS (see below). Suitably qualified a better understanding can be derived. Good definitions give such insight without qualification. However, for analytical and development purposes qualification is an essential requirement to understanding. The following two definitions provide a degree of explanation.

1.2.3 ETP EPoSS Definition

Internet of Things is defined as *"the network formed by things/objects having identities, virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate with the users, social and environmental contexts".*

Semantically, "Internet of Things" is defined as *"a world-wide network of uniquely addressable interconnected objects, based on standard communication".* Using this network, smart wireless identifiable devices are able to seamlessly interact and communicate with the environment, thereby helping to make our society more efficient, secure and inclusive.

While the current Internet is a collection of rather uniform devices, heterogeneous however 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.

Under this vision, objects will be able to transport themselves, implement fully automated processes thus optimising 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, they will self dispose at the end of their lifecycle, helping to preserve the environment.

In this context smart wireless identifiable devices (EMID-Electro Magnetic ID: USID-Ultra Sound ID, RFID-Radio Frequency ID, MMID-Millimetre waves ID, etc,) will form the backbone of "the Internet of Things" infrastructure allowing new services and enabling new applications.

The smart wireless identifiable devices will open the door to the fusion of the real, virtual and digital worlds and will create 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. At the same time it will react autonomously to the real world and influence it by running processes that trigger actions, without direct human intervention.

Provided through ETP EPoSS these definitions and supporting explanations provide insight, and given appropriate analysis and comparison in functional and structural terms, can be seen to align with the CASAGRAS definition.

1.2.4 World Internet Definition

The IoT concept was initially based around enabling technologies such as Radio Frequency Identification (RFID) or wireless sensor and actuator networks (WSAN), but nowadays spawns a wide variety of devices with different computing and communication capabilities - generically termed networked embedded devices (NED). While originating from applications such as supply chain management and logistics, IoT now targets multiple domains including automation, energy, e-health etc. More recent ideas have driven the IoT towards an all encompassing vision to integrate the real world into the Internet - The Real World Internet (RWI). RWI and IoT are expected to collaborate with other emerging concepts such as the Internet of Services (IoS) and the building block of parallel efforts, such as the Internet of Energy (IoE) is expected to revolutionise the energy infrastructure by bringing together IoS and IoT/RWI. It is clear that the RWI, will heavily impact the way we interact both in the virtual and physical world, overall contributing to the effort of the Future Internet.

Introduced as a World Internet proposition (IoT in FIA/RWI) it is more a statement than a definition.

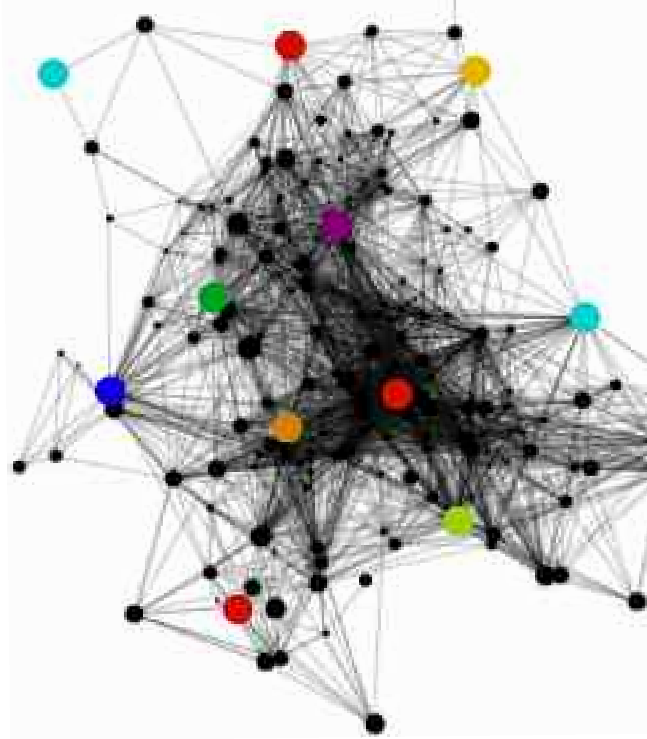
Reference:http://rwi.future internet.eu/images/c/c3/Real_World_Internet_Position_Paper_vFINAL.pdf

<http://rwi.future-internet.eu/images/c/c3/Real_World_Internet_Position_Paper_vFINAL.pdf>

While CERP-IoT has sought consensus of what constitutes a best definition for the Internet of Things it is clear that the basis for comparison is somewhat flawed. However, it does provide some insight into thinking on the subject. There are facets to these definitions and statements that direct attention to the dimensions and issues relating to any attempt to specify an IoT. The CASAGRAS approach has been to consider such propositions and to qualify its own definition with a view to enhancing understanding and establishing a basis for specification.

1.3 Qualifying the CASAGRAS Definition

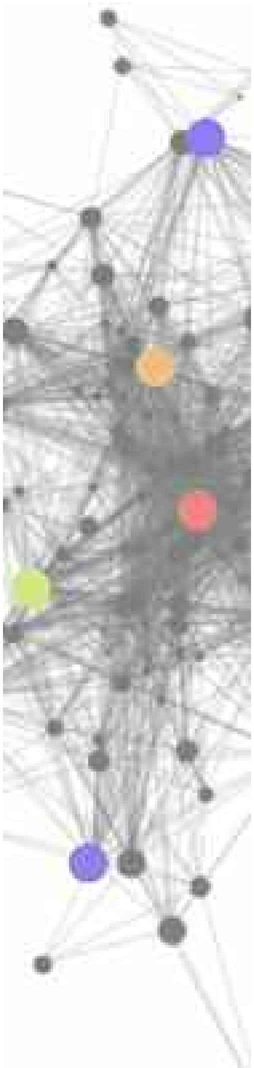
As with many definitions that seek to encapsulate a multi-faceted concept there is a need to qualify what is meant by particular words in order to minimize ambiguity. Where a definition has to serve wide ranging nationalities and language barriers the difficulty of achieving clarity is even more demanding particularly where words are not seen to have any direct counterparts. This is the case with the definition for the Internet of Things. By way of qualification the following component parts of the CASAGRAS definition are explained. For convenience the definition is repeated:



"A global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and evolving Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterised by a high degree of autonomous data capture, event transfer, network connectivity and interoperability."

Wherein the contributory terms are considered to have the following meanings:

"Global network infrastructure" describes what it is. It is a structure that is similar in many ways to that of the global or world-wide Internet itself. It allows messages from communicating devices to be communicated to other communicating devices via a network of computer connections, packets of data comprising the message being sent via routing devices to the final destination and in the right order. The Internet of Things will invariable exploit this Internet infrastructure, at least initially, but with the computer nodes becoming increasingly replaced by autonomous computer functionality facilitated by 'smart devices' or embedded computer-based systems that avoid the need for human intervention yet serve to satisfy human defined needs, be they personal, corporate or otherwise.



"physical objects" refer to any tangible physical entity or thing, be it animate or inanimate, at item or any other level of complexity and able to be characterized in some way for the purposes of type of unique identification.

'Virtual objects" are those objects that are represented in media space and may exhibit a proxy relationship with a physical object. Again the need is seen to assign identity to the object if it is to be accommodated within the Internet of Things.

"data capture" and "autonomous data capture" refers to the process of obtaining data from a particular source and introducing the data into a communication, to a computing, or other data handling system. Increasingly, the data capture process will exploit the advantages of automatic identification and data capture (AIDC) systems with less and less human intervention when implementing applications or services within the Internet of Things.

"specific object-identification" refers to the way in which objects will be identified, either through natural features where this is appropriate or by codes in data carriers such as linear bar codes, two-dimensional codes or radio frequency identification (RFID) tags.

"sensor" or "sensors" refer to a particular category of devices that can sense or measure defined physical, chemical or biological quantities and generate associated quantitative data. This is in contrast to other sensor definitions that are encountered in relation to the Internet of Things in which devices such as RFID readers are considered to sense the data they acquire.

"actuation" and "sensor-actuation networks" (SANs) are often coupled with sensors and the notion of sensing, implying a coupling that features in most control systems. Actuation is therefore a further important aspect for the IoT, not only in respect of sensing but also in respect of particular human-to-object applications in which a device or system has to be activated or operated (such as an access barrier or door).

"connection capability" and "connectivity" both refer to the ability to introduce or interface between a source of data and a device that can carry or handle it. The greater the capability or connectivity the more effectively data can be transferred. Performance factors and criteria will be associated with such capabilities.

"event transfer" refers to a transfer of functionality embedded in the message delivered from source to destination or any other situation or activity relating to an application or service.

"independent cooperative services and applications" refers to services and applications wherein there is an agreement on the part of parties to use a particular infrastructure (albeit constrained by contractual details) to develop their respective applications or services but are free to determine the nature of those services and applications (within the contractual bounds of the infrastructure), and how they manage them.

The latter introduces a further, potentially very significant dimension to object-connected ICT and the practical impact it can have upon businesses and life generally. By defining a suitable, commonly accessible, communications and server support structure for object-based applications, the facility can be provided for independent development of these cooperative services, analogous to, and potentially as expansive as the world wide web (www). By exploiting the potential of new domain structures, such as a world object web (wow.) the service and associated application framework can be considerable enhanced and expanded. The same sort of approach may also be used to accommodate within an Internet-integrated structure the emerging concepts of Internet of Services, people and media.

The CASAGRAS definition has been used as a basis for proposing a fully inclusive model for the Internet of Things, as described in section 2 of the report.

1.4 International Cooperation

Like the Internet, the Internet of Things is a development having significant global implications and requiring global cooperation on the way in which it is realised, maintained and governed. The European commission have already identified the importance of on-going international dialogue on issues concerning the Internet of Things, recognising that "many IoT systems and applications will be borderless by nature and therefore require a sustained international dialogue, notably on matters of architecture, standards and governance." [16] Within its communication COM(2009) 278 the EC declared its intension to intensify the existing platforms for dialogue on all aspects of IoT with its international partners. Notably, current dialogues include cooperation with the US concerning best practices to optimise the economic and social impact of RFID [17] and cooperation with the Japanese Ministry of Economy, Trade and Industry on, among other things, RFID, wireless sensor networks and Internet of Things . [18] CASAGRAS has, through its international team extended cooperation with respect to US and Japan and added further partners with respect to China and Korea.

The international cooperation demands in respect of the IoT are likely to go beyond those of the established Internet. They are extended by the nature of essentially autonomous networked structures that will facilitate interfacing with the physical world, to both collect and deliver data and information, and to facilitate actuation and control in situations where there is no immediate human intervention to provide sentient functionality. On issues concerning standards, regulations, privacy, governance and the practical requirements in respect of the associated enabling technology and infrastructure, the need for international collaborative effort is clearly obvious. In addition to these more obvious areas of cooperation the need may also be seen in areas of cross-border IoT applications, such as networks to counter fraud and counterfeiting. CASAGRAS has sought to clarify the issues of international cooperation and to define a process of on-going cooperation with respect to the IoT.

[16] Commission of the European Communities (2009) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions ; Internet of Things – An action plan for Europe. COM(2009) 278 final.

[17] Commission of the European Communities (2007) Framework for Advancing Transatlantic Economic Integration between the European Union and the United States – ec.europa.eu/enterprise/policies/international/cooperating-governments/usa/transatlantic-economic-council/index_en.htm

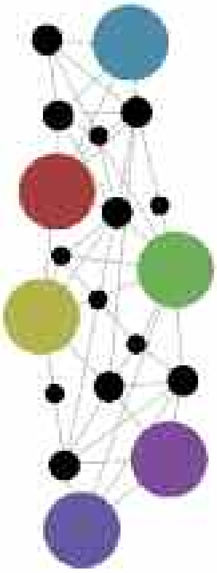
[18] Commission of the European Communities (2009) Memorandum of the Commission signed by the Directorate-General Information Society and Media.

One of the primary issues identified within the CASAGRAS project for international cooperation was the requirement for a global coding approach to identification. This has been viewed as “extremely challenging and extremely unlikely” due to the divergence of communication-based systems, including those for RFID. The challenge for CASAGRAS has been to tackle this issue and in so doing has proposed a resolver approach that can accommodate legacy systems of numbering and identification.

1.5 Motivation for CASAGRAS.

The primary motivation for the CASAGRAS project was routed in the needs of the European Commission to intensify its international dialogue in respect of revolutionary developments such as the Internet of Things which clearly presented global dimensions and the need for international cooperation. The CASAGRAS stakeholders aligned with this need and have been motivated in the task of identifying a model and a strategically acceptable way forward in realising an inclusive model for the Internet of Things. The ensuing activities have revealed the need for wider international cooperation.

The CASAGRAS view of the IoT is based upon a suggested imperative of appropriate cooperative principles that will allow rapid, but effective, growth in services and applications, characterised by enterprise and innovation and providing a significant platform for SME involvement, analogous to that of the world-wide-web.



- The requirements for international cooperation appear to go well beyond those of the established Internet and yet will need to align with cooperative initiatives on the evolving Internet. They are extended by:
- 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

  A ‘no-action’ scenario, that fails to accommodate these international requirements, will impact upon the competitive position of Europe and its standing within an evolving digital world.

CASAGRAS
an EU Framework 7 Project

RFID **Final Report**

and the Inclusive Model for the
Internet of Things

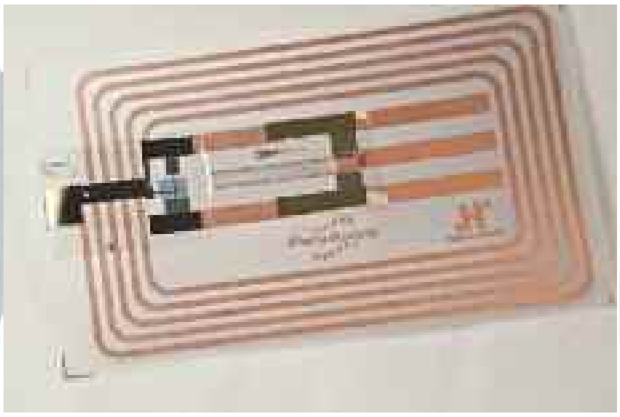
2 The CASAGRAS Framework

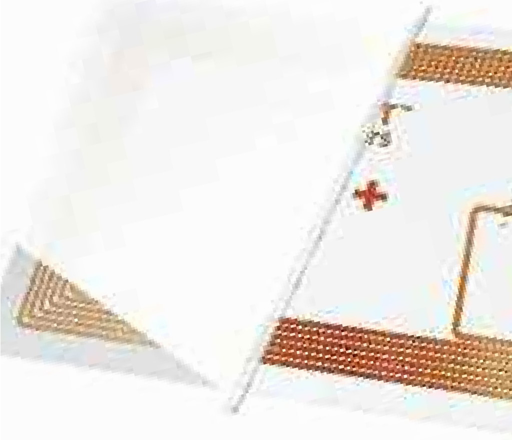
As a Coordination and Support Action for Global RFID-related Activities and Standardisation CASAGRAS has been concerned with providing materials and recommendations that can assist the European Commission in developing its strategy and roadmap for developing an Internet of Things. Introduced amidst other EU projects concerned with radio frequency identification (RFID) and the Internet of Things, the CASAGRAS objective has been to consider the international dimensions with respect to regulations, standardisation and other requirements for realising the Internet of Things and the role within it of RFID. Through appropriate attention to the IoT concept and technological means of interfacing with the physical world the goal was revised to embrace not only RFID, but other technologies for identification, location, communication and data capture.

Three categories of hardware technology and associated layering can be distinguished as a basis for realising an Internet of Things:

- Identification and data capture technologies forming the physical interface layer
- Fixed, mobile, wireless and wired communication technologies, with associated interface support, for data and voice communications
- Network technologies (in combination with communication technologies) to facilitate grouping of supported Objects for application and service purposes

Added to this are the software, middleware components and associated protocols which provide the means of linking and driving the hardware, and service discovery support to constitute a fully operational system or systems. Within the CASAGRAS framework attention has been directed to relevant European policy documents concerning such structures.





One such document, the European Policy Outlook RFID document,[19] proposes embedded processing capability as a useful determinant in specifying models for the Internet of Things. For the purposes of CASAGRAS three models were considered:

1. A model based specifically on read-only RFID data carriers
2. Additional Object Connected data model based specifically on RFID (ostensibly with read-write functionality and added data carrying capability)
3. Additional Object Connected data model based on RFID and other Edge technologies (ostensibly covering sensory data capture, extended data carrying capability and other attributes such as location or positioning facilities)

The most basic model for an Internet of Things has data carriers which are essentially passive RFID tags carrying unique identifiers, with each tag having the capability for interrogation and response via a wireless channel. There is no intrinsic processing capability within the tags and no facility for communications between tags.

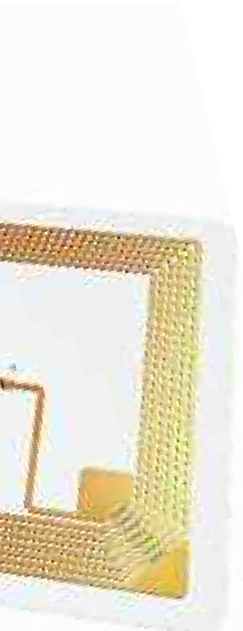
Applications using these data carriers rely upon the identifier as the means of locating remotely stored information about the item to which it is attached. The tags are interrogated using reader, interrogator or gateway devices that have the facility to communicate wirelessly with the tags and further communicate with an application-supporting information management system.

For the purposes of this report, the term Interrogators will generally be used and can also mean reader, base station and gateway.

The interrogators may be fixed or mobile devices. The communication link between the interrogation device and the host may be wired or wireless, depending upon type of device, requiring appropriate interface and communication protocols. The interrogators may perform particular processing functions and have the added facility to communicate with other interrogation or gateway devices and be networked.

It must also be recognised that active RFID devices may perform both the function of a responding tag and, in other circumstances, that of an interrogator to collect/collate data from other RFID devices within its range, and may form local ad-hoc networks. Such capabilities appropriately deployed may greatly enhance the realisation of the IoT.

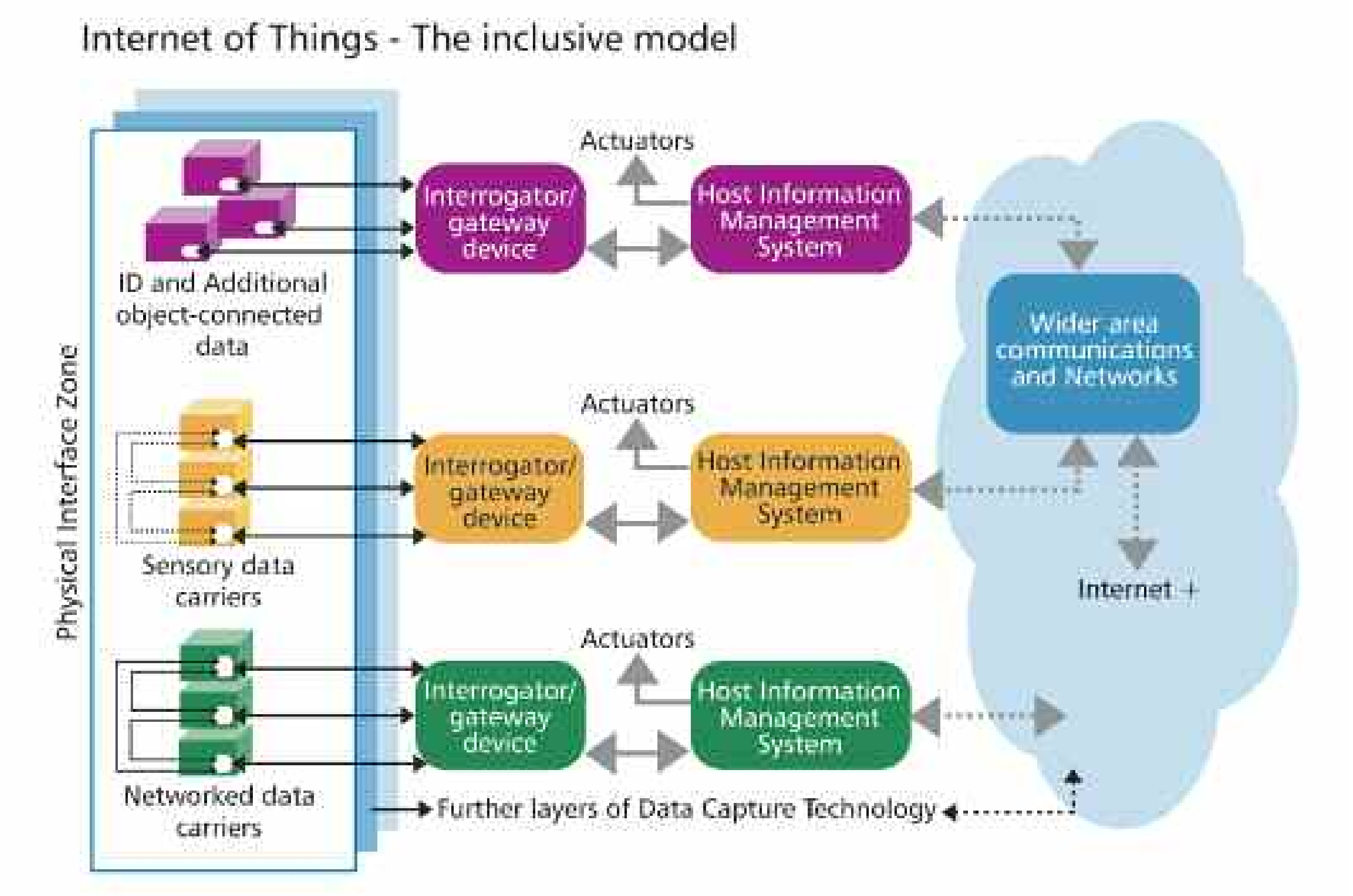
Host systems handle the application needs, exploiting item-numbering schemes to facilitate the item-specific support functions and to derive and communicate appropriate responses, including those that result in physical actuation. The host systems may be connected, again via wired or wireless communication channels, and networked. This further communication and networking capability may include the Internet and World Wide Web, depending upon application requirements. To achieve this degree of communications requires appropriate standardisation of numbering, data structure, communication and interface protocols at a global level if a truly global Internet of Things is to be achieved.



[19] European Policy Outlook RFID

2.1 The CASAGRAS Inclusive Model for the Internet of Things

While models for the Internet of Things have been suggested that are simply based upon RFID and other radio-based edge technologies, a more inclusive model is necessary to accommodate the potential for interfacing with the physical world and the inevitable vagaries in connectivity that are likely to arise in realising practical, scalable systems. While the inclusive model is more demanding in its outlook and realisation it is a vision that can be approached in a staged, standards-supported manner. The framework considerations may be grouped into those that relate to the various layers distinguishable between the real world objects and the integration with the evolving Internet.



Internet of Things - The inclusive model
Physical Interface Zone
ID and Additional object-connected data
Sensory data carriers
Networked data carriers
Actuators
Interrogator/ gateway device
Host Information Management System
Actuators
Interrogator/ gateway device
Host Information Management System
Actuators
Interrogator/ gateway device
Host Information Management System
Wider area communications and Networks
Internet +
Further layers of Data Capture Technology

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

These layers comprise:

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

The European Commission (2006) report, From RFID to the Internet of Things – Pervasive networked systems [20] identifies the following network-supporting communication devices:

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

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

While not explicitly stated the implication is that the technologies (1-4) are essentially RF-based structures if not totally RFID devices.

Layers may be distinguished that relate to different AIDC technologies offering different levels of functionality. They naturally include RFID as a layer, but other layers can extend to the whole range of AIDC technologies, including linear bar codes, two-dimensional codes, optical data recording devices, contact memory devices and a range of natural feature identification technologies including biometrics for personal identification. Also of significance in interfacing with the physical world are the radio-based communication technologies, some of which are object-connected (including WiFi, Bluetooth, Zigbee and near field communication (NFC) and others providing the facility for much wider communications (GPRS, 3G). Broadband and mobile networks, and associated service developments add further dimension and opportunity in realising the edge layers for the Internet of Things.

The range and functional richness of these technologies present a substantial determinant in realising object-connected applications, innovation and enterprise. They are contributory to the applications framework.

On this basis layers can be identified for different data capture devices. Accommodating them within the architecture for the IoT ideally requires the development of a 'plug-and-play' universal data capture appliance protocol (UDCAP). Moreover, in defining the layers in this way a basis is provided for migrating to a fully inclusive accommodation of edge technologies over a period of time.

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

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

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

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

Although interfaces are necessary between each layer, interfacing may also bypass layers, adding still further flexibility and options for object-connected applications and services. Network-based structures, as well as those that require gateway support, also add to the flexibility. Moreover, the developments in ubiquitous computing and networking, with integral communication capability, provide the key technological foundation for the Internet of Things infrastructure and its integration within the existing and evolving Internet.

2.2 Exploiting Edge Technologies - Automatic Identification and Data Capture

Licence-plate data carrier principles, together with a complementary set of principles exploiting data carriers with additional data or information payloads, are prima fascia foundations for the subject of automatic identification and data capture (AIDC). Natural feature identification techniques and technologies, including biometrics and inanimate physical feature identification, adds further dimension to these foundations. The data carrier foundations have, in particular, served as a radical and revolutionary source of beneficially disruptive technology for business process re-engineering and constitute a little recognised but immensely powerful sector of ICT. It is in relation to these foundations that the concept for the Internet of Things emerges and requires appropriate consideration with respect to the potential it provides for integration and functional synergy. However, a further level of traditional exploitation of AIDC technologies requires recognition and that is the use of local area networks for data capture of data or information from object-connected data carriers and the use or dissemination of that data or information in business or industrial processes.

Many inventory, asset and product handling activities can exploit AIDC technologies.Furthermore, developments in radio-based wireless communications, including mobile-phones, have extended the reach and capability of such systems, with global positioning and local location capabilities adding still further to the application potential. Within these systems the objects concerned are rarely connected permanently to a reader or interrogation system and are invariably transferring data for only short periods of time. These features of functionality are also likely to characterise objects connected to the Internet of Things, and constitute formative considerations when issues of scalability are to be resolved.

The AIDC data carrier and transfer principles referred to here constitute an important and continuing legacy. The principles require positioning within main stream ICT and as a foundation for supporting IoT application design methodology. As emerging principles they can be collectively referred to as item-attendant or object-connected ICT and a brief introduction to them is presented in Annex B (A Brief Introduction to Object-connected ICT). Since the Internet of Things is so strongly founded upon objects or things it is logical that these principles should align with and provide a foundation for the IoT.

2.3 Natural Feature Identification in the Internet of Things

Natural feature identification can be seen as a potentially very important category of support technologies with respect to the Internet of things and in application areas where other, data carrier based technologies are being seen to be inappropriate. Broadly speaking the primary categories for natural feature identification technologies comprises animate (biometric-based technologies) and inanimate technologies, the latter embracing emergent physical, chemical and biological techniques for both type and unique identification.

The biometric, personal identification techniques have been evolving for decades, with moderate impact. However, improvements in performance, reductions in the costs of devices and systems, together with integration with data carrier technologies, particularly smart card and contactless smart card, are now positioning biometrics as an important foundation for unique personal identification with a significant role to play in IoT human-interface applications and services. However, during this development, there must be awareness of, and sensitivity to, issues of personal and data privacy to avoid accidental compromise of basic rights, or the stimulation of political objections.

Emergent physical surface-feature identification techniques are also now presenting a powerful platform for object-based applications. One particular area of importance is in solving object-based counterfeit problems and, through appropriate integration, facilitating IoT applications in which national and global nodal services could support anti-counterfeiting measures to combat counterfeiting activities.

2.4 Important Developmental Influences upon the Internet of Things

A number of important developments, in addition to those associated with RFID and mobile communications, are now influencing the form that these layers might take and the applications and services they may support. These developments, which are being seen to have significant potential in areas such air travel development [21] include:

Service Oriented Architecture (SOA)

Collaborative Decision Making (CDM)

Cloud Computing

Web 2 and Semantic Web

Two of these, Cloud computing and Web 2 and Semantic Web, are Internet based and as such constitute considerations in the integration of the Internet of Things with that of the Internet itself.

2.4.1 Service Oriented Architecture

Service Oriented Architecture (SOA) can be viewed as a toolkit for separating functions into distinct unit or services that can be made accessible over a network and used to develop business applications, allowing a library of business functions to be created as software modules that can be reused or drawn upon to develop new applications or services. The flexibility that this provides yields faster development times, easier integration and the addition of functionality on the fly rather than through time-consuming software coding.

SOA further allows services to communicate with each other, by passing data from one service to another, and to co-ordinate activities between one or more services. It also allows software on demand, allowing a host to automatically deliver software modules in response to requests.

[21] SITA (2008), The Airport IT Trends Survey 2008./ SITA (2009) New Frontiers Paper, “Ten Technology Advances that will change air travel”.

This software module and bus capability offers considerable potential for developing applications and services with the Internet of Things. SOA can also be combined with Software-as-a-Service applications, a capability that paves the way for highly scalable architectures.

The SOA concept assumes discrete transactional processes within its application provisioning and as such presents a challenge in integrating event-driven processes. It has been estimated that "SOA will be used in more than 50% of new mission-critical operational applications and business processes in 2007 and more than 80% by 2010" .[22]

2.4.2 Collaborative Decision Making (CDM)

It is generally accepted that the Internet of Things will generate vast amounts of data and associated information, much of which will be needed in decision support situations. While intelligent processing systems may seek to achieve decision-making and predictive analyses in automated ways, situations will also be distinguished in which information will invariably need to be shared and presented to support human decision making. Collaborative Decision Making (CDM) is an approach that facilitates decision-making functions by providing timely and accurate information essential for operational planning. It also provides the facility for predictive analysis in the event of unforeseen circumstances or disruption in operations and processes. This can be seen to be of vital importance in industries, such as the Airlines, which incorporate expensive buffers into their scheduling to absorb the consequences of unforeseen circumstances. In such situations savings in minutes can translate into savings in millions of Euros per annum in better use of resources. An essential and significant feature of CDM-defined rules is information exchange and to the extent that it can handle time-critical business support processes.

CDM is both a tool and concept that could be effectively exploited in service and application offerings within the Internet of Things, particularly where the need is seen for improved decision making and predictability, optimisation of resources, improved productivity and reduction in costs.

As an example of its potential it is estimated that "within the next three to five years around half of airports will have made some investment in CDM tools" [23]

2.4.3 Cloud Computing

Cloud computing is a term that is used to describe services in which elements of a company's computer needs, such as software, processing power and data storage, are provided through the Internet. Through improvements in Internet infrastructure cloud computing builds upon earlier type services characterised by utility computing, software-as-service and application service providers, and provides the feasibility for fully running applications over the Internet. Through its browser based access facility it also offers the flexibility of access through mobile platforms and at different sites, including the capability of servicing and synchronising services at defined sites and kiosk-type facilities. The mobility advantage offers significant potential for wireless-based integration and the delivery of wireless-based applications and services.

[22] Gartner (2007), Press release – "Gartner says SOA will be used in more than 50 percent on new mission-critical operational applications and business processes designed in 2007" (25-04-2007).

[23] SITA (2008), The Airport IT Trends Survey 2008./ SITA (2009) New Frontiers Paper, "Ten Technology Advances that will change air travel"

While offering considerable potential and efficiency in the provision of computing support, connectivity and security issues present a degree of inhibition in its take-up. Because loss of connectivity or service continuity may be a critical issue in some applications it is necessary in these circumstances to have adequate backup provision and cashing capability.

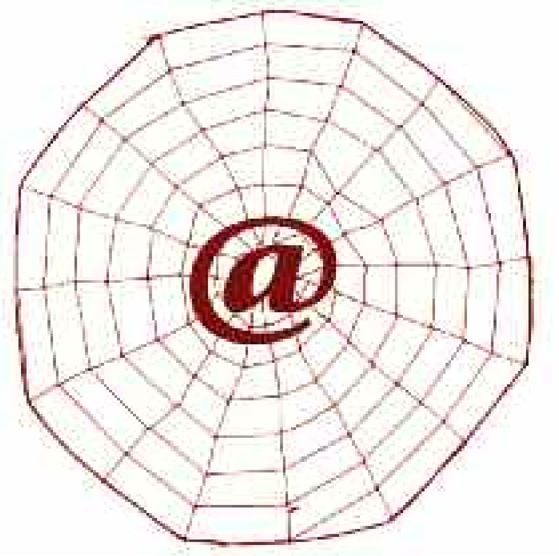
Similarly, in considering security issues the remote handling of data and tasks requires appropriate safeguards in respect of both privacy and security to provide the necessary assurance in using such schemes.

Despite these limitations, the key features of cloud computing, including lower capital costs, mobility and global capability for access, ease of deployment, flexibility and scalability and reduced infrastructure, offer significant benefits.

With respect to the Internet of Things and its integration within the evolving Internet cloud computing can be seen as an integral feature. Because of inherent wastage in distributed computing systems, it has been estimated (McKinsey & Co.) that 80% of such demand is characterised by between 5% and 30% utilisation. Cloud computing can be seen as a powerful alternative.

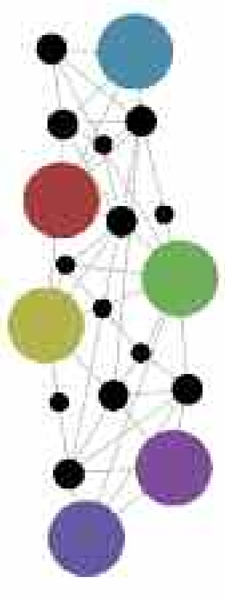
2.4.4 Web 2 and Semantic Web

Although the Web 2 developments are largely about people-generated content it can be seen to have relevance to the Internet of Things in respect of the objects, virtual and real, to which personal content may relate. Given this perspective it becomes an integral part in the integration of the Internet of Things with that of the evolving Internet. Within the sectors for travel and leisure, for example, such integration could offer opportunities for service development that are able to yield significant benefits in terms of quality of service and personalisation. It also provides significant capability for 'mashups' in which application programmable interfaces (APIs) are used to combine data and functionality openly from different sources.



The second of these developments, the Semantic Web, also offers potential for the Internet of Things, exploiting the semantic capability of machines, as well as humans, to basically understand information delivered through the Web. With its meta-data foundations for empowering applications to discover, understand and utilise even unfamiliar data or services it can provide a powerful capability for functionality and services within the Internet of Things.

It is developments such as these that will provide on-going impact upon the structure and functionality of the IoT making it a dynamic, evolutionary entity analogous to the Internet itself.



2.6 Migration to an Inclusive Model for the Internet of Things

The complexities involved in realising a fully inclusive model for the Internet of Things are clearly daunting, and extended by the need for international cooperation. However, the prospect can be seen for a progressive and systematic migration to, or at least towards, a fully inclusive structure for the IoT based upon a strategic roadmap for development.

This strategic, internationally supported, roadmap would take as its guiding principle the layered approach presented in the CASAGRAS inclusive model, starting with a minimalist generic framework and adding to this framework the layers of edge support technology, supported by an appropriate universal data capture appliance protocol, a resolver-based coding support system and a service oriented network and interfacing support structures.

The roadmap would further allow for the integration and support of legacy identification systems, discovery services in relation to independent developments such as those advanced through EPCglobal, appropriate consideration and accommodation of socio-economic factors, such as privacy and security, and developments in applicable technology.

CASAGRAS
an EU Framework 7 Project

RFID Final Report

and the Inclusive Model for the
Internet of Things

3 CASAGRAS Findings

As a coordination and support action initiative CASAGRAS has gone beyond its initial remit of looking at radio frequency identification (RFID) in relation to the emerging concept of the Internet of Things and the international dimensions for achieving a global infrastructure. CASAGRAS has proposed an inclusive model for the IoT that embraces a range of other identification and object-connected technologies to allow effective interfacing between the physical and virtual networked-based worlds.

What follows is a resume of findings arising from this extended view of the IoT. It has to be remembered that CASAGRAS was not a research project and consequently does not distinguish the depth to which a research initiative would go to in seeking to realise a concept. The project has sought to identify a framework and a range of technological opportunities for realising such a network, together with appropriate commentary on the technological, social and economic issues relating to its realisation, and in the context of international regulatory, standards and operational thinking.

The framework is that of the inclusive model, described in section 2.1, which distinguishes a number of physical layers relating to different technological platforms for identification and data transfer, together with various layers distinguishable between the real world objects and the integration with the evolving Internet. What follows relates in more detail to these various layers and associated issues, together with a propositional basis for an applications and services framework that can be considered representative of an IoT. In these respects attention has been directed at:

- Interfacing with the physical world
- Communications and Networking
- Use of Identifiers to link with the IoT
- Realisation of the IoT with regulations using standards
- Standards and Regulations
- Applications and services framework

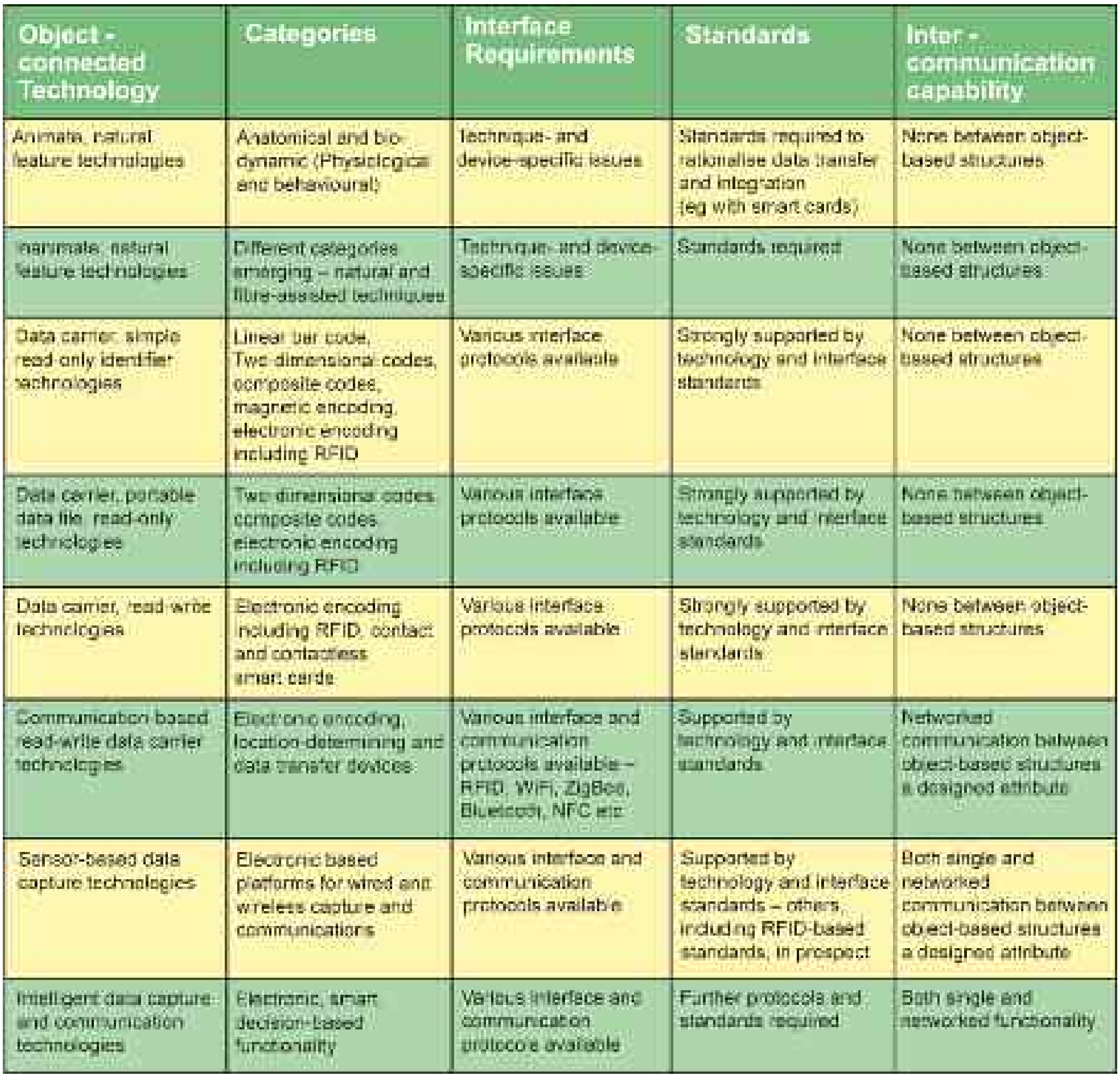
Finally attention is directed at Governance.

3.1 Interfacing with the Physical World

Irrespective of the wide ranging definitions for the Internet of Things one inescapable requirement for the IoT is to interface with the physical world, and that requires appropriate levels of identification. Within CASAGRAS an ontology for object identification (see Annex C) has been derived and distinguishes the basis on which objects, inanimate, animate and virtual can be automatically identified and engage in an interfacing function. That interfacing function may relate to information or data transfer to a host and/or transfer from a host to an object-supported platform for functional purposes, including actuation of some kind. The manner and level of interfacing is dependent upon the application requirements and the technological platforms available and suitable for satisfying the application concerned. The inclusive model is focused upon exploiting existing and emergent object-connectable technologies, but with a strategy for inclusion that is systematic and well-founded upon appropriate standards and protocols.

3.1.1 Object-connected technologies

While a lot of attention has been focused upon objects 'talking to one another' within an IoT the immediate reality is that an IoT, will involve a lot of objects that are simply identifiable as single entities or in groups of entities within application scenarios and without any direct connection with each other. The object-to-object communication and intelligent functionality will, at least initially, be the exception rather than the rule, even with RFID-based technology. With humans identified as animate objects within an IoT concept it is clear that there will be categories of linkage and functionality involving human-to-human communication (through attached or accompanying devices), human-to-object and object-to-human communications, as well as object-to-object communications. Each category will have its own issues concerning privacy, security, reliability and performance; and each will have requirements in respect of standards, regulations and governance. Within this structure there are also requirements concerning interfacing, and interfacing relating to different object-supported platforms and data transfer devices. The following table summarises these platforms and their interface requirements. In all cases an international standard will be required if not already in place.



Object - connected Technology	Categories	Interface Requirements	Standards	Inter - communication capability
Animate, natural feature technologies	Anatomical and bio-dynamic (Physiological and behavioural)	Technique- and device-specific issues	Standards required to rationalise data transfer and integration (eg with smart cards)	None between object-based structures
Inanimate, natural feature technologies	Different categories emerging – natural and fibre-assisted techniques	Technique- and device-specific issues	Standards required	None between object-based structures
Data carrier, simple read-only identifier technologies	Linear bar code, Two-dimensional codes, composite codes, magnetic encoding, electronic encoding including RFID	Various interface protocols available	Strongly supported by technology and interface standards	None between object-based structures
Data carrier, portable data file, read-only technologies	Two-dimensional codes composite codes electronic encoding including RFID	Various interface protocols available	Strongly supported by technology and interface standards	None between object-based structures
Data carrier, read-write technologies	Electronic encoding including RFID, contact and contactless smart cards	Various interface protocols available	Strongly supported by technology and interface standards	None between object-based structures
Communication based read-write data carrier technologies	Electronic encoding, location-determining and data transfer devices	Various interface and communication protocols available – RFID, WiFi, ZigBee, Bluetooth, NFC etc	Supported by technology and interface standards	Networked communication between object-based structures a designed attribute
Sensor-based data capture technologies	Electronic based platforms for wired and wireless capture and communications	Various interface and communication protocols available	Supported by technology and interface standards – others, including RFID-based standards, in prospect	Both single and networked communication between object-based structures a designed attribute
Intelligent data capture and communication technologies	Electronic, smart decision-based functionality	Various interface and communication protocols available	Further protocols and standards required	Both single and networked functionality

Additionally, as part of an inclusive edge-technology model, other object-connectable technologies can be identified as potentially useful in certain IoT applications, including global positioning and various local communication technologies.

3.1.2 Inter-communications capability

As far as the inter-communications (object talking to object) capability is concerned, the technology landscape is somewhat restricted to electronically-based, read-write object-connected devices. However, it is important to note that the interrogator/ gateway devices used to interface with objects can incorporate communication and networking capabilities thus allowing object-groups to be distinguished in applications even though they are not connected at the object level.

As more and more processing and communication capabilities are engineered into object-connected devices, the balance in usage of the different identifier technologies and structures will change. Size, format, embedding capability, power provision, functionality and cost will factor in such changes.

From an interface standpoint the need for a universal data capture appliance protocol (UDCAP) to facilitate plug-and-play capability has been identified. This may prove to be very important. Such a protocol requires attention to identifiers, data structure (source encoding and meta data) and data transfer considerations. Consequently, an approach based upon an initial, selective technology strategy geared towards achieving increasingly intelligent capability would appear to be the sensible route to take, progressively introducing more technologies and devices to support progressive needs. This to some extent aligns with the concept of Real World Awareness (RWA), the essence of which is “the automated collection of real-time data from the physical world via an array of intelligent, connected sensors, and then parsing the data into information and filtering it in useful and beneficial ways”[1].

One of the particular attributes considered in this approach is to “be able to collect data without human intervention or errors and use it to react to events more quickly and effectively” – a principle that has been part of the very foundation for the automatic identification and data capture (AIDC) industry for decades. However, it is an important and sustaining principle and one that is also associated with other developments towards a Real World Internet (RWI)[2]. Within the RWI concept and proposed architecture there is particular reference to sensor and actuator networks (SANs), as well as to RFID. This also ties into the concepts of 'uCity' being developed in Korea and Japan. Even with these technology-selective models there are many architectural and operational issues that require attention.

With the emphasis upon automated systems and absence of human intervention there are needs in terms of network functionality that go beyond those associated with the Internet. Self-monitoring, self-diagnosis and even repair are representative of such needs, together with enhanced levels of security, quality of service, protection against attack, and the important requirement to protect privacy where autonomic data transfer occur that may relate to personal information. Added to this are other dimensions of architectural structure and functionality that will have to be addressed.

[1] Heuser, L., Alsdorf, C & Woods, D (2006) International Research Forum 2006, Evolved Technologist Press.

[2] Gluhak, A et al., (2009), Towards an architecture for a Real World Internet, Towards the Future Internet – A European Research Perspective, IOS Press 2009.

Given that “the RWI will provide an infrastructure that enables augmentation of and interaction with the physical world, without human intervention”, it is a conceptual model in which the overall architecture separates into a real world resource layer and an underlying communication service layer, the latter forming the connectivity link with the existing and future Internet. It is representative of prospective architectures for realising the IoT and illustrative of the extent to which a dedicated architecture is being pursued.

As the consequence of the real world implementation proposed in the CASAGRAS inclusive model incorporates a large diversity of real world information sources and interaction capabilities, a 'resolver identification engine' is proposed that supports architecture for co-operative services and applications. Moreover, the CASAGRAS model also proposes the need for underpinning principles for defining the ways in which identifiers and data can be carried and exchanged to fulfil a wide range of application needs (see Annex B – An Introduction to object-connected ICT).

3.1.3 Interfacing with Enterprise systems

While it is necessary to interface with the physical world, it is clearly a requirement within an IoT model to interface with appropriate structures within an enterprise environment. These considerations are exemplified in the growing set of standards for RFID (see following section). Added to interfacing requirements associated with specific AIDC technologies is the implicit requirement to integrate with the evolving Internet. This in turn points to the need for accommodating web-based services, which by their very nature need to support a wide range of functionalities. To accommodate this level of complexity requires a common architecture. One such approach is through Service -Oriented Architecture.

Web Services (WS) are usually deployed in a heterogeneous circumstance, using different hardware, different operating systems (OS), middleware, or development languages. This therefore creates a challenge in order to realize system coordination across the organizations in a way that is flexible, quick, and at reasonable cost. The use of WS technology can significantly simplify and reduce the cost of Internet-based service provision, which may well affect the level and speed of take up of use of IoT services.

W3C, an international body developing and promoting WS and SOA, defines WS as follows:

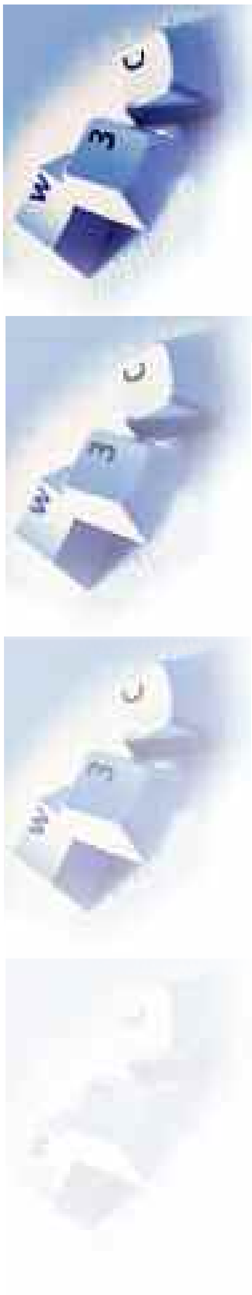
"A web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL{WS Description Language}). Other systems interact with the web service in a manner prescribed by its description using SOAP-messages, typically conveyed using HTTP with an XML serialization in conjunction with other web-related standards."

WS require quite a lot of functionalities, and as a result architecture is indispensable. WS standardization organizations construct standards by "Service-Oriented Architecture" (SOA). SOA is an evolutional form of distributed computing and object orientation.

The World Wide Web Consortium (W3C) develops interoperable technologies (specifications, guidelines, software, and tools) to lead the Web to its full potential. W3C is a forum for information, commerce, communication, and collective understanding.

OASIS (Organization for the Advancement of Structured Information Standards), another international body developing and promoting WS and SOA, is a not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society. The consortium produces Web services standards along with standards for security, e-business, and standardization efforts in the public sector and for application-specific markets.

Their deliverables, relevant to IoT and the use of WS / SOA include:



W3C, Extensible Markup Language (XML) 1.0 (Third Edition) (04 February 2004)

W3C, Namespaces in XML (14-January-1999)

W3C, XML Schema Part 1: Datatypes (02 May 2001)

W3C, XML Schema Part 2: Datatypes (02 May 2001)

W3C, Note, web services Description Language (WSDL) 1.1 (15 March 2001)

W3C, Web Services Description Language (WSDL) Version 2.0: Core Language and schema (26 June 2007)

W3C, Web Services Description Language (WSDL) Version 2.0: Adjuncts and SOAP 1.2 binding schema, HTTP binding schema (26 June 2007)

W3C, Simple Object Access Protocol (SOAP) 1.1 W3C Note (08 May 2000)

W3C, SOAP Version 1.2 Part 1: Messaging Framwork (Second Edition) (24 June 2003)

W3C, SOAP Version 1.2 Part 2: Adjuncts (Second Edition) (24 June 2003)

W3C, Web Services Policy 1.5 – Framework (04 September 2007)

W3C, Web Services Policy – Attachment (04 September 2007)

W3C, XML Path Language (XPath) Version 1.0 (16 November 1999)

W3C, XPointer Framework (25 March 2003)

W3C, Web Services Addressing 1.0 –Core (09 September 2006)

W3C, Web Services Addressing 1.0 – SOAP Binding (09 June 2006)

W3C, Web Services Addressing 1.0 – Metadata (04 September 2007)

W3C, MTOM Serialization Policy Assersion 1.1 (18 September 2007)

OASIS, WS-SecurityPolicy 1.2 (1 July 2007)

OASIS, Web Services Reliable Messaging Policy Assersion (WS-RM Policy) Version 1.1, 07 January 2008

OASIS, UDDI Version 3.0.2, UDDI Spec Technical Committee Draft, Dated 20041019

Web services Interoperability Organization, Basic Profile Version 1.1 Final Material (2004-08-24)

Service-Oriented Architecture (SOA) is a software architecture in which functionality is grouped around business processes and packaged as interoperable services. SOA also describes an information technology infrastructure which enables different applications to exchange data with each other with a view to enhancing business processes.

SOA is designed to separate functions into distinct services or service components, which are made accessible over a network in order that they can be combined and reused in the production of business applications.

These services communicate with each other by passing data from one service to another, or by co-ordinating an activity between two or more services.

This SOA software-data-bus facility can thus be seen as a significant facilitator in the provision of not only web-services but also services within the context of an IoT concept.

In applying SOA based standards the following business-related benefits can be expected:

- Increased service value
- Internationalization
- Expansion of business automation

From a system development viewpoint the benefits can be seen to reside in:

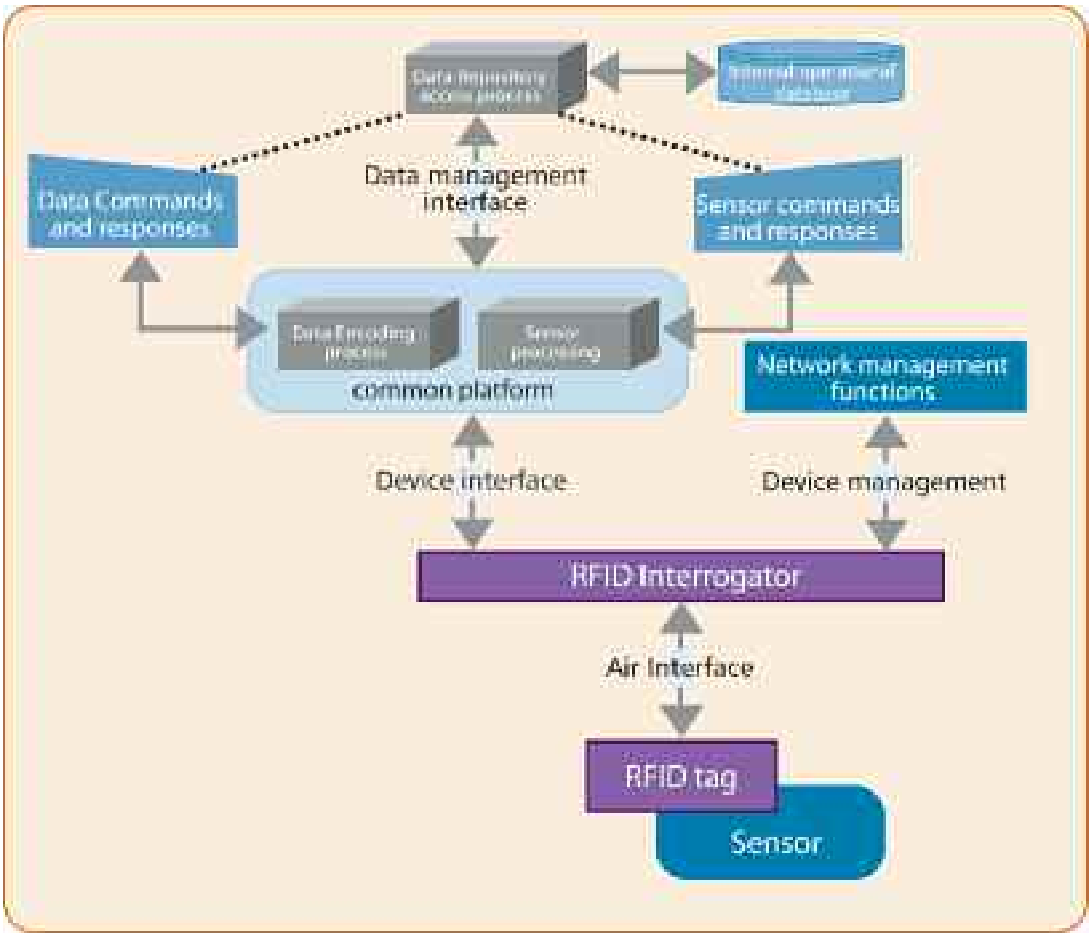
- Easy and rapid development of service co-ordination and service area expansion
- Quick and easy system software development ;
- Service standards based on SOA with a composable structure, and so promoting reusability of software
- Easy connection to legacy systems

Given these attributes SOA can be seen as an important structure feature in developing an IoT.

3.1.4 RFID role in the interfacing with the physical world

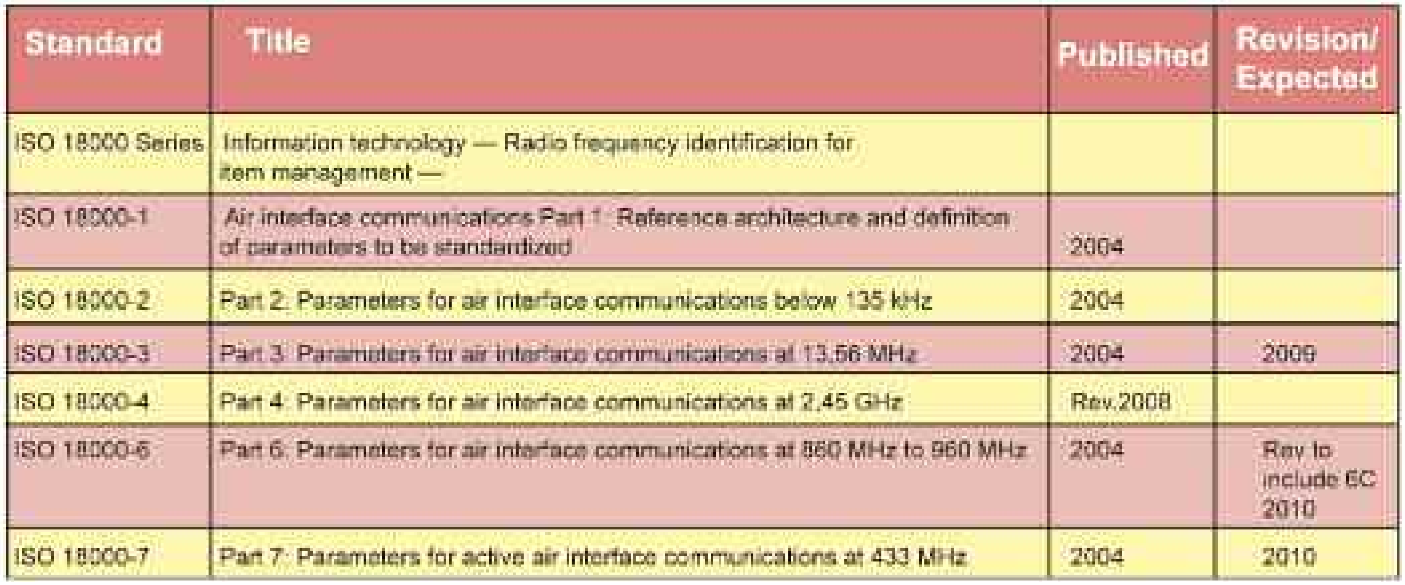
In view of the obvious complexity associated with a fully inclusive model, and even models based upon more selective technologies, a migration strategy to achieve a target structure is a sensible consideration. Applied to interface edge technologies a reasonable starting point for architectural development is to consider the role of RFID, the various interface requirements relating to an enterprise solution and the associated standards. The basic architectural framework for considering these standards is presented below.

Basic RFID Device and Process Architecture



Data Repository access process
Internal operational database
Data Commands and responses
Data management interface
Sensor commands and responses
Data Encoding process
Sensor processing
common platform
Network management functions
Device interface
Device management
RFID Interrogator
Air Interface
RFID tag
Sensor

The IoT will require things or items to be identified. The ISO/ IEC SC31 WG4 RFID for Item Management Committee has the responsibility to develop relevant standards. There are other standards for RFID for animals, but here we focus on inanimate items. The main air interface standards are shown in the table.



Standard	Title	Published	Revision/ Expected
ISO 18000 Series	Information technology — Radio frequency identification for item management —		
ISO 18000-1	Air interface communications Part 1: Reference architecture and definition of parameters to be standardized	2004	
ISO 18000-2	Part 2: Parameters for air interface communications below 135 kHz	2004	
ISO 18000-3	Part 3: Parameters for air interface communications at 13.56 MHz	2004	2009
ISO 18000-4	Part 4: Parameters for air interface communications at 2.45 GHz	Rev.2008	
ISO 18000-6	Part 6: Parameters for air interface communications at 860 MHz to 960 MHz	2004	Rev to include 6C 2010
ISO 18000-7	Part 7: Parameters for active air interface communications at 433 MHz	2004	2010

To effectively encompass the open-systems role for RFID it is important to have a set of standards that cover the identifier, interface (air interface and device interfaces) and the data encoding and transfer requirements. This becomes increasingly important as systems are networked.

Currently, for data interface, transfer and management purposes, the standards comprise two types:

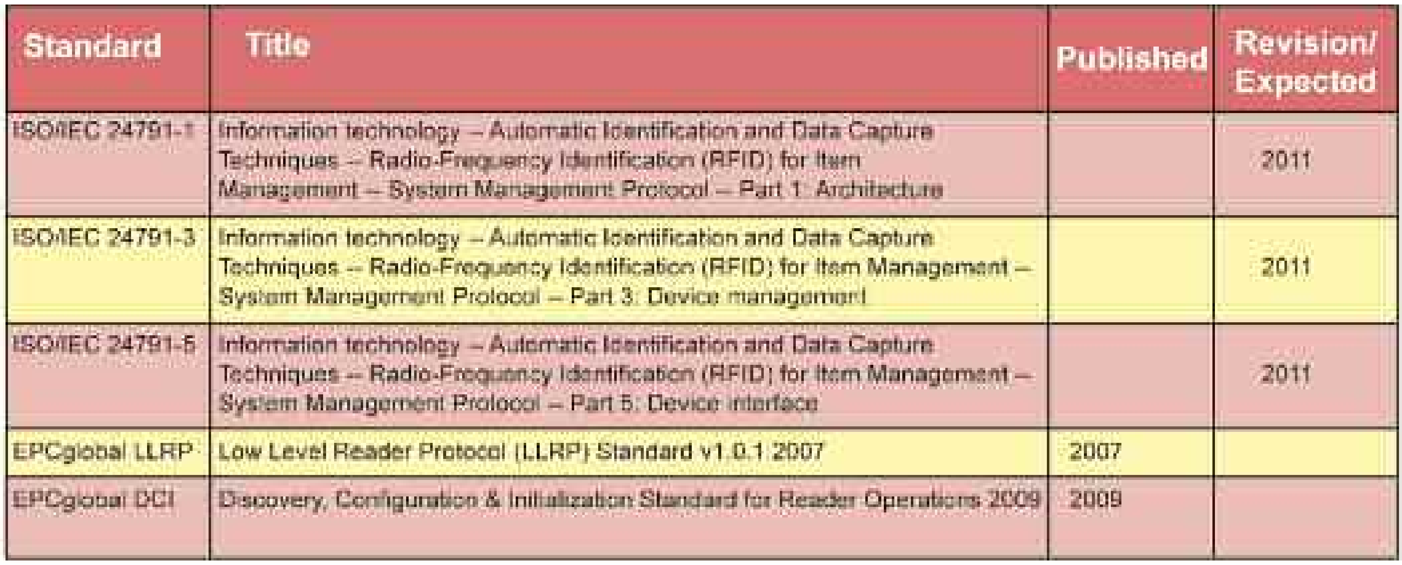
- Device interface standards that provide instructions to the interrogator to transfer data between the application and the interrogator. All of this has to be specific to a particular air interface protocol so that the interrogator can convert the messages into an appropriate form and generate commands for communication via the air interface. A similar process is required to generate a message structure for communication with the system component that is handling the application.
- Device management standards are more concerned with initialisation, monitoring and control of all the RFID devices within a network.

Until recently these aspects of systems infrastructure were invariably accommodated through proprietary solutions. The standardisation effort in this respect is currently focussed on the ISO 18000 series of standards, developed by ISO/JTC1 SC31, to provide standards for air interfaces at a number of carrier frequencies (125-134 KHz, 13.56 MHz, 868 MHz, 2.45 GHz).

This standards work was initiated by IEAN.UCC with the active involvement of Intermec and Texas Instruments and leading AIDC consultants. EPCglobal has subsequently taken the initiative to extend ISO 18000-6 to include the supply chain focussed 18000-6Cfor its UHF Class 1 Gen 2 protocol; and this has been extended by ISO to cover non-EPC functional requirements for the ISO/IEC 18000-6 Type C protocol.

As a consequence of EPCglobal's legacy work the EPCglobal standards associated with these interface and data management functions have been published and have been implemented by a number of solution providers, the approach showing acceptability within the vendor community.

The most relevant data device interface and management standards, other than those covered by the ISO/IEC 18000 series air interface standards, are considered to be those depicted in the table of standards presented here:



Standard	Title	Published	Revision/ Expected
ISO/IEC 24791-1	Information technology – Automatic Identification and Data Capture Techniques – Radio-Frequency Identification (RFID) for Item Management – System Management Protocol – Part 1: Architecture		2011
ISO/IEC 24791-3	Information technology – Automatic Identification and Data Capture Techniques – Radio-Frequency Identification (RFID) for Item Management – System Management Protocol – Part 3: Device management		2011
ISO/IEC 24791-5	Information technology – Automatic Identification and Data Capture Techniques – Radio-Frequency Identification (RFID) for Item Management – System Management Protocol – Part 5: Device interface		2011
EPCglobal LLRP	Low Level Reader Protocol (LLRP) Standard v1.0.1 2007	2007	
EPCglobal DCI	Discovery, Configuration & Initialization Standard for Reader Operations 2009	2009	

While at present these standards relate to only one air interface protocol (ISO 18000-6) it is fully expected that the functionality will be extended to cover the EPCglobal HF Class 1 Gen 2 (and ISO/IEC 18000-3 Mode 3) protocol within the foreseeable future. In fact, device interface standards might be developed closely in parallel to the ISO development for the air interface protocol standards. Without these developments there is a risk of an ongoing proliferation of proprietary solutions with consequential impact upon interoperability and realisation of inter-connecting networks. For long-established protocols, where proprietary interface solutions are already in place, there is a need to explore whether developing an XML interface has any merits in achieving a standardised approach.

Clearly, there is a continuing opportunity to develop device interface and device management standards to satisfy new air interface protocols as they are introduced. Unfortunately, this has not happened as yet with respect to the new ISO/IEC 18000-6 TOTAL (Tag Only Talks After Listening) standard. Such a development would most certainly help to promote and support the implementation of this technology.

With respect to device management standards there is a different type of challenge. These standards are still in the development stage with both EPCglobal and ISO considering differing approaches. The EPCglobal approach is based upon a new, and as yet to be ratified, IETF standard for Control and Provisioning of Wireless Access Points (CAPWAP). Within the ISO community there has been a strong lobby to consider using Web Services to provide an XML-based means of communication for device management. After some significant level of debate ISO have agreed to support the two communications options.

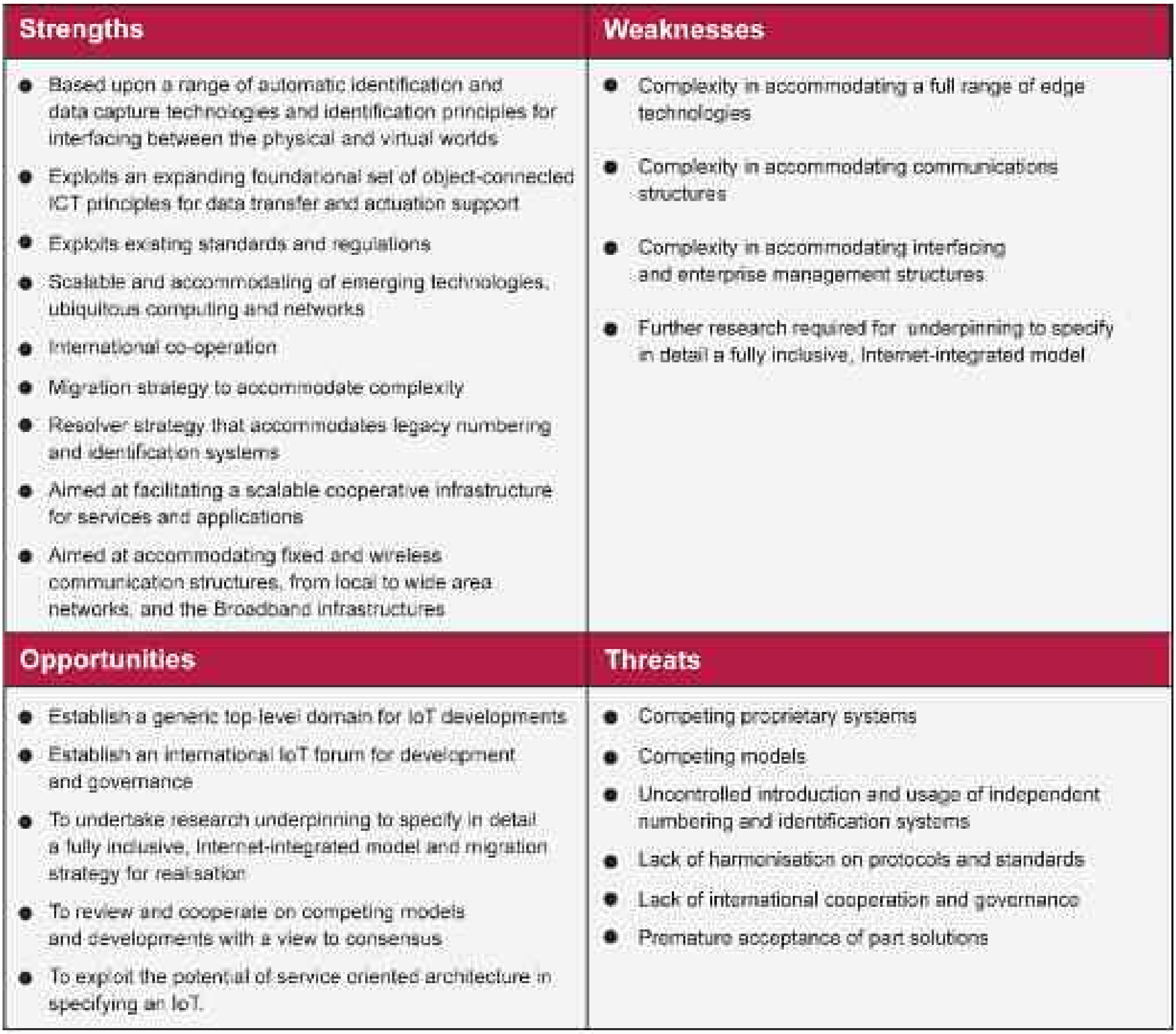
Actuation and control are essential features of many applications involving RFID and while the device management standards are clearly directed at the control of RFID interrogators it is far from clear whether any detailed consideration has been given to the control of other devices. It has been suggested that these standards can support other types of device. However, it is uncertain as to whether detailed analyses of requirements for other types of device have been taken into account, and whether the present methods of controlling such devices (e.g. a network of bar code readers) have been taken into consideration.

There is a need to explore the prospect of developing standards that can support new types of devices based upon common communication architectures. In moving towards a fully inclusive model for the Internet of Things, in which a range of edge technologies will be accommodated, the needs for such standards are intensified.

In distinguishing the inclusive model, or indeed any model that specifies various layers of architecture to support applications and services, the need can be seen for associated levels of identification, over and above object identification – user, service, addressing identification, for example, and, where Internet integration is concerned, specific Internet identifiers.

3.1.5 SWOT Analysis - Interfacing with the Physical World

Here and throughout the report SWOT analyses are presented to provide a concise summary of the identified strengths, weaknesses, opportunities and threats (SWOT) with respect to a particular issues or set of issues. They are intended to encourage further thoughts and considerations within these dimensions. This section deals with those SWOT features concerning interfacing with the physical world.

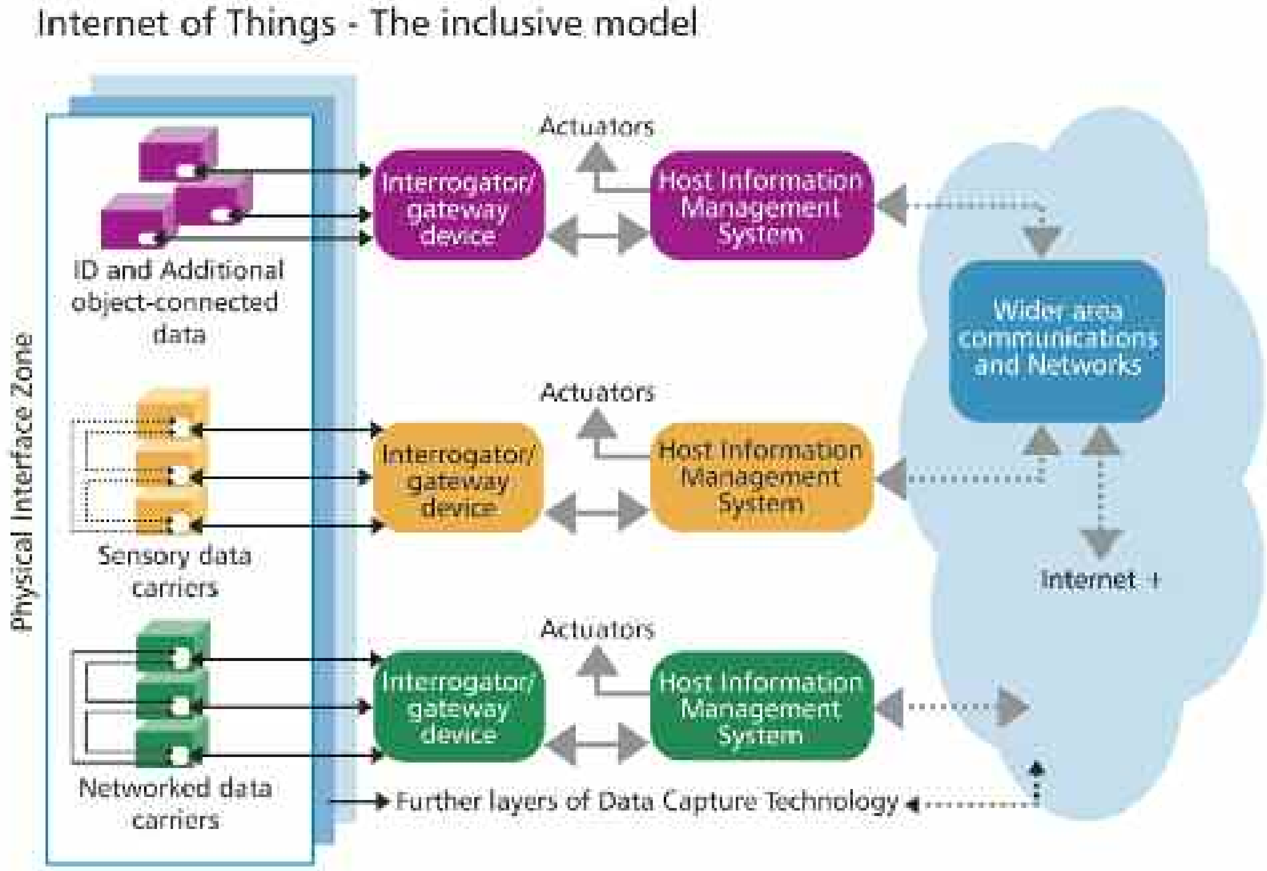


Strengths	Weaknesses
● Based upon a range of automatic identification and data capture technologies and identification principles for interfacing between the physical and virtual worlds ● Exploits an expanding foundational set of object-connected ICT principles for data transfer and actuation support ● Exploits existing standards and regulations ● Scalable and accommodating of emerging technologies, ubiquitous computing and networks ● International co-operation ● Migration strategy to accommodate complexity ● Resolver strategy that accommodates legacy numbering and identification systems ● Aimed at facilitating a scalable cooperative infrastructure for services and applications ● Aimed at accommodating fixed and wireless communication structures, from local to wide area networks, and the Broadband infrastructures	● Complexity in accommodating a full range of edge technologies ● Complexity in accommodating communications structures ● Complexity in accommodating interfacing and enterprise management structures ● Further research required for underpinning to specify in detail a fully inclusive, Internet-integrated model
Opportunities	**Threats**
● Establish a generic top-level domain for IoT developments ● Establish an international IoT forum for development and governance ● To undertake research underpinning to specify in detail a fully inclusive, Internet-integrated model and migration strategy for realisation ● To review and cooperate on competing models and developments with a view to consensus ● To exploit the potential of service oriented architecture in specifying an IoT.	● Competing proprietary systems ● Competing models ● Uncontrolled introduction and usage of independent numbering and identification systems ● Lack of harmonisation on protocols and standards ● Lack of international cooperation and governance ● Premature acceptance of part solutions

3.3 Communications and Networking

The “Internet of Things” may in many respects be viewed as a global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. So communications and networking are kernel to the concept and while it is often suggested that everything from our ordinary life, such as yogurt or toothbrushes, will be connected to such a structure the reality may be quite different, with more realistic and responsible use of connectivity and infrastructure being essential.

While the CASAGRAS inclusive model, introduced in section 2.1 as the reference framework for the CASAGRAS considerations, is more demanding in its outlook and realisation than a number of the restricted technology proposals, it is a vision that can be approached in a staged, standards-supported manner. The framework considerations may be grouped into those that relate to the various layers distinguishable between the real world objects and the integration with the evolving Internet.


Internet of Things - The inclusive model
Physical Interface Zone
ID and Additional object-connected data
Sensory data carriers
Networked data carriers
Actuators
Interrogator/ gateway device
Host Information Management System
Actuators
Interrogator/ gateway device
Host Information Management System
Actuators
Interrogator/ gateway device
Host Information Management System
Wider area communications and Networks
Internet +
Further layers of Data Capture Technology

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

A wide range of communications and networking developments present a foundational set of architectural components essential to the realisation of an inclusive IoT, but requiring a controlled and effective, globally-responsible approach to network development for interfacing with and exploiting connection with the physical world. In approaching this myriad of evolving resources it is important to respond to the range and complexity in a systematic manner and with appropriate attention to standards, regulations and international reach with respect of their combined influence and potential role within an Internet of Things. The CASAGRAS inclusive model sees the wide ranging wired (including fibre-optic) and wireless communications platforms an essential set of platforms for linking components within the IoT infrastructure, from object-level to the Internet. Clearly these communications platforms also form the basis for linking nodes in network structures, with the nature of the nodes determining to a high degree the functionality of the respective networks. From the nodal standpoint developments in ubiquitous computing and embedding capability will have a profound influence upon the nature of networked structures through the functionality that can be delivered, from simple data exchanges to intelligent decision making.

Along with ubiquitous computing there are other factors that will bear upon the realisation of the IoT, including:

- Communications platforms
- Sensor networks
- Wireless sensor networks
- Ubiquitous networking
- Identification in ubiquitous networking

3.2.1 Communications platforms

Communications platforms in relation to the Internet of Things must clearly accommodate those that relate to the various RFID carrier frequency and functional modalities as well as both wired and wireless communications modalities that accommodate data transfer. Wireless platforms for radio communication provide an extensive and extending capability for RFID systems and applications, extending reach from a few centimetres to 1000's of kilometres. Of particular significance in this respect are the IEEE protocols:

- WiFi (IEEE 802.11 variants)
- WiMax (IEEE 802.16)
- Bluetooth (IEEE 802.15.1)
- UWB (IEEE 802.15.3a)
- ZigBee (IEEE 802.15.4)
- Flash OFDM (IEEE 802.20)

These protocols facilitate greater capability for networks and, based upon the RFID functionality, contribute to the range of network structures that will form part of the Internet of Things and allow mobile communications technologies and mobile phones to become an integral part of such a structure. Associated RFID systems exploit the user devices as tags and access points as interrogators. Integral identifiers such as MAC addresses are exploited for identification purposes.

Integration is a further feature in the development of 'communication systems-based' RFID with, for example, mobile phones incorporating NFC (Near Field Communication) tags and or interrogators.

With RFID front-end interrogators linked or integrated into wireless communications devices the prospect is presented for wide ranging and innovative applications. Moreover, the communications platforms invariably allow structuring of Body-area networks (BAN), Personal-area networks (PAN), Local-area networks (LAN), Metropolitan-area networks (MAN), Wide-area networks (WAN) and Global-area networked (GAN) systems. The boundaries between standard communications systems and the methods that are employed by RFID systems to communicate in the edge layer can become blurred.

3.2.2 Ad hoc networks and Mobility

The ad hoc category of networks, based upon wireless local network protocols, such as WiFi, allow constituent terminals to communicate between each other without external support and with the capability of evolving according to access and user intervention. A further feature often associated with ad hoc networks, particularly wireless networks, is that of mobility. Mobility can have a particularly important role in achieving ‘anywhere, anytime’ communication and as such can be seen as an important consideration in realising an IoT. The mobility platform can be associated with a range of physical devices, including mobile phones, smart-phones, personal digital assistants (PDAs) and mobile or pocket PC computers which collectively contribute to the physical data transfer layer in a prospective Internet of Things.

Wider communications for network support can extend to a wide variety of access networking technologies, including, Digital subscriber lines (xDSL), Hybrid fibre coaxial (HFC), Power line communication (PLC), satellite, General packet radio service (GPRS), Code division multiple access (CDMA), Global system for mobile (GSM), High-speed downlink packet access (HSDPA) and Wireless broadband (WiBro).

While the Internet protocols were essentially designed for fixed networks, the progression to encompass wireless and more specifically mobile communications for access purposes is also reflected in the need to exploit wireless and mobile communication networks within the Internet of Things. Mobile ad hoc wireless networks may be considered particularly significant in this respect because of the absence of fixed infrastructure, ease of network construction, relatively lower costs and relevance to object management applications in which movement beyond fixed cell wireless zones is a requirement. In contrast to wireless networks that require objects and readers to remain within a fixed cell, to ensure connectivity in mobile structures, connectivity is essentially maintained in moving between cells. As with other network supported services quality of service (QoS) provision is an important consideration.

3.2.3 Heterogeneous Networks

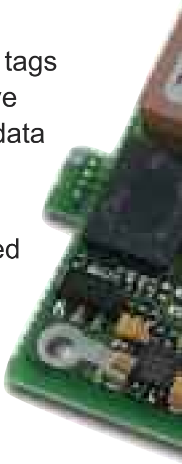
Heterogeneous networks are networks connecting computers and other devices, including embedded processing devices, having different operating systems and / or protocols. Notably such networks include, for example, local area networks (LANs) that connect Microsoft Windows and Linux-based systems to Apple Macintosh systems or Tron-based operating system exploiting ubiquitous ID. The term is also used to denote networks that exploit different access technologies. As such they constitute a significant consideration in structuring an IoT.

Structures involving different access technologies become a necessity in some wireless-based network applications where there is a need to maintain connectivity and a service in moving from one cellular network to another. Such structures are known as wireless heterogeneous networks.

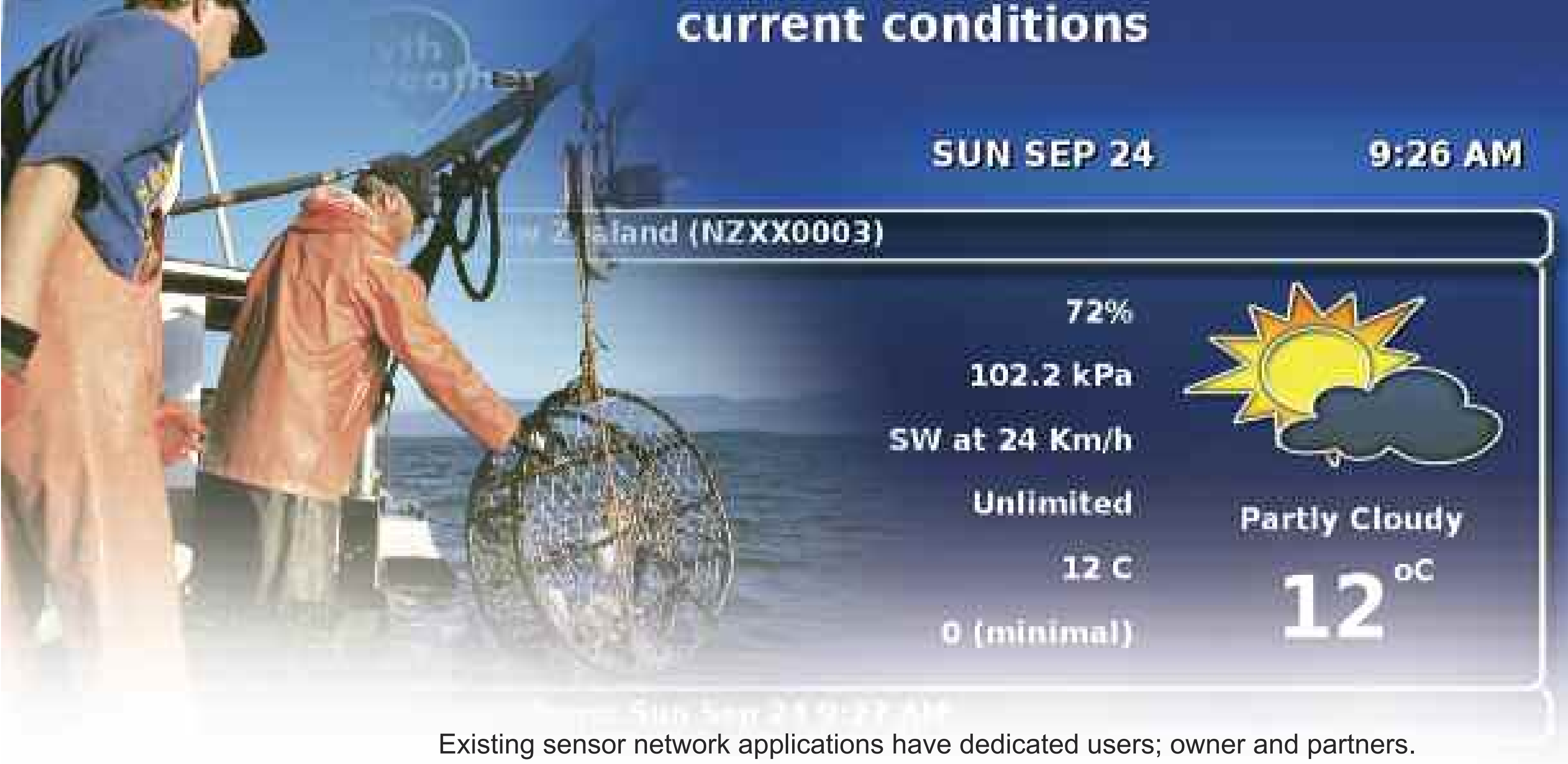
3.2.4 Sensor Networks

Existing sensor network applications have a straightforward operational chain involving sensing, data transmission, processing and provisioning. Sensor nodes and resulting sensor networks detect or measure physical quantities; they then transmit sensor data to backend sensor network application systems; the application systems collect sensor data and perform data processing functions; and the application systems produce application-dependent information. Evolving sensor networks and their applications/services exhibit more sophisticated functions within the transmission, processing and provisioning steps:

- Sensor networks may be structured in various ways using a variety of technology platforms such as 6LoWPAN, ZigBee, WirelessHART, I SA100, and others. There are so many legacy sensor networks installed in wire-line networking techniques like RS-232, RS-422, RS-423, RS- 485, Ethernet, and so forth. Sensors built-in to RFID tags may provide the basis for other solutions. Such networks may be integrated to derive sensor data from nation-wide, regional or l ocally-specific areas. Moreover, sensor data may be acquired by business contracts via other sensor network manipulated by public organizations, private enterprises, government agencies and so forth;
- Due to dynamic service models, a variety of application functions have to be involved such as filtering, analyzing, context processing, data mining, decision making, forecasting, integration, exporting, etc; and
- Since anyone can be an information user and information content cannot be pre-defined, sensor data may be delivered in different forms such as text, audio, voice, image and so forth, according to information user requirements.



There are so many kinds of legacy sensor network applications, including industrial automation, various monitoring and control applications, civil engineering, intelligent building, home automation. Such sensor network applications work usually within a single application domain. But, evolving sensor networks and their applications can extend beyond these single domain structures. For example, a sensor network service provider may need to interoperate with other service providers to get raw sensor data, processed results, or information services for more improved service provisioning.



Existing sensor network applications have dedicated users; owner and partners. But evolving sensor networks and their applications/services aim at consumers as well as business partners. For example, weather information may be provided to arbitrary consumers such as tourists and fishermen as well as business partners such as air lines, shipping companies and travel agencies. Pre-defined user (i.e. business partners) contracts or agreements result in B2B-type sensor network services and arbitrary consumers by service subscriptions result in B2C-type sensor network services.

Ubiquitous sensor networks (USN) applications have vertical service characteristics. This means that each application has unique requirements rather than common requirements, and has a unique profile of functional requirements. Thus, architectural configurations of hardware equipments and functional software components might be often made uniquely for each USN application model. But a set of common technology domains can be identified as shown below. More technology domains may be identified.

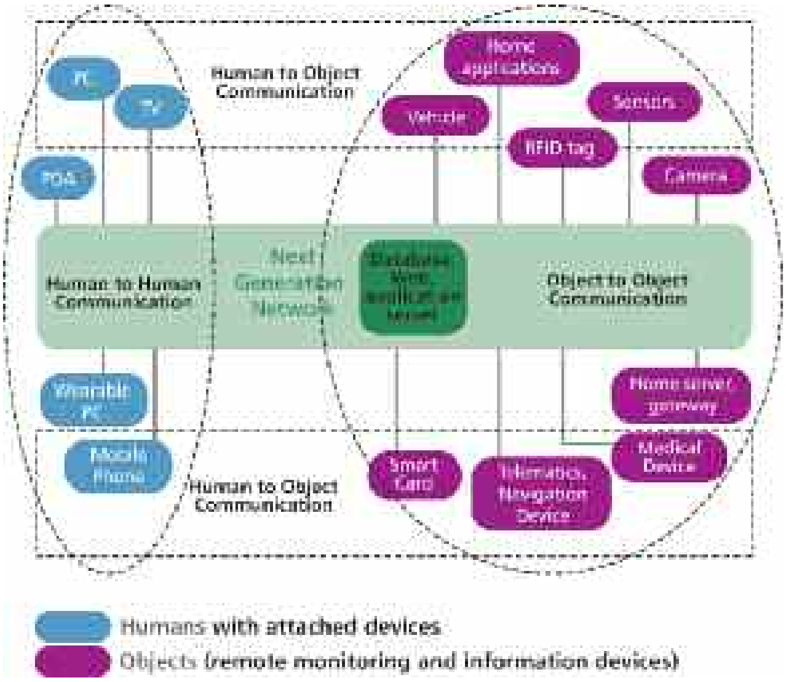
A choice of wired and/or wireless networking technologies depends on service characteristics and requirements of a USN application/service. Networking technology examples include, RS-422, 423, 485, PLC, CAN, Ethernet, RFID, Bluetooth, WLAN, IEEE 802.15.4, etc. where leaf sensor devices may be sensor tags and/or sensor nodes including actuators.

Sensor networks are not isolated but connected, usually to enterprise networks or telecommunication-based sensory information service providers, via various access networks and core networks. USN might require some extensions and/or additions to core network architectures in order to cover new functional capability requirements extracted from USN applications and services. The Next generation network (NGN) and the Internet may be considered core networks in this respect.

The USN middleware will comprise many software functionalities such as context models and processing, sensory information gathering, data filtering, data mining, contents management, web service functions, network and software management, sensor profile management, directory services, inter-working gateways and so forth.

Actuators are often an important part of sensor-based structures and networks, used to effect a wide range of physical functions, such as raising or lower a barrier, operating a valve, adjusting a temperature controller and so forth. Such structures will become increasingly important in IoT applications where physical control functions are required, and often are part of sensor-actuator networks (SANs). This is a particular feature of the proposals presented in the concept for the Real World Internet (RWI) .[3]

[3] Gluhak, A et al., (2009), Towards an architecture for a Real World Internet, Towards the Future Internet – A European Research Perspective, IOS Press 2009.

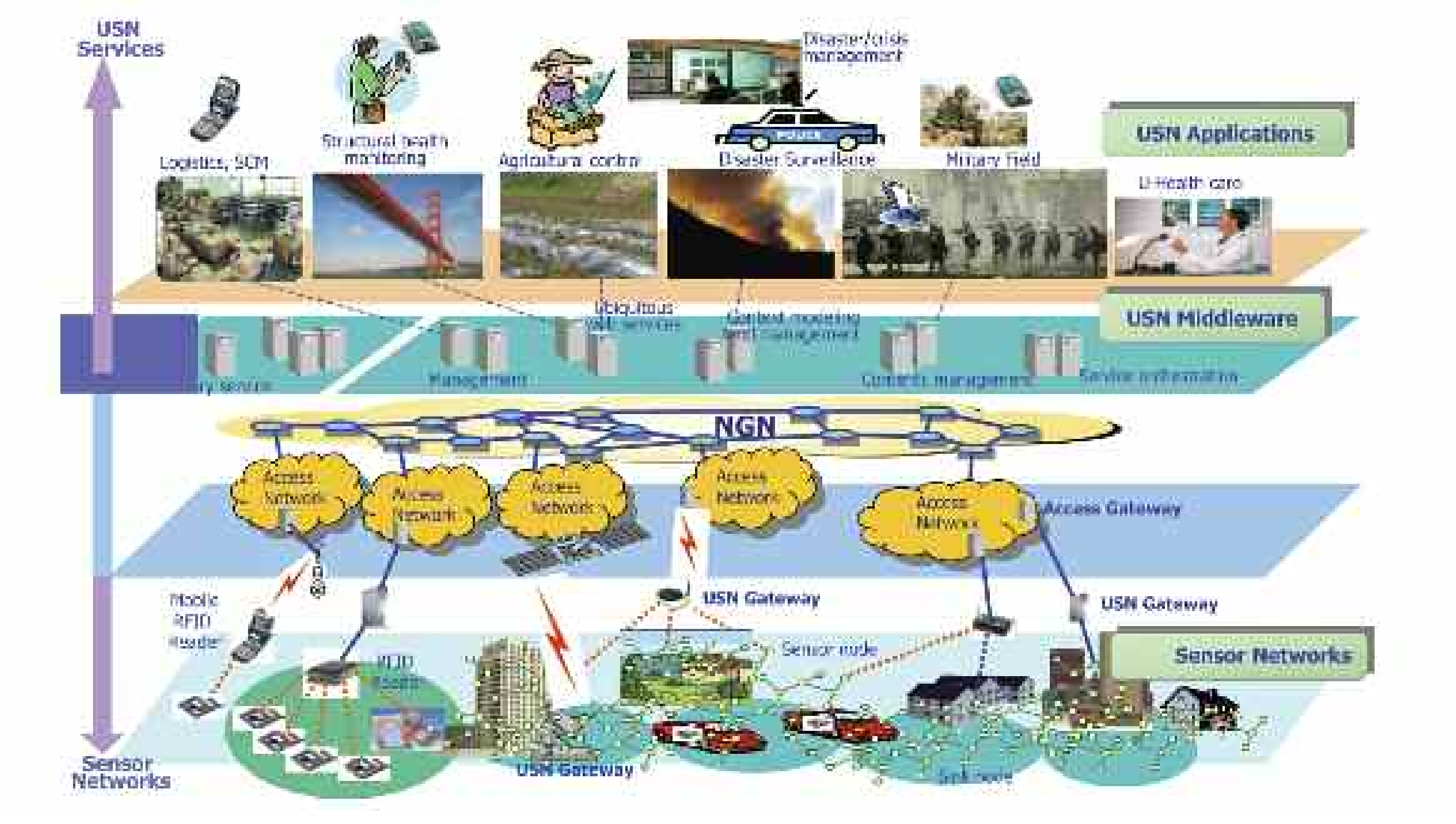

Human to Object Communication
PC
TV
PDA
Home applications
Vehicle
Sensors
RFID tag
Camera
Human to Human Communication
Next Generation Network
Database Web application server
Object to Object Communication
Wearable PC
Mobile Phone
Human to Object Communication
Smart Card
Telematics, Navigation Device
Medical Device
Home server gateway
Humans with attached devices
Objects (remote monitoring and information devices)

3.2.5 Ubiquitous networking

As identified in the term, the ubiquitous networking is the networking capability to support various types of communications. Therefore from the viewpoint of the physical configuration of communication, they are not so very different and every configuration is actually the same but with differing capabilities. However, the ubiquity will reflect the variety of heterogeneous and ad hoc network types and the accommodation of sensor-actuator (SAN) systems and so called ubiquitous sensor networks (USNs).

"Human-to-Human" communication has been the dominant capability supported by communications and with the USN concept "Human-to-Objects" communications are emerging and extending the communication capabilities. In addition, the ubiquitous networking will expand communication capabilities to cover "Objects-to-Objects" as well as support legacy communications.

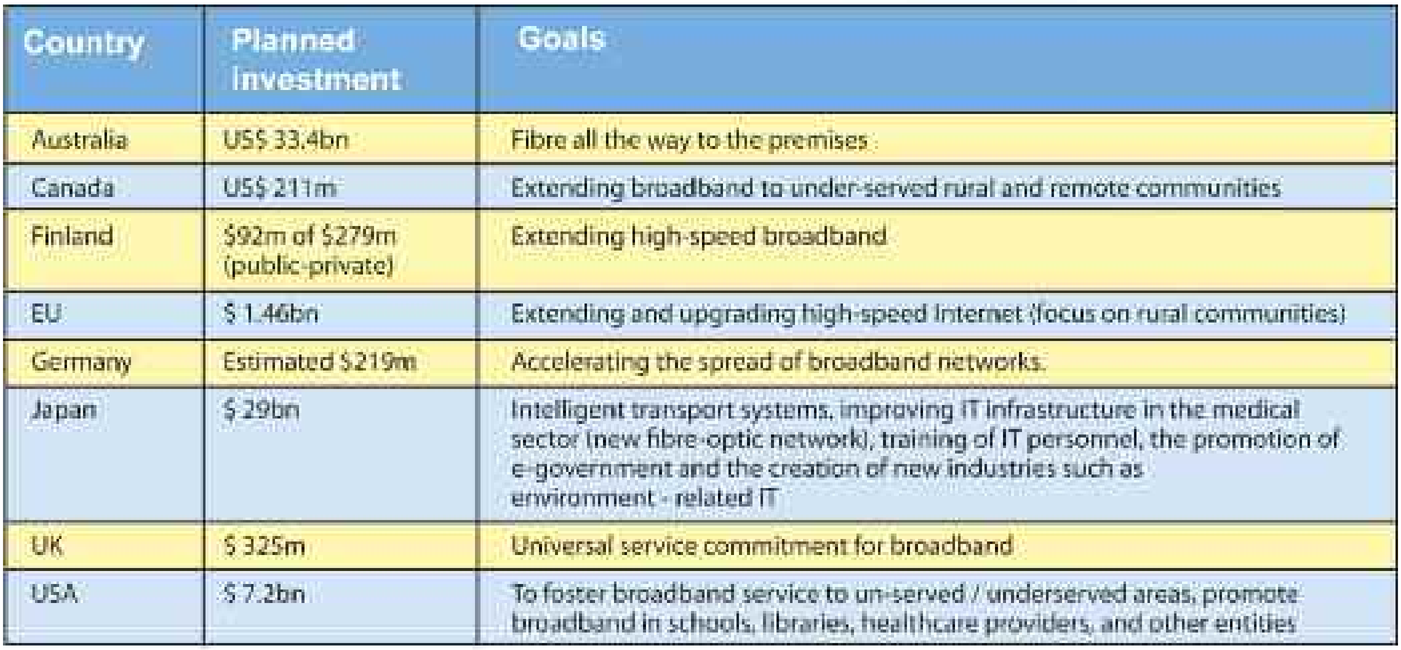
With proliferation in networks and connections between networks the need can be seen for greater architectural control and governance, together with additional support features in respect of security and defences against attack, loss of connectivity and issues relating to privacy and protection of personal information.



3.2.6 The Broadband Dimension

Extending the reach of broadband, coupled with upgrading networks to support very high speed communications, is being seen as a priority in many countries around the world. As a vehicle for supporting an Internet-integrated Internet of Things the broadband high speed networks and network reach into homes and businesses is of considerable significance.

The scale and nature of the global investment is depicted in the table below



Country	Planned Investment	Goals
Australia	US$ 33.4bn	Fibre all the way to the premises
Canada	US$ 211m	Extending broadband to under-served rural and remote communities
Finland	$92m of $279m (public-private)	Extending high-speed broadband
EU	$ 1.46bn	Extending and upgrading high-speed Internet (focus on rural communities)
Germany	Estimated $219m	Accelerating the spread of broadband networks.
Japan	$ 29bn	Intelligent transport systems, improving IT infrastructure in the medical sector (new fibre-optic network), training of IT personnel, the promotion of e-government and the creation of new industries such as environment - related IT
UK	$ 325m	Universal service commitment for broadband
USA	$ 7.2bn	To foster broadband service to un-served / underserved areas, promote broadband in schools, libraries, healthcare providers, and other entities

Source: Collins, L (2009), A networked recovery, Engineering and Technology, 4, (13), 66, July 2009./ OECD Ministerial Council Meeting, 24-25 June 2009, “Networked recovery” – Investing in ICT infrastructure.

One of the consequences of the global recession is that various countries around the world are providing significant fiscal stimuli in the form of stimulus plans, the content of which can be seen to provide considerable opportunity for extending communications and both wired and wireless networking. China, Japan, South Korea and India are particularly significant in this respect, with China showing considerable investment in 3G mobile communications. Such developments would appear to present an important opportunity for exploiting the extending communications and broadband platform as part of an integrated platform for the Internet of Things. International cooperation would of course be an essential requirement for accommodating and exploiting the broadband platform.

While the country-specific intentions are generally directed towards achieving universal broadband coverage the various networked-based propositions could result in lack of interoperability on a global basis if not considered with international cooperation.

Europe provides a case in point, where attention is being directed towards a fibre-optic networked infrastructure. EU investment of a €1 billion is being seen as the basis for a regulatory driver to release tens of billions of Euros of private investment, leading prospectively to problems of access control and lack of interoperability unless the conditions of public support demand open access and interoperability requirements.

There are also arguments over the potential of fibre-optic based networks,[4] suggesting that:

- Innovation will not materialise for fibre-optic networks without competition
- Lack of know-how in exploiting the potential of fibre-optic networks
- Lack of key applications

What is viewed here as limitations on potential may equally be viewed as opportunities for innovation with respect to interfacing with the physical world and the Internet of Things. It is clear from the goals identified for Japan and USA that broadband and optical-fibre networks are being directed at significant areas of application. The need can be seen for a level playing field, a view expressed by Commissioner Vivian Reding [5] at a meeting with telecoms executives in June 2009, stating that “the last thing we need is new monopolies” and “all the artificial scarcity of services that could go with it”.

The broadband platform is clearly a significant component in any plan or specification for realising a global reaching Internet of Things, but requires some well defined levels of on-going international cooperation to achieve the potential it has to offer.

3.2.7 An Internet Domain for developing the Internet of Things

Given the enormous latent potential that can be seen in principles and technologies the realization of an Internet of Things is a global imperative. However, because of the political, governmental, social and commercial ramifications of an Internet-integrated Internet of Things the need can be seen for a tangible platform for researching and developing the infrastructure and associated platform for applications and services. An internationally-supported generic top level Internet domain (gTLD) could conceivably provide such a domain.

In 1998 the International not-for-profit organization, the Internet Corporation for Assigned Names and Numbers (ICANN) was set up to oversee the structure of the Internet and the requirements for maintaining its stability. It regulates the way in which the web addresses are assigned to ensure that the computers exploiting the addressing can communicate appropriately. In June 2008 ICANN announced a significant liberalization in top-level domain naming, allowing applications for virtually any top-level domain name (akin to .uk, .org, .net), at a cost of at least $100,000 per name and with a strict requirement on resourcing capability (including, servers, routers and data bases).

As a consequence of the ICANN announcement the prospect may be seen, possibly through an .iot domain, for more easily accommodating the integration of the Internet of Things and attending to the specific performance and service-support needs that the Internet of Things will demand. Such a domain is a consideration that requires further attention and should constitute a study in its own right. However, the rationale for proffering such a proposal is essentially to assist in dealing with likely problems in IoT development in a more controlled manner, particularly where the need is being seen for greater international cooperation. However, it may also be seen as an explicit vehicle for the IoT rather than an evolutionary diffusion into the Internet at large.

With greater degrees of automation, complexity and networked application support without direct human intervention the needs with respect to performance, quality, maintenance and security issues are likely to assume a greater significance than conventional Internet services.

[4] Collins, L (2009), A networked recovery, Engineering and Technology, 4, (13), 66, July 2009.

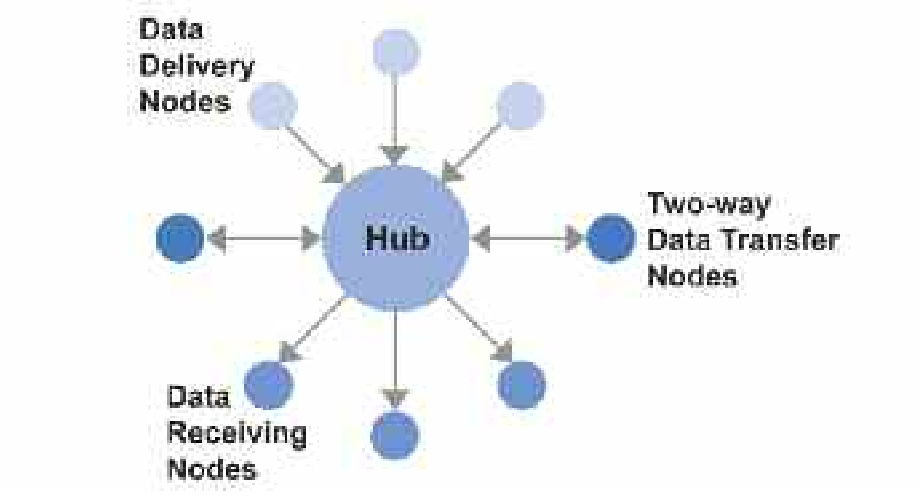
[5] Neroth, P 2009), Open for business, Engineering and Technology, 4, (13), 67, July 2009

Various options will need to be explored:

- One option is to have a gTLD exclusively for the Internet of Things, for example .iot This has the disadvantage that while it appears to provide a cohesive entity, commercial pressures from some companies will want to retain, for example a.com address.
- Another option is for a gTLD to relate to a sector and for sector specific identifiers, resolvers and discovery services. Such an established gTLD is .aero where the organisation that manages this namespace also provides other computer-related service to the air transportation sector.

The URL, being the basic addressing scheme for the World Wide Web, provides the capability of accommodating legacy numbering systems. EPC can be encoded as a URL. As such the EPC URI provides the basis for ensuring that the EPC Network is compatible with the Internet development. Taking a more international viewpoint other legacy systems may be recognised, including ubiquitous ID (UID) that will require attention both in specifying a global identification scheme and in specifying a range of data carrier technologies.

Be it a world object web (wow) simply in name or as a defined gTLD structure, the concept offers a platform for discerning applications and services at various levels (personal, domestic, corporate, public, regional, environmental, national and international) and in respect of object-groupings initially discernible from a consideration of the nature of object-space. Development and exploitation of the service oriented architecture (SOA) provides the foundation for a software bus capable of supporting such applications and services.



The processor-based servers that will constitute the nodes within the Internet of Things may extend to devices embedded-in or attached to objects that allow the objects to be identified and communications to be supported between such nodes. Objects carrying such processor platforms have been referred to as smart objects.

Further structures are also required to fulfill the necessary functionality of an Internet of Things, such as hubs linking data acquisition nodes and data receiving nodes or a combination of both. Two-way communication protocols may be supported to effect data transfers be they uni-directional or two way.

As in the Internet, or in exploiting the Internet itself, the Internet of Things will invariably use hubs and routers to ensure packets of data reach their specified destinations. Particular nodes within the Internet of Things will exhibit sensor capabilities as well as identification and communication attributes. Supported by appropriate processing capability, localized or distributed, network components may be grouped and configured to support wide ranging application and service needs.

In any application or service defined within the Internet of Things machine-readable unique identification is a key requirement. For the Internet of Things a resolver scheme is necessary to accommodate legacy and future identification coding systems. Such an approach [6] has been proposed within the CASAGRAS project which, suitably integrated with the use of internet protocol (IP) provides the identification framework for supporting the Internet of Things. The scheme provides the structure for accommodating legacy and evolving systems such as the EPC systems and services as one among many identification-initiated services.

Given this framework and the network features identified above new applications and services can be designed; prompting too the possible need for a design standard.

Many of the application scenarios that have appeared in the media for the Internet of Things, such as the intelligent fridge, ambient intelligent home and assisted living, can in many respects be structured as localised services without any particular internet-type requirements. Localised solutions may often be effective and efficient and more easily structured. However, in defining an Internet of Things development that simplifies and effectively supports the realisation and maintenance of new applications and services, in much the same way as web sites can be structured and operated, object-connected applications may be designed and initiated by software transfers and supporting communications from appropriate domain sites (Internet of services component of the Internet of Things). Thus, efficient energy control within the home, for example, may be initiated by such a service, available, up-datable algorithms being used to achieve more effective usage of available resources and in response to measurable environmental quantities.

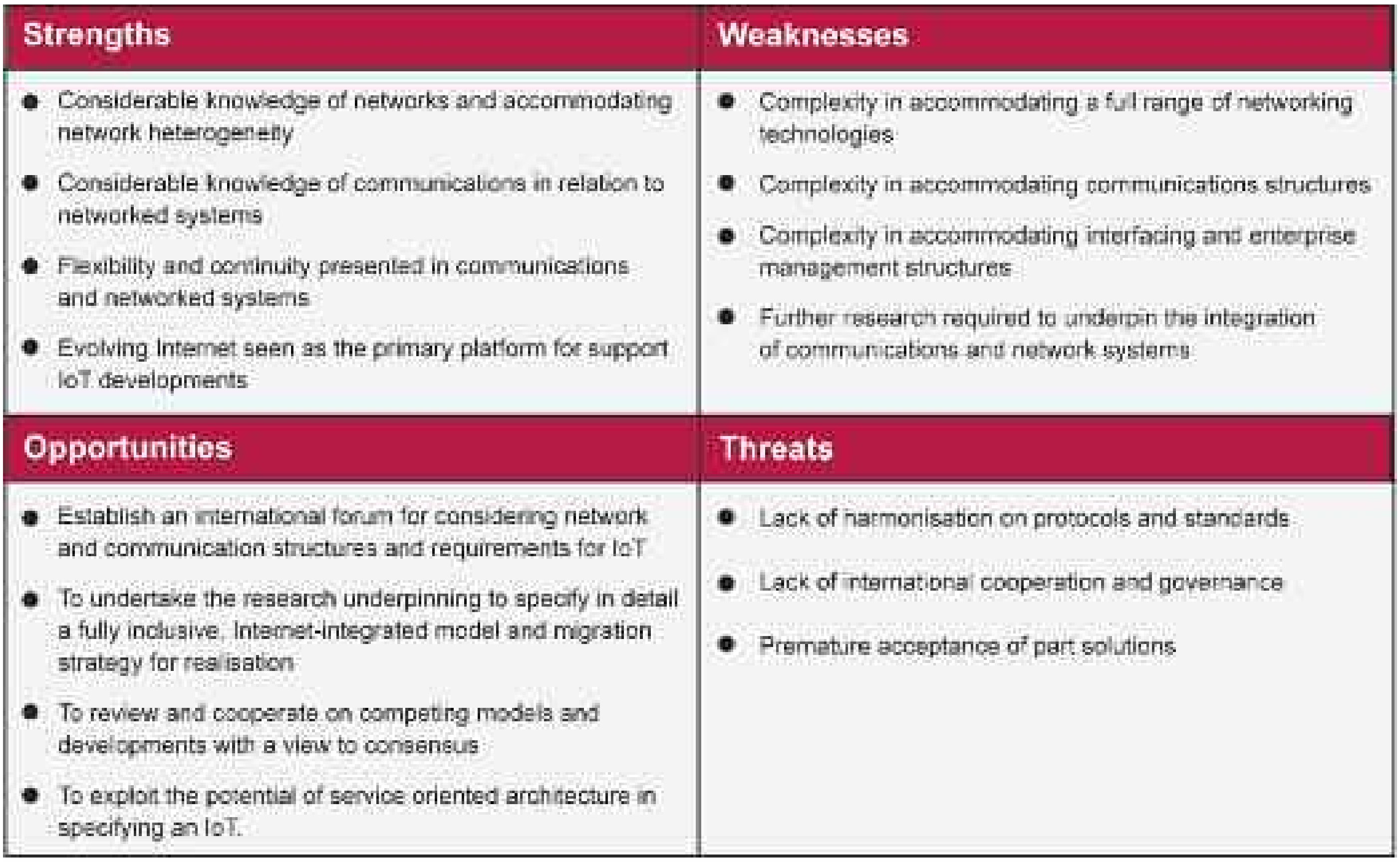
Integration with the evolving Internet may exploit the conventional Internet offerings such as the world wide web to link services and extend capability. For example a conventional web site might offer object-connected software support services that would be implemented through a separate Internet of Things domain. Services may exploit direct linkage between data carrier readers and the Internet. Already camera-equipped and RFID reader- equipped mobile phones are being used to read data carriers on objects, such as posters, the IP identifiers so derived yielding access to information on particular web sites. The camera-equipped devices generally exploit new and established, standards-supported matrix code data carriers printed or applied to particular objects.

[6] CASAGRAS white paper on Global coding and Resolvers

Other types of identifier carried in the same or different types of data carrier may be resolved to point to particular IP addresses depending upon the application software.

Using appropriate IP addressing edge-implemented object-connected applications, including networked structures, may exploit Internet connections to derive application support information, share information or generate new information and knowledge. Such capability could be exploited in what may be called business process transformation (BPT), in contrast to business process re-engineering (BPR), and exploiting a principle of extended process functionality (see section 3.7.3 Object-connected ICT).

3.2.8 SWOT Analysis – Networking and Communications



Strengths	Weaknesses
● Considerable knowledge of networks and accommodating network heterogeneity ● Considerable knowledge of communications in relation to networked systems ● Flexibility and continuity presented in communications and networked systems ● Evolving Internet seen as the primary platform for support IoT developments	● Complexity in accommodating a full range of networking technologies ● Complexity in accommodating communications structures ● Complexity in accommodating interfacing and enterprise management structures ● Further research required to underpin the integration of communications and network systems
Opportunities	**Threats**
● Establish an international forum for considering network and communication structures and requirements for IoT ● To undertake the research underpinning to specify in detail a fully inclusive, Internet-integrated model and migration strategy for realisation ● To review and cooperate on competing models and developments with a view to consensus ● To exploit the potential of service oriented architecture in specifying an IoT.	● Lack of harmonisation on protocols and standards ● Lack of international cooperation and governance ● Premature acceptance of part solutions

3.3 Using identifiers to link objects to the Internet of Things

It might seem obvious that the vast majority of control schemes for physical objects are given man-made identification codes when linked to computers. In fact, many legacy systems that predate computers were transferred lock stock and SKU number into the computer era. Such examples include engineering part numbers that are based on drawing numbers with significant in-built contextual structure for easier filing. Computer-based searches and encoding in bar codes and other data carriers had to contend with a large variety of defined code structures.

The ingenuity of individuals, committees, and industry bodies has resulted in hundreds, maybe thousands of different schemes. Not only is there a significant legacy of coding schemes, but even some of the newer schemes being invented in the RFID era add yet more variants. A challenge that will need to be addressed is how to incorporate such different schemes into an overall structure for the Internet of Things.

For the purposes of the CASAGRAS project the focus has been upon identifiers that are linked to data carriers, and even more specifically on the data input and output (the source code) as opposed to any specific data carrier channel encoding schemes. This approach could result in greater flexibility between different data carriers being capable of interacting with the Internet of Things.

3.3.1 Coding schemes and data carriers

This year marks the 35th anniversary of what is now known as the GS1 bar code system. In this period of time over a million businesses, particularly those associated with retail products, have migrated to a common product identification scheme that is encoded in a common bar code data carrier. While this is a significant achievement, it has to be put into perspective: the system does not cover all retail products, or all products from manufacturers who have coded some products to the GS1 rules. It certainly only covers a small fraction of all manufactured products.

As the EPCglobal system is built on the foundation of the GS1 system there is the prospect that a significant proportion of the items will either carry a GS1 bar code or an EPCglobal RFID tag.

Other sectors also adopted barcode technology for item identification purposes: automotive parts, baggage, casks of whisky, donations of blood. It is possible to continue with examples through the alphabet. These examples are all supported by specific sectoral bar code application standards that are in turn based on item code structures that are generally only relevant to the sector. There are also more formal code structures that have been specified in International Standards; in fact there are over 25 formal registration authorities for different types of item code or organisation codes that support item identification .

A coarse assessment of the share of[7] revenue for bar code systems made some years ago was that three sectors each contributed one third of the revenue:

- GS1 applications
- other open systems
- closed system applications

While this is fairly crude division, it does indicate that following decades of bar code applications, considerable diversity will need to be addressed in any migration to RFID and beyond that to the Internet of Things.

3.3.2 Bar code standards for "cooperative solutions"

As more industry-based bar code applications were implemented for supply chain purposes in the 1980s, it became clear that there was a potential clash of identifier codes used by different industries. There was certainly a crossover issue between the European automotive, chemical and electronics sectors. The codes from one sector were quite naturally through trade appearing in the other sectors. So a European standard (EN 1572) was developed to define a solution that would enable multi-industry applications to coexist. The standard specified a hierarchical registration structure, where the first level defines an Issuing Agency Code (IAC) followed by a membership code assigned by the registered IAC (e.g. Odette for the automotive sector), followed by the individual organisation's identifier code.

The principle is straightforward. Each business unit can retain its own code structure, but applies the IAC and membership code as a prefix when this is encoded in a bar code. Such concatenated codes are easy to construct

[7] http://www.iso.org/iso/standards_development/maintenance_agencies.htm

with front-end software. At the receiving end, the company can either accept the full code structure or strip off the IAC and membership code.

The full code structure does result in a unique code across all the sectors that use the system originally specified in EN 1572, without having to go through a complex migration path.

All of the work to develop EN 1572 is now incorporated in ISO/IEC 15459 (Parts 1 to 6) Information technology -- Unique identifiers. Part 2 of the ISO standard deals with the registration rules for the IAC, Part 3 deals with some common rules and the other parts are used to identify different classes of unique item identifier that are common in the supply chain. The current 15459 IAC register [8] shows that many leading industries make use of the system. Besides the original European groups, the system now extends to cover codes from NATO, UPU, various bodies concerned with coding in the health sector, and also extends to international codes. One IAC is assigned to the Dun and Bradstreet business identification system, which allows any business in the world to be identified. The IAC structure not only impacts inter-industry communications, but also intra-industry communications. For example the European automotive sector now uses, without any problem, codes assigned by Odette, Dun and Bradstreet, and an IAC code assigned to the Japanese automotive industry.

There is still significant potential to exploit ISO/IEC 15459 to achieve a more unified structure at relatively low cost to many other sectors. Capacity is not a problem: less than one percent of the IACs have been assigned. Cost is not a barrier: registration for an entire sector costs a few hundred Euro. The standard is one of the best kept secrets for delivering a cost effective multi-sector identification and tracking system. Its lack of publicity is a serious weakness, especially as it could provide a basic migration for the Internet of Things.

3.3.3 RFID Object Identifiers for "cooperative solutions"

The development of RFID standards by ISO had to take account of the legacy bar coding systems and the associated identification codes for the items being coded. Research pointed to the potential of using another ISO standard as the corner stone for encoding and the RFID communications network. This standard is: ISO/IEC 9834-1 *Information technology -- Open Systems Interconnection -- Procedures for the operation of OSI Registration Authorities: General procedures and top arcs of the ASN.1 Object Identifier tree.* There are many different Object Identifier (OID) schemes but all have one of three roots: ITU-T, ISO (including ISO/IEC), and joint ITU-T ISO structures. Most of the effort for RFID has focused on the ISO root, but the other two roots are also capable of being supported.

The ISO OID root provides a lot of flexibility under three registration sub-structures:

- Each national standards body may act as a registration authority and provide an OID to any organisation wishing to register.
- Each ISO and ISO/IEC standard may also declare relevant object identifiers, with part of the OID being the reference number of the standard itself (to be described later).
- Using this second approach, a registration authority has been set up for RFID data constructs as defined in ISO/IEC 15961. This means that when RFID data constructs are registered, and the organisation does not have a pre-existing OID structure one can be created as part of the 15961 process.

The objective was to develop a system for encoding unique item identifiers in RFID tags by creating a concatenated {object identifier + data} pair. Let us use an example from the RFID data constructs registered for IATA baggage handling. The registration requires the data to be unique within the domain, and the object identifier defines that domain and the particular class of unique item identifier within the domain.

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

[8] http://www2.nen.nl/getfile?docName=196579

This clearly shows that IATA did not have its own OID structure for its baggage handling data, so the registration authority simply assigned one under the 15961 arc, with the next arc "12" indicating that this was for IATA baggage handling. IATA then assigned the final arc "1" to identify the baggage identification number (BIN), and distinguish this from any other data element. The BIN itself is exactly the same structure as that used by IATA for about 20 years for bar code track and trace of baggage.

So for a minimal registration fee, retention of an existing code structure, and adopting ISO RFID standards, IATA was able to establish its RFID standard for baggage handling (RP1740C) that enabled airports and airlines to integrate RFID with existing bar code system. No "big bang" for the industry, no need for fundamentally different computer systems, just the challenge of introducing RFID. Industry experts have assessed that this transition process has saved hundreds of millions of Euro. Any new RFID installation has no negative impact on the established bar code installations.

The transition to RFID can be assessed on the benefits to the individual operation, but as more airports install RFID for baggage handling each destination airport will get some additional marginal benefit when they decide to adopt RFID. This approach of introducing RFID technology in a non-disruptive manner from the perspective of identification codes will save the migrating sector the otherwise significant investment in new computer systems and probably delay take up.

It is obvious that the OID is a long code, and encoding this would consume tag memory and increase the time of each air interface communications. So an encoding "trick" is employed that effectively means that only the final arc (or Relative-OID) together with the BIN is encoded on the tag. However, in external communications from the interrogator through to the application the entire {object identifier + data} pair is transmitted. This has two advantages. The first is that it enables generic RFID equipment to be used for almost any application. Secondly it exploits the difference between a limited capability communication relay (the RFID tag) from the greater encoding and communication capabilities of network systems.

It has also been possible to encompass all of the ISO/IEC 15459 codes as a subset of the OID structure. As all this RFID OID activity started in ISO before the beginning of the EPCglobal system, at one stage it was also possible to encompass all of the GS1 system within the same scheme. The advent of EPCglobal will again result in the need for different schemes to be supported.

Object identifiers are formerly recognised as part of the URN namespace for the Internet, where the OID rules are defined in RFC 3061.

3.3.4 The Internet URN schemes

The Internet's Uniform Resource Name (URN) system is considered fundamental to the development of the Internet of Things. IETF Document RFC 1737 specifies the functional requirements for URNs including:

Global scope – URN being a name with global scope which does not imply a location, having the same meaning everywhere.

Global uniqueness – the same URN will never be assigned to two different resources.

Persistence – the lifetime of the URN is unlimited, remaining permanent even beyond the lifetime of the resource to which it is assigned.

Scalable – URNs can be assigned to any resource conceivably available on the network, indefinitely with respect to time.

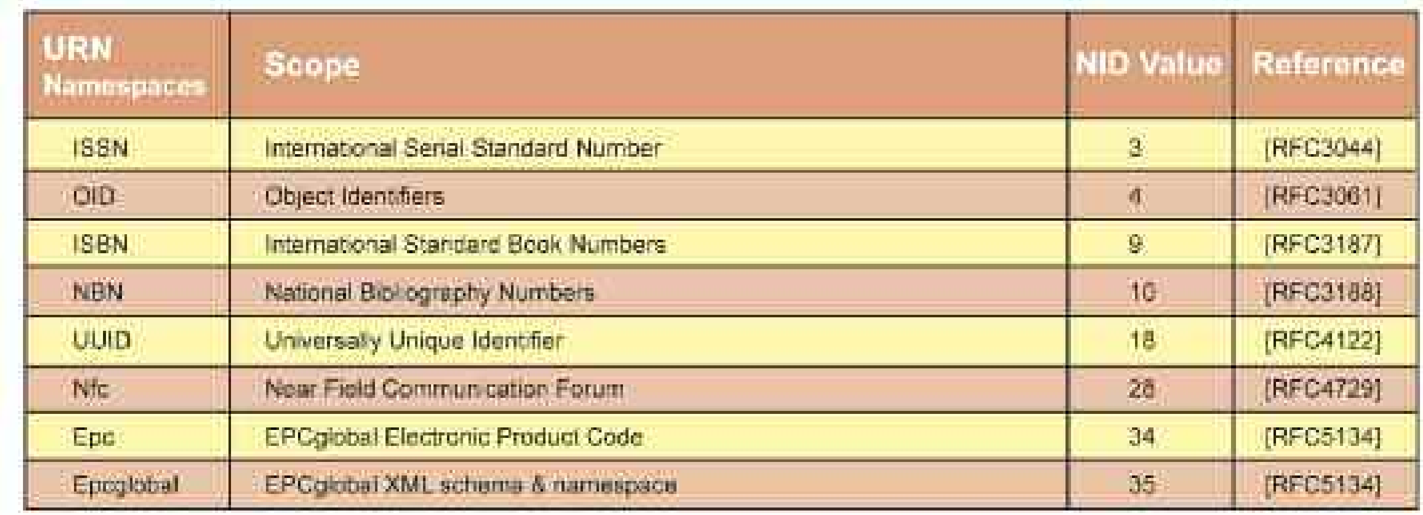
Legacy supporting – permits the support of existing legacy naming systems insofar as they satisfy other requirements of the scheme.

Extensibility – any scheme provided for URNs must permit future extensions.

Independence – it is solely the responsibility of the naming authority to determine the conditions under which it will issue a name.

It is important to note that while the URN may be globally unique and persistent it makes no guarantee that the resource to which it is assigned is unique or of permanent existence.

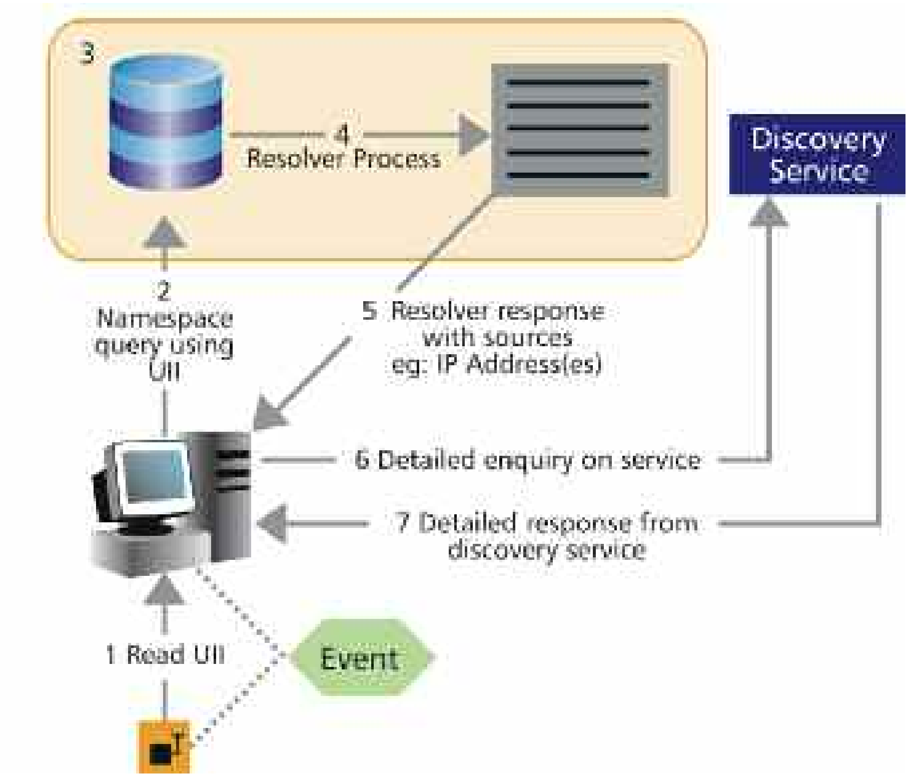
The URN has a number of sub-schemes registered under a URI namespace, using a namespace ID (NID). The list below identifies a few that might be relevant to the Internet of Things.



URN Namespaces	Scope	NID Value	Reference
ISSN	International Serial Standard Number	3	[RFC3044]
OID	Object Identifiers	4	[RFC3061]
ISBN	International Standard Book Numbers	9	[RFC3187]
NBN	National Biblography Numbers	10	[RFC3188]
UUID	Universally Unique Identifier	18	[RFC4122]
Nfc	Near Field Communication Forum	28	[RFC4729]
Epc	EPCglobal Electronic Product Code	34	[RFC5134]
Epcglobal	EPCglobal XML schema & namespace	35	[RFC5134]

In principle, all the URN systems should have the same features. While they all possess the functional requirements specified in RFC 1737 as identifier systems, they are not all what could be called "resolver ready". In addition to the hierarchical structure defined in the respective RFC documents, this structure needs to be converted into a syntactical format for processing through a set of computers residing on the Internet (as illustrated in the figure below).

Schematic of a resolution process


3
4
Resolver Process
Discovery Service
2
Namespace query using UII
5 Resolver response with sources eg: IP Address(es)
6 Detailed enquiry on service
7 Detailed response from discovery service
1 Read UII
Event

Some of the URN schemes do not have a specified resolver, and many do not have an established discovery service. Some of these URN schemes and other candidates as identifier codes for the Internet of Things will be addressed in 3.4.14 the SWOT analysis.

There is a particular challenge with respect to the URN for the ISO RFID object identifiers. Currently, there is no resolver specified for the URN type for object identifiers. If the basic Internet DNS principles are followed, eventually the root of the tree either becomes ISO, ITU, or ISO/ITU combined. As it is extremely unlikely that a name server will be maintained by these organisations, some alternative scheme needs to be developed.

One possible solution would be to specify a syntax in such a way that the root for resolving within the Internet of Things is equivalent to the root-OID that is registered using the rules of ISO/IEC 15961-2. The very same table that enables a long OID to be truncated for encoding on the RFID tag could also be used to identify a root nameserver. This would result in different roots for IATA's baggage handling data, for library identifiers, for ISO/IEC 15459 traceability codes, and so forth. Not only does this parallel the DNS system of having different root nameservers for .com, .org, .net, .info, and .eu, but it would also enable different levels of security to be designed into the domain-based systems.

There are also a number of relatively new identifier codes that are also candidates for linking to the Internet of Things, as discussed below.

3.3.5 EPCglobal

The EPCglobal system supports a number of code structures for unique item identifiers. A few have been specified to comply with pre-existing GS1 serialised codes, or to add serialisation to other such codes. The long term potential therefore is for all the products carrying a GS1 bar code, applied by more than a million businesses, will carry a serialised RFID tag. In addition, some generic code structures are specified such as the General Identifier (GID-96) with a number of other code structures to be reserved.

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

urn:epc:id:sgtin:900100.0003456.1234567

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

3.3.6 Short-OID

The short-OID was introduced in ISO/IEC 9834-9 (ITU-T Rec X.668) in 2008 by a joint ITU-T ISO committee, with a view of providing a short root-OID for encoding on RFID tags and other data carriers. The OID structure is fully compliant with the IETF requirement, and has the following format:

urn:oid:2.27.n.r

where: n = the third arc of the OID structure assigned by the Registration Authority

r = the next (and any subsequent) arcs assigned by the registering organisation

NOTE: All arcs have to be numeric, and the alphabetic notation is used to show the structure

To some extent, the short-OID parallels the ISO RFID-based Object Identifiers discussed, but there are some differences:

- Because the short-OID avoids a long root-OID, in those situations where the full OID needs to be encoded, it offers the prospects of shorter encoding.
- However, the Registration Authority for ISO/IEC 15961-2 assigns a data format (5-bits and eventually 13-bits) as a shorthand means of minimising the encoding of a root-OID. This feature is not addressed in ISO/IEC 9834-9.
- The ISO/IEC 9834-9 OID structure is designed to be applied to "tags", meaning different AIDC data carriers. As such, it could be used as a basis for encoding an entire OID in any data carrier and offer similar solutions to different edge technologies. ISO/IEC 15961-2 applies only to RFID.

3.3.7 Near Field Communication Forum and UIIs

The Near Field Communication Forum is developing a parallel set of data capture and communication standards to those being developed by ISO and EPCglobal. These standards use an RFID-enabled mobile phone as the data capture device, with a tag based on the contactless smart card ISO/IEC 14443 standard, and proximity smartcard ISO/IEC 15693, specifying an operating carrier frequency of 13.56 MHz. (ISO/IEC 15693 uses the same specifications as ISO 18000-3 MODE 1).

Probably, in a B2B situation, these developments might have little impact. However, with the potential in a few years of NFC-enabled phones being as common as camera phones are today, it is a development that cannot be ignored for its potential to provide services to consumers.

Basically a number of URN schemes have been specified for encoding as literal strings. As an example the EPCglobal SGTIN seems to require 31 bytes (248 bits) compared to the 96 bits required for an EPC tag. This is because the NFC approach appears to be encoding an expanded translation of the EPCglobal SGTIN that is not present until some higher level stages in the EPCglobal system.

It is important to note here that the reason the term "appears" is used is because not all the NFC standards are published, even some that are defined as normative in standards that are published.

3.3.8 The 'Handle' System and Digital Object Identifiers

The Handle system uses a resolver mechanism that has similar basic functionality as, for example, the World Wide Web; but has some fundamentally different mechanisms.
Here the focus is on Digital Object Identifiers (DOIs) although the Handle system can support other structures

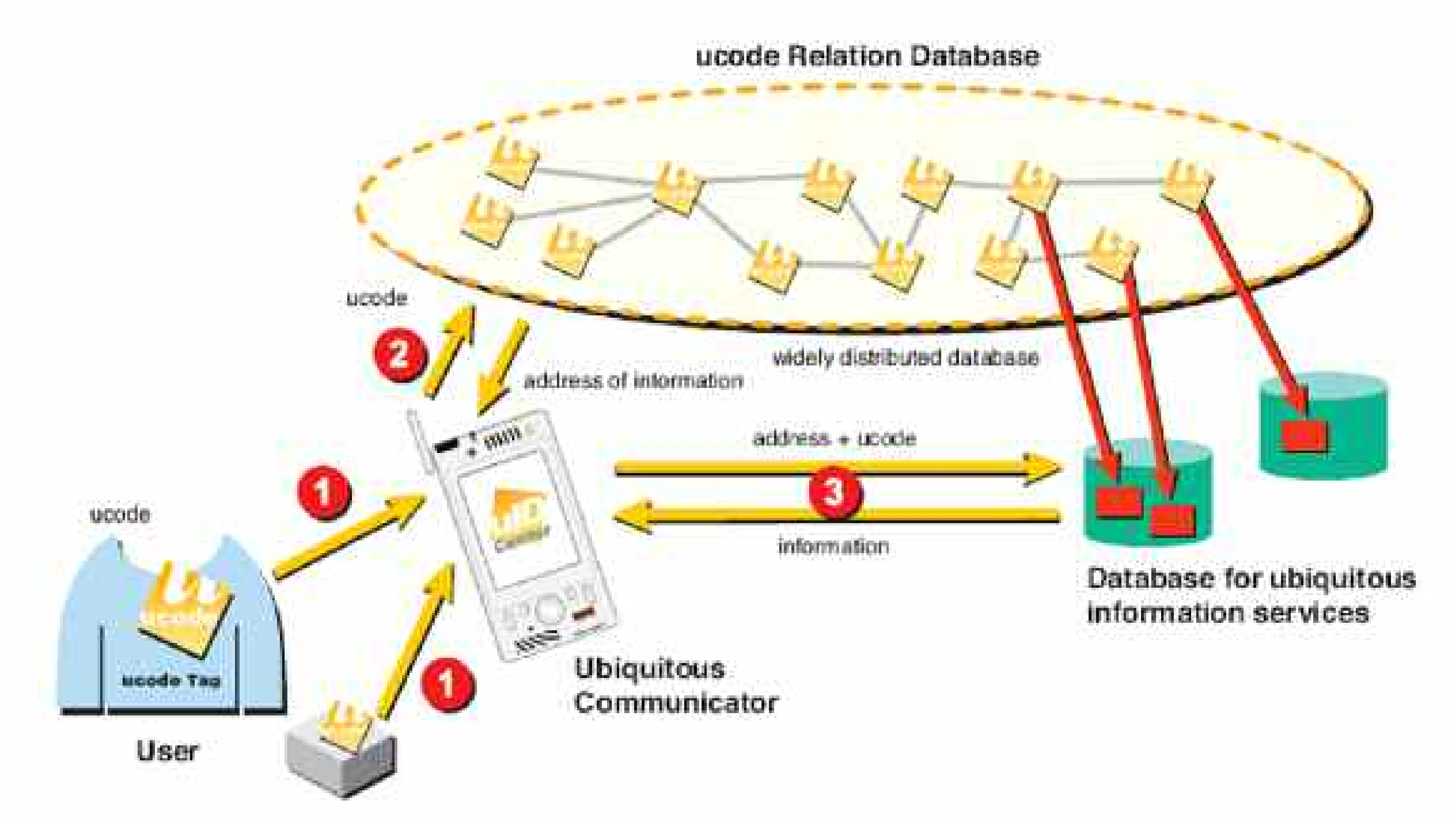
The DOI system has grown to be the predominant method for identifying digital media, particularly electronically available reports and papers. A typical DOI is:

10.1000/123456

The structure is as follows. The "/" separates the prefix from the suffix code. The Handle resolving process uses the prefix, whereas the suffix is used to access the content details (i.e. the discovery service). The prefix is sub-divided into at least two parts: the numeric code before the first "." identifies the particular Handle application (10 identifies DOI), and the part(s) after the "." identify the registration.

3.3.9 Ubiquitous Code

The Ubiquitous Code or ucode offers an end-to-end system that is capable of linking objects with the Internet of Things. Most of the development work has taken place in Japan and the Far East under the umbrella of the T-Engine Forum and, more specifically, the Ubiquitous ID Center. The T-Engine is the name for an architecture, that is arguably one of the most advanced platforms for ubiquitous computing to be found anywhere in the world. It has evolved from an open computing and communications architecture (TRON project) developed in the 1980's by Professor Ken Sakamura, one of Japan's leading computer architects.



The system has some fundamental differences from some of the other means of linking objects to the Internet of Things. Firstly, in addition to the basic ucode uniquely identifying objects, other ucodes identify space (locations) and even concepts and relationships (e.g. name, materials, producer). Thus, to access particular information, it is necessary to use a relational database of the different ucodes.

The basic ucode consists of 128 bit code structure where the first few bits are metadata in the form of a code ID, which then allows an existing code structure to be incorporated and then appended by a serial code if one is not already included in the code structure. An example of the code structure is provided in the literature from the Ubiquitous ID Centre to encode an EAN-13 product code (the fundamental GS1 product code), as follows:

- The first 12 bits identify a code assigned by the Ubiquitous ID Center for EAN-13 (in the literature this is referred to as the Japanese subset JAN-13).
- The EAN-13 code, as seen on many retail products, is then encoded in 4 bits per digit, presumably using some binary coded decimal structure, requiring a total of 52 bits for identification.
- Finally, the remaining 64 bits are for a serial number, making the complete 128 bit ucode unique from all others. Readers will observe some significant differences with the EPC system, where the 14-digit GTIN, and not the EAN-13, is used for product identification. Also the additional serialisation and EPC encoding rules over 96 bits follow completely different encoding rules to those for encoding mass market retail products as a ucode.

3.3.10 The Uniform Resource Locator (URL) as an identifier

Strictly speaking, the Internet Engineering Task Force (IETF) now considers the URL system to be a URI scheme (based on http) but in this section the more common and more widely used name is used.

The DNS, while it is structured to resolve does not directly provide access to unique data. However, the "absolute URL" does. This is illustrated in the example:

EXAMPLE

DNS:	www.mycompany.com
Absolute URL:	http://www.mycompany.com/AboutUs/Management.html

The DNS is sub-divided into "labels" divided by the dot ".". Each label can be up to 63 octets (bytes) long, with the total DNS being 255 octets long. And this is before the extensions to create the absolute URL, which is of unbounded length.

It is clear from this that compared with other identifiers, the URL is verbose; but has the advantage of being more acceptable to humans. There have been attempts (e.g. TinyURL) to shorten a verbose URL with an alias, that is as the TinyURL slogan claims is "making long URLs usable." This is achieved by using redirecting or forwarding techniques to the same web page. There are about 100 services similar to TinyURL, shortening long URLs to very short identifiers.

3.3.11 The IP address as an identifier

The general principle behind a resolving system is to separate the identity from the source of associated information. So, www.mywebsite.info as a URI is separate from the current (even permanent) IP address where associated web pages are held. Therefore, encoding an IP address directly in an RFID tag is usually considered to be a bad thing from an Internet operational perspective.

While general use in this way needs to be avoided, there is certainly one case where encoding an IP address could be valid. This is at the basis of proposals from the Internet Protocol for Smart Objects (IPSO) Alliance. The types of device that the IPSO Alliance is addressing are far more sophisticated than RFID tags. They are talking of CPU-based devices with memory in the region of 100 Kbytes of ROM and 10 Kbytes of RAM. Such devices would be capable of monitoring and applying logic at the edge, and would be truly the basis for Smart Objects in this respect.

If the purpose is to identify a sophisticated RFID tag with some in-built intelligent processing capability as a device in a network, then an IP address is probably the only suitable identifier. The caveat is that this needs to be a permanently assigned identifier while on a particular network.

Such an identifier structure requires no resolving process or discovery service. There are additional requirements for services and protocols for applications, including the structure of messages. These are considered to be beyond the scope of the IETF.

3.3.12 An overall assessment of identifier codes and the Internet of Things

It should be fairly clear that no single identifier code system will be able to claim the sole rights to the Internet of Things. The level of investment in legacy systems – and by the time that the Internet of Things becomes a reality some of the new systems will have a significant infrastructure investment – will provide the inertia of "change for change sake". So there will be a number of different identifier systems. Many of the identifier code systems discussed over the previous pages either use the DNS system, some variant of it (e.g. the EPCglobal ONS), or could adopt or adapt the DNS model.

The challenge remains in three areas:

Getting the particular identification code scheme adoption to a critical mass for specific Internet of Things services to be developed. So far, the DOI system appears to have achieved this for virtual things.

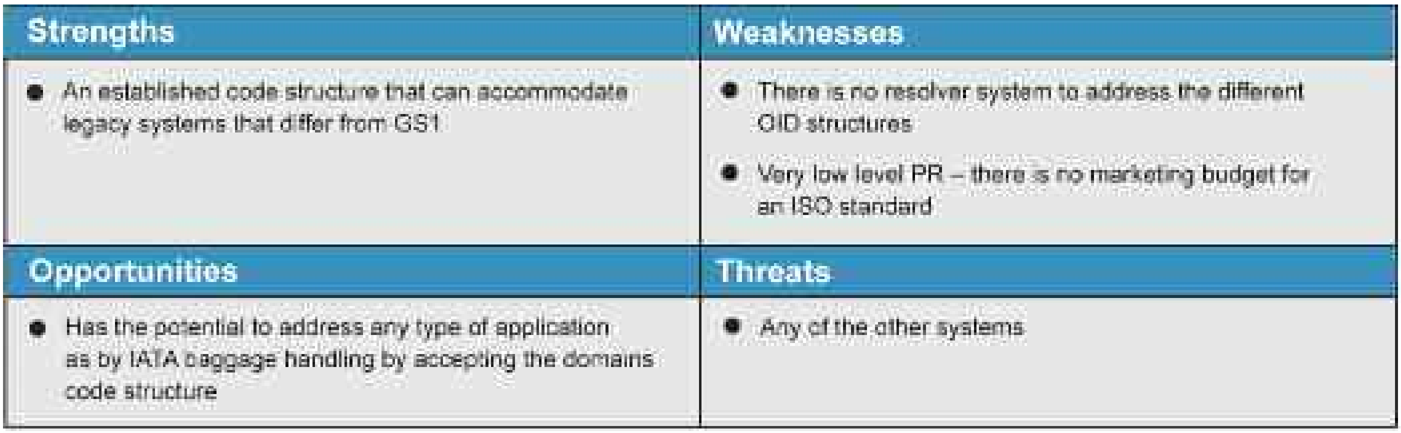
Getting the edge data capture technologies to be able to process different identifier schemes in parallel. Even focussing on RFID data capture, this only seems to have been achieved for EPCglobal and ISO RFID object identifiers. Systems like Near Field Communication and Ubiquitous Codes appear to be inoperable with the EPC/ISO RFID data capture systems.

Achieving resolver protocols that can accommodate the different identifier codes and support the multifarious domains that use a particular identifier code. The EPCglobal ONS is almost a clone of aspects of DNS, whereas the DOI / Handle uses a significantly different protocol but the computer network. The Ubiquitous Code system offers parallel functions, but through the use of the TRON engine. The biggest challenge is finding a solution for the ISO RFID OID system that could support multiple application domains.

3.3.13 SWOT analysis – Identification Coding

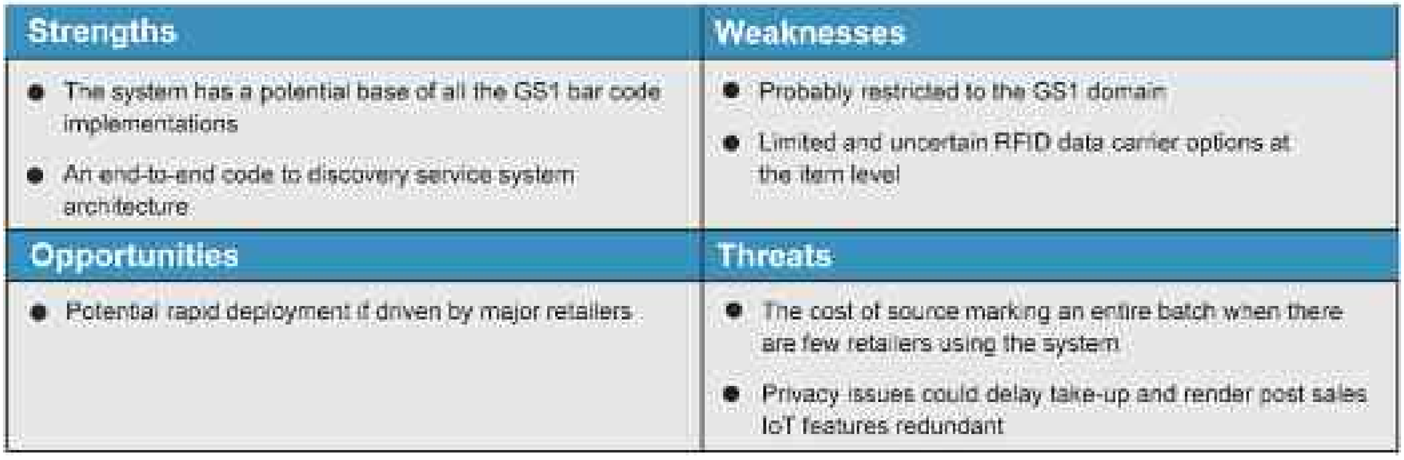
It is probably more appropriate to provide a SWOT analysis for each of the identifier codes discussed above.

RFID Object Identifiers



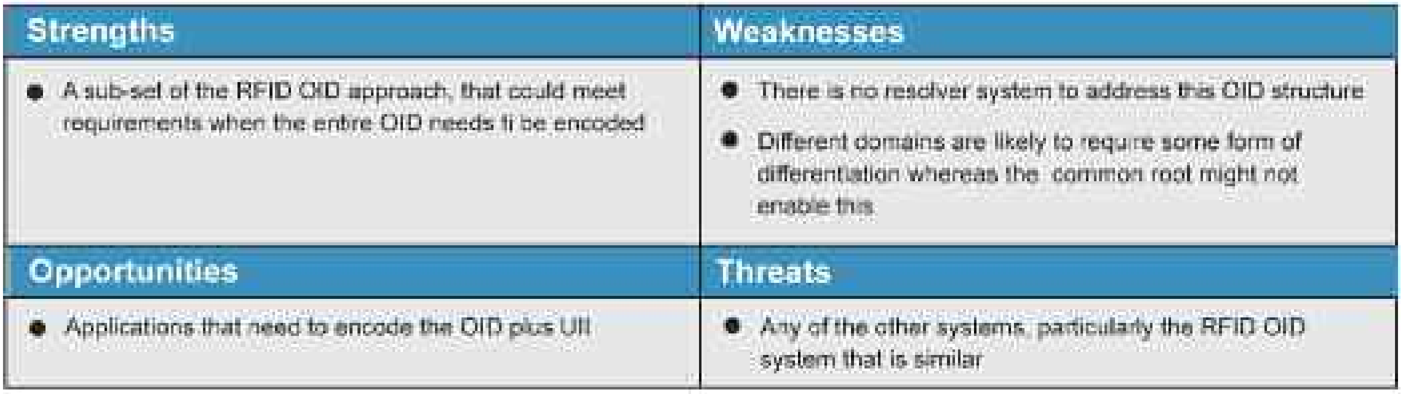
Strengths	Weaknesses
● An established code structure that can accommodate legacy systems that differ from GS1	● There is no resolver system to address the different OID structures ● Very low level PR – there is no marketing budget for an ISO standard
Opportunities	**Threats**
● Has the potential to address any type of application as by IATA baggage handling by accepting the domains code structure	● Any of the other systems

EPCglobal



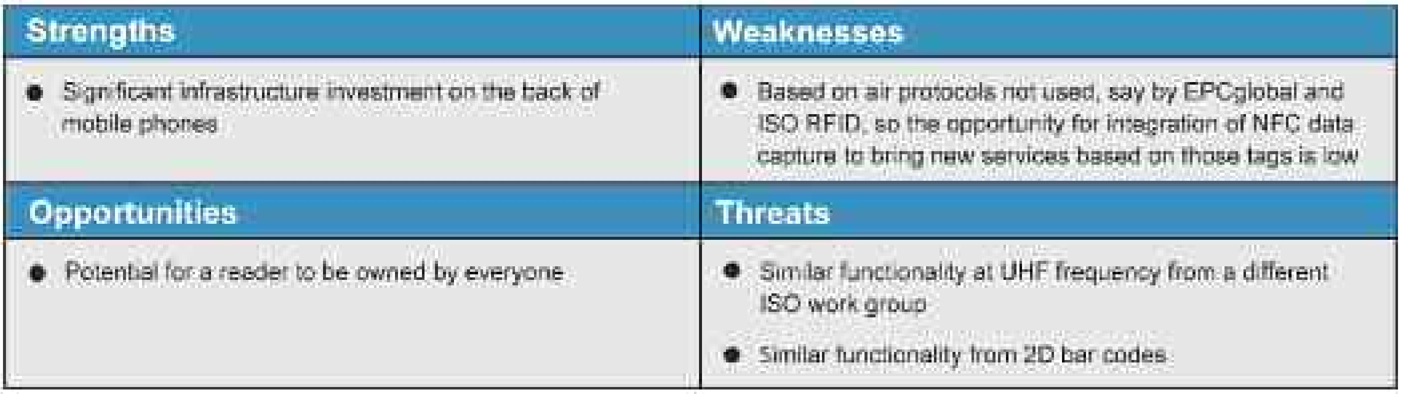
Strengths	Weaknesses
● The system has a potential base of all the GS1 bar code implementations ● An end-to-end code to discovery service system architecture	● Probably restricted to the GS1 domain ● Limited and uncertain RFID data carrier options at the item level
Opportunities	**Threats**
● Potential rapid deployment if driven by major retailers	● The cost of source marking an entire batch when there are few retailers using the system ● Privacy issues could delay take-up and render post sales IoT features redundant

Short-OID



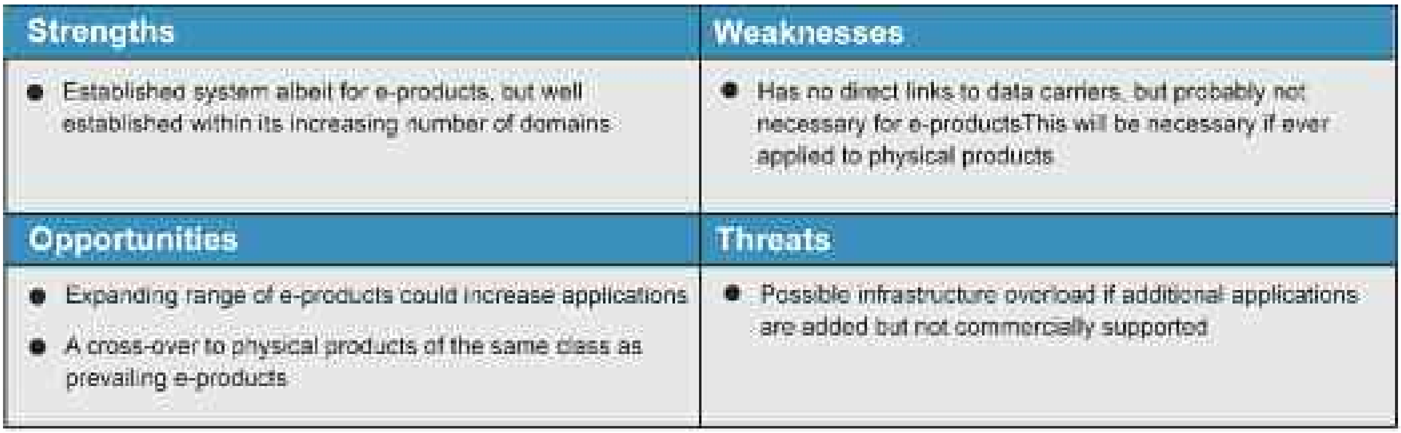
Strengths	Weaknesses
● A sub-set of the RFID OID approach, that could meet requirements when the entire OID needs fi be encoded	● There is no resolver system to address this OID structure ● Different domains are likely to require some form of differentiation whereas the common root might not enable this
Opportunities	**Threats**
● Applications that need to encode the OID plus UII	● Any of the other systems, particularly the RFID OID system that is similar

Near Field Communications Forum



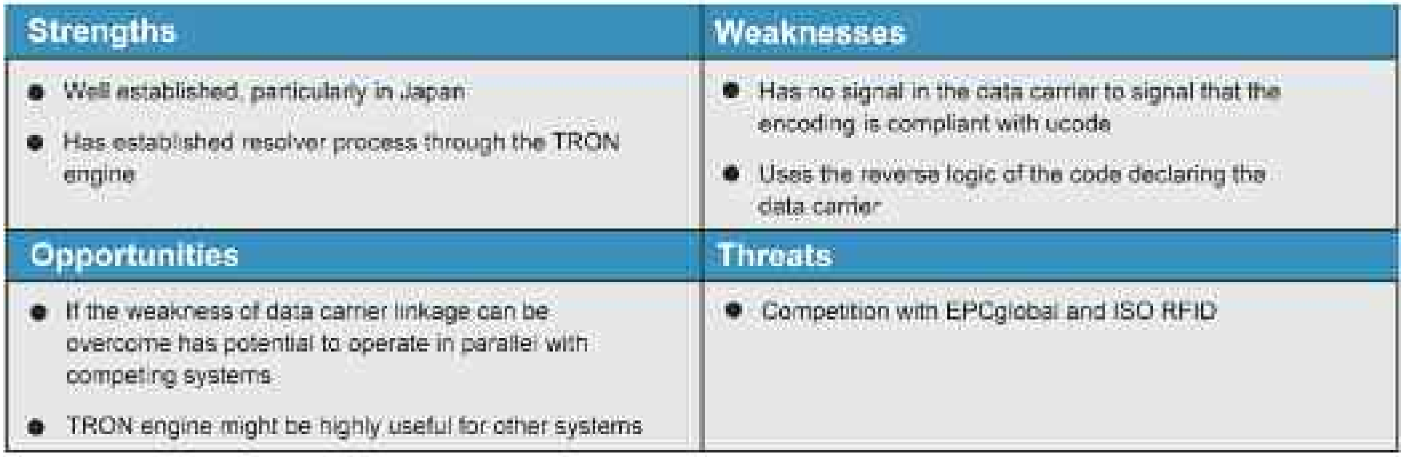
Strengths	Weaknesses
● Significant infrastructure investment on the back of mobile phones	● Based on air protocols not used, say by EPCglobal and ISO RFID, so the opportunity for integration of NFC data capture to bring new services based on those tags is low
Opportunities	**Threats**
● Potential for a reader to be owned by everyone	● Similar functionality at UHF frequency from a different ISO work group ● Similar functionality from 2D bar codes

Handle and DOI



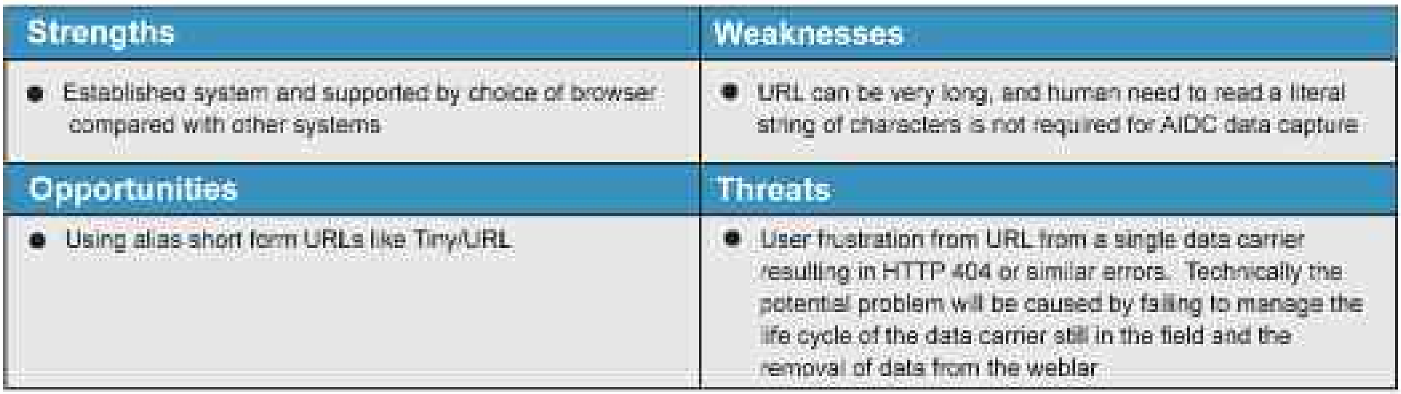
Strengths	Weaknesses
● Established system albeit for e-products, but well established within its increasing number of domains	● Has no direct links to data carriers, but probably not necessary for e-productsThis will be necessary if ever applied to physical products
Opportunities	**Threats**
● Expanding range of e-products could increase applications ● A cross-over to physical products of the same class as prevailing e-products	● Possible infrastructure overload if additional applications are added but not commercially supported

Ubiquitous Code



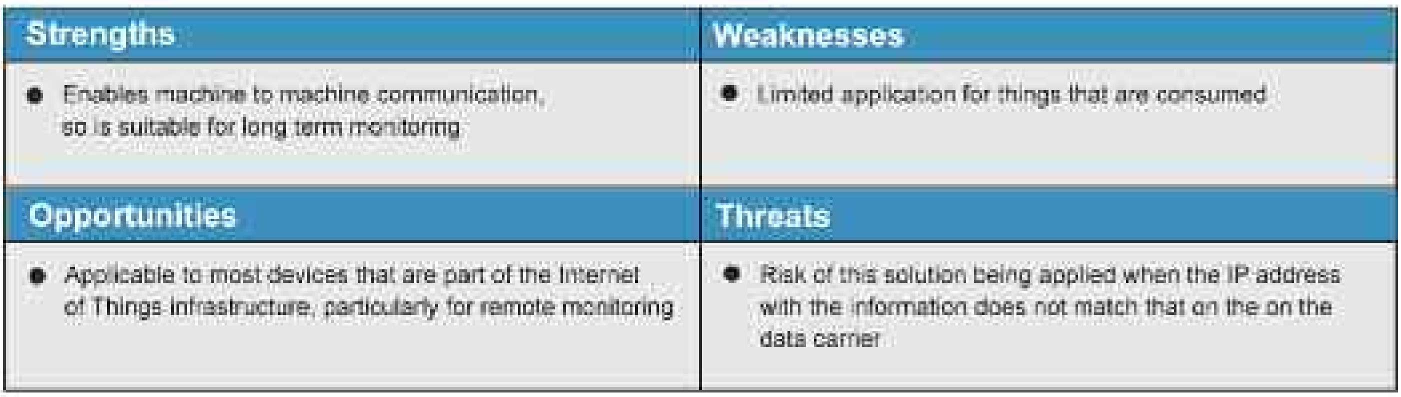
Strengths	Weaknesses
● Well established, particularly in Japan ● Has established resolver process through the TRON engine	● Has no signal in the data carrier to signal that the encoding is compliant with ucode ● Uses the reverse logic of the code declaring the data carrier
Opportunities	**Threats**
● If the weakness of data carrier linkage can be overcome has potential to operate in parallel with competing systems ● TRON engine might be highly useful for other systems	● Competition with EPCglobal and ISO RFID

URL as an Identifier



Strengths	Weaknesses
● Established system and supported by choice of browser compared with other systems	● URL can be very long, and human need to read a literal string of characters is not required for AIDC data capture
Opportunities	**Threats**
● Using alias short form URLs like TinyURL	● User frustration from URL from a single data carrier resulting in HTTP 404 or similar errors. Technically the potential problem will be caused by failing to manage the life cycle of the data carrier still in the field and the removal of data from the weblar

IP address as an Identifier



Strengths	Weaknesses
● Enables machine to machine communication, so is suitable for long term monitoring	● Limited application for things that are consumed
Opportunities	**Threats**
● Applicable to most devices that are part of the Internet of Things infrastructure, particularly for remote monitoring	● Risk of this solution being applied when the IP address with the information does not match that on the on the data carrier

3.4 Realising IoT within Regulations using Standards

The RFID aspect of the IoT, and some aspects of background communications networks rely on the use of radio. Radio is controlled by National Regulations, and these vary from country to country either in the bands allocated or the conditions of use of such bands.

The EU, working with ETSI, has done much to harmonise the use of bands in Europe. The availability of Standards has helped to bring this about. Globally ITU have also carried out initiatives to encourage harmonisation, and to some the availability of IEEE has also helped. However, there is no central point where these regulations are collated and made available to implementers, and implementers of IoT will be similarly affected by this lack of clarity. A central global library of these regulations, updated regularly would be of great assistance.

A useful trend of the past two decades, and particularly in Europe, is to make the implementation of regulations, particularly harmonised regulations, dependent upon operation in conformance with specified Standards. These are known as 'Harmonised Standards'. And in general 'Harmonised Standards' are those associated with regulatory control, in this case, with radio regulations. But it is important to realise that while these harmonised standards may achieve interoperability of the air interfaces, many other, non harmonised, standards need to be used to obtain interoperability of the data across the air interface.

Developments in RFID data carrier platforms and user demands mean that there is also a need to accommodate data other than a unique identifier in data carriers. This object connected data capability may be accompanied by additional functionality and processing capability. The primary groups of RFID data carriers (tags) include passive devices with greater data capacity and both read-only and read-write capability, sensory devices and devices to support other functions such as locating and security functions.

The European Commission (2006) report "From RFID to the Internet of Things" identifies the following network-supporting communication devices:

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

RFID interrogators may be integrated into business infrastructure via input and output ports such as Ethernet (RJ45), serial (RS232), Wi-Fi (802.11), USB and other public or proprietary standards. These ports allow the interrogator to send and receive information and instructions to and from current infrastructure. RFID interrogators are usually linked to a host information management system and can either be fixed or handheld. Mobile devices are available with a wide range of form factors, data storage and processing capability. Some may have on-board processing capabilities while others simply allow capture, storage and data exchange capabilities. The RFID component of the mobiles may be in the form of an attachment or integral to the device depending upon the product.

Wireless platforms for radio communication should provide an enhanced capability for RFID applications, extending reach from a few centimetres to 1000's of kilometres. These platforms contribute to the range of network structures that will form part of the IoT and allow mobile communications technologies and mobile phones to become an integral part of such a structure. Associated RFID systems exploit the user devices as tags and access points as interrogators. Integral identifiers such as MAC addresses are exploited for identification purposes. Integration is a further feature, for example as in the development of 'communication systems-based' RFID with mobile phones incorporating NFC (Near Field Communication) tags and interrogators.

Host systems handle the application needs, exploiting item-numbering schemes to facilitate the item-specific support functions and to derive and communicate appropriate responses, including those that result in physical actuation. The host systems may be interconnected and networked via wired or wireless communication channels. To achieve this degree of communications requires appropriate international standardisation of numbering, data structure, communication and interface protocols if a truly global IoT is to be achieved.

Other SRDs include alarm systems, telemetry, anti-theft devices, radio microphones and radio-based wireless local area networks (WLANs). Generally speaking they are characterised by short range, uni-directional or bi-directional communication operating at low power levels, typically below 500mW and as low as 1mW. However, channel allocations with 2W (erp) operation levels have also been introduced in Europe for RFID systems operating at UHF carrier frequencies. Although specific regulations may vary from country-to-country there is a strong move towards harmonisation within the EU.

The manufacturers of RFID systems need to comply with the essential regulations and standards in respect of:

- Spectrum allocations and associated operating and equipment constraints
- Health and safety
- Electromagnetic compatibility
- Avoidance of interference with other spectrum users
- Compliance with national interface regulations
- Other regulations and directives that may arise from time to time concerning system usage

Electromagnetic spectrum regulations prevailing in different countries have the potential to be constraining influences upon RFID and associated network usage and performance.

The development and standardisation of open and harmonised systems usage of RFID and integrated networks requires the analysis of existing regulations and developments, including networked exploitation of RFID devices and interrogators.

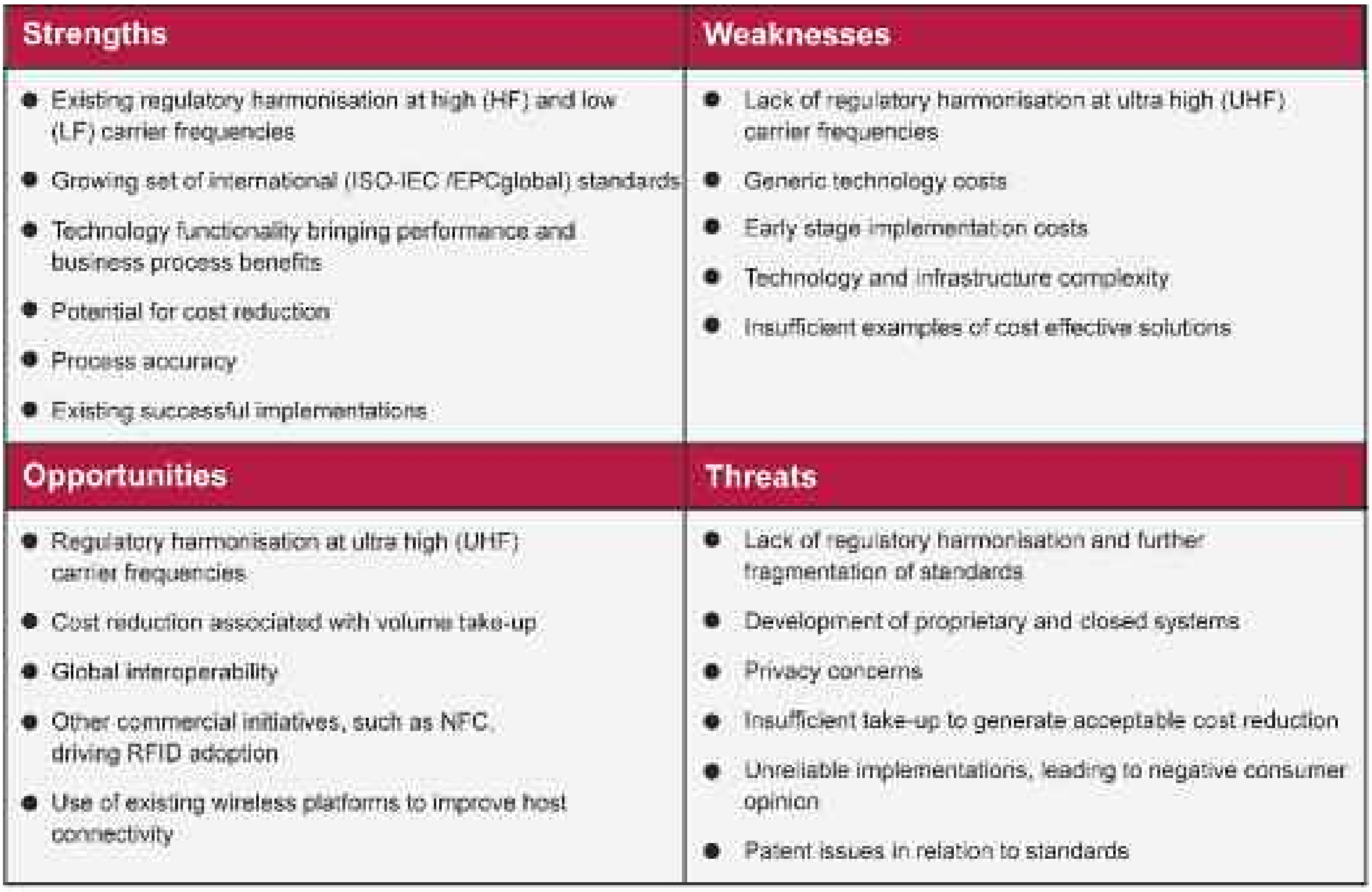
In general equipment and systems operating in the LF and HF bands use magnetic (inductive) coupling whereas systems operating above 30 MHz use propagating communication. The data rate and modulation between interrogator and tag(s) determines the occupied bandwidth and radio regulation determines the permissible emitted radio frequency power.

The use of LF and HF bands is well established and the regulatory environment is well understood and harmonised in most of the developed world. The same cannot be said of the UHF and microwave bands where there are many anomalies and in some countries a severe lack of available spectrum. Where spectrum is allocated, the regulatory requirements may restrict either the performance or utility of RFID systems.

Because LF and HF are magnetically coupled, the coupling range is relatively localised, even with high power interrogators. This minimises the possible interference that LF and HF RFID systems can cause to other non-RFID devices.

Clearly there can still be problems within the coupling range, but this is relatively contained. UHF and microwave are "problem" frequencies for RFID. In these bands interrogators and tags communicate via propagation and it is possible for a propagating RFID interrogator to transmit potentially interfering signals over a long range.

3.4.1 SWOT Analysis – Standards and Regulations



Strengths	Weaknesses
● Existing regulatory harmonisation at high (HF) and low (LF) carrier frequencies ● Growing set of international (ISO-IEC /EPCglobal) standards ● Technology functionality bringing performance and business process benefits ● Potential for cost reduction ● Process accuracy ● Existing successful implementations	● Lack of regulatory harmonisation at ultra high (UHF) carrier frequencies ● Generic technology costs ● Early stage implementation costs ● Technology and infrastructure complexity ● Insufficient examples of cost effective solutions
Opportunities	**Threats**
● Regulatory harmonisation at ultra high (UHF) carrier frequencies ● Cost reduction associated with volume take-up ● Global interoperability ● Other commercial initiatives, such as NFC, driving RFID adoption ● Use of existing wireless platforms to improve host connectivity	● Lack of regulatory harmonisation and further fragmentation of standards ● Development of proprietary and closed systems ● Privacy concerns ● Insufficient take-up to generate acceptable cost reduction ● Unreliable implementations, leading to negative consumer opinion ● Patent issues in relation to standards

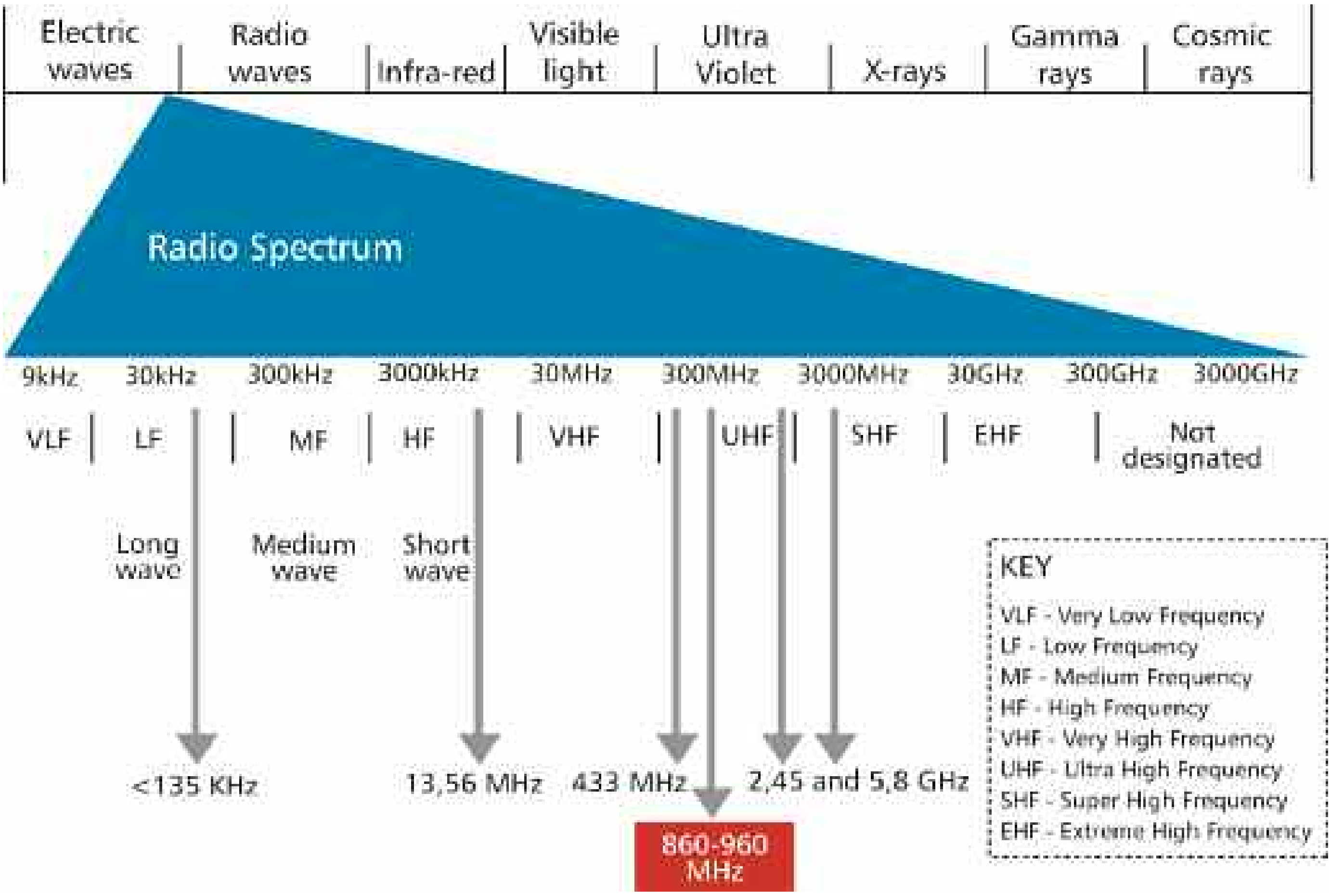
3.5 Standards and Regulations

3.5.1 Regulations

RFID systems can generally be taken to encompass any data carrier (tag) and interrogator devices (readers) that can facilitate data transfer between the data carrier and interrogator using wireless, radio frequency communication means. RFID systems generally operate in the Industrial, Scientific and Medical (ISM) bands.

With respect to spectrum occupancy, radio frequency ranges from 118kHz through to microwave frequencies up to 5.8GHz (exceptionally up to 25GHz) with particular bands < 135kHz, 13.56MHz, 433MHz, 860- 960MHz, 2.45GHz, 3GHz-10GHz) in accordance with regulatory controls. Some of these regulations are specifically designed to control RFID, but most are generic to control radio emissions of SRDs, but can be/are used for RFID.

RFID Radio Spectrum



The use of other parts of the EM spectrum, particularly for radio broadcast and communications usage is carefully controlled. SRDs generally operate in shared bands of the spectrum and are not permitted to interfere with other spectrum users and cannot claim protection from licensed spectrum users. It is therefore incumbent upon manufacturers of SRDs to ensure compliance and to be aware of any implications concerning potential inference from other spectrum users. In Europe SRD products must comply with the Radio and Telecommunications Terminal Equipment (R&TTE) Directive (1999) before they can be marketed within the European Community.

The International Telecommunications Union (ITU) has established frequency allocations for the so called “Industrial, Scientific and Medical” (the ISM bands). These bands are distributed throughout the radio spectrum from low frequencies (LF) up to the microwave bands. Below 50 MHz ISM bands are generally common (harmonised) throughout the world. However, in the UHF and microwave bands there is somewhat less commonality.

There are differences in band allocations between ITU Region 1 (Europe, Middle East and Africa), Region 2 (North and South America) and Region 3 (Asia and Pacific Rim countries).

There are also regional and national frequency allocations that may differ from the ITU recommendations. An example is in the high UHF band in the region of 900 MHz. The European allocation for ISM and short-range devices is 862 – 870 MHz, in North America it is 902 – 928 MHz and across Asia there a variously allocations in the above bands with other national allocations between 840 MHz and 956 MHz.

The main opportunity and challenge for regulatory harmonisation that can immediately benefit global RFID usage and, potentially, the establishment and uptake of the IOT is at UHF. There are other bands and technologies that will also be very relevant to such uptake, but factors other than just RFID usage are likely to influence the regulation of these bands. The challenge at UHF is where to get unified spectrum, plus how to address concerns of high power/spectrum saturation when considering co-existence (band sharing) with ISM use and SRDs.

There is an ETSI initiative to introduce more radio spectrum for RFID applications in the UHF band 915-921 MHz. It is being discussed by the FM WGCEPT. Such a new use of this band could help in the implementation of the IoT. (See ETSI document TR 102 649.)

If the request is finally approved, it would give the following benefits:

- **Operation at internationally accepted frequencies;**
- **Higher power (4 W erp) for better reading reliability and greater range;**
- **Faster data rates**

Some regulatory bodies have regulations regarding the co-existence of RFID applications with other unlicensed devices or incumbent services within this band. In addition, note needs to be made of the regulatory environment for mobile wireless connectivity, particularly with respect to WiFi, WiMax and UWB. Wireless platforms for radio communication should provide an enhanced capability for RFID applications.

There is a potential issue because the World Radio Council (WRC) made a resolution in 2007 that the use of telecommunications devices in ISM bands has to stop. This will include RFID. This resolution will be discussed at the next WRC meeting with the possibility of the subject being tabled for a decision on action at the 2011 conference.

The current ITU-R Radio Regulations (2008) state that ISM bands may not be used for telecommunications. One interpretation of these guidelines could cause very real problems. There is an expectation that a frequency be set-aside for SRDs (including RFID) outside of the ISM bands. There are meetings in 2009 and 2010 that will work on these issues and the outcomes of these deliberations will presented to the WRC-11 conference. The FCC, while not bound to agree to a WRC decision, will be unlikely to work against ITU and the WRC after a ruling is made.

3.5.2 Standards

'Harmonised Standards' may enable the interoperability of air interface communications, and require the application and adherence to such 'Harmonised Standards' to achieve compliance with supporting regulations. However, attention has been focused upon regulatory issues associated with the edge technology layer, the layer involving the interaction between a data carrier and interrogator. This is the layer where the key RFID-specific regulatory issues are most prominent. Interrogator-to-host data transfer typically utilises existing infrastructures and protocols used by other systems, and therefore become instances of use of more generic standards.

Standardisation provides a means for different users and manufacturers to produce RFID systems that are globally operable. The International Organisation for Standardisation (ISO), has published the 18000 family of RFID standards covering a range of frequency bands and application requirements. EAN International and UCC established EPCglobal to produce a standard for consumer product tagging. RFID data tags and associated systems are generally considered to be part of a general category of radio-based short range devices (SRDs) designed to operate in regions of the electromagnetic (EM) spectrum that do not necessarily require operating licenses and do not incur operating fees. Being licence-free they invariably share the spectrum allocation with other spectrum users and without the benefits of protection afforded to licensed users of EM spectrum.

As a result of the analysis and data collection undertaken within CASAGRAS the following recommendations are made with respect to regulatory issues associated with the edge technology layer.

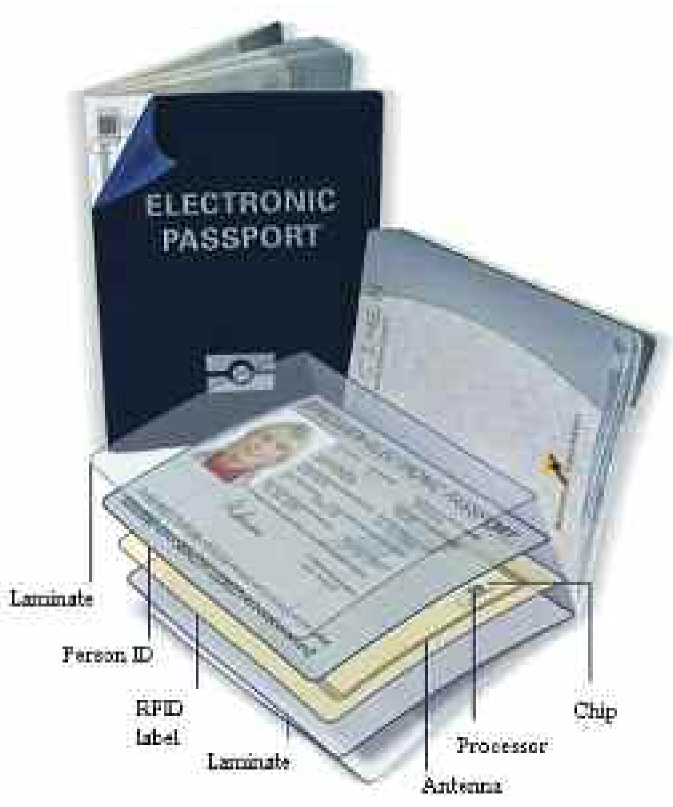
- **Promote the widespread adoption of ETSI EN 302 208-2 V1.2.1 (4 Channel Plan).**
- **Support the ETSI initiative to establish more radio spectrum for RFID applications in the UHF band 915-921 MHz. See ETSI document TR 102**
- **Make representations to the WRC to ratify the validity of using telecommunications devices (including RFID) in ISM bands. Although not obligatory under the R&TTE Dir.**
- **Support the categorisation of (passive) RFID data carriers and associated systems as SRDs.**
- **Support global harmonisation of the UHF RFID band.**
- **Support global harmonisation of the UHF ISM bands.**
- **Monitor plans and/or proposals for spectrum re-farming (Band Re-planning) elsewhere in the world.**
- **Monitor the justification being used by countries considering exclusive bands for RFID use.**
- **Monitor the regulatory environment for mobile wireless connectivity, particularly with respect to WiFi, WiMax and UWB.**
- **Monitor the take up of NFC devices and the impact on RFID usage.**
- **Re: Health & Safety concerns – Monitor work being undertaken on non-ionising radiation safety concerns or regulatory proposals concerning RF output power in the frequency band of interest.**
- **In the absence of useful/relevant Health & Safety information being available, consider funding relevant studies.**
- **The timescales for implementing the above recommendations are immediate, with an objective of influencing policy over the next 3-5 years.**

3.6 Privacy and Security

On a separate but related matter, detailed analysis of privacy and security issues associated with the use and deployment of RFID technologies is clearly needed, especially as the vision of the IoT becomes a reality. Privacy is a most important aspect which concerns the rights of the individual and must be taken most seriously in IoT applications. However, fears about loss of privacy caused by RFID frequently go well beyond the capabilities of the technology, or relate to downstream use of data, which is already well protected by legislation, and no different from the protection required for data captured by bar code or input using a keyboard. Three general principles can be applied to help address concerns about privacy in existing and new applications of RFID.

These are the principles of:

- Technology neutrality;
- Privacy and security as primary design constraints;
- Consumer transparency



RFID technology in and of itself does not impose threats to privacy. Rather, privacy breaches occur when RFID, like any technology, is deployed in a way that is not consistent with good management practices that foster sound privacy protection.

Privacy is not about the technology, it is about the responsible and secure management of the data or the data repositories to which an identifier points. The ePassport debate is a case in point. There must be a link between the presented token and the individual carrying the token, and preferably the validation processes should not rely on human judgement. It is not the token that one is seeking to validate in its own right; in this case one is seeking to confirm the identity of the person carrying the token, that the token is valid and that the valid token matches the person carrying it.

Users of RFID technology should address the privacy and security issues as part of the initial system design. Rather than retrofitting RFID systems to respond to these issues , it is much preferable that privacy and security is designed in from the beginning. In an ideal world there would be no secret RFID tags or readers. Use of RFID technology needs to be as transparent as possible, and consumers should know about the implementation and use of any RFID technology (including tags, readers and storage of PII) as they engage in any transaction that utilises an RFID system. At the same time, it is important to recognise that notice alone does not mitigate all concerns about privacy.

Notice alone does not, for example, justify any inappropriate data collection or sharing, and/or failure to deploy appropriate security measures. Notice must be supplemented by thoughtful, robust implementation of responsible information practices. Data, once captured, whether from an RFID device, bar code, keyboard or other means of input is governed by European Directives, which are implemented through National legislation.

At the time of writing the key European Directives are :

European Data Privacy Directive Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995

European Privacy and electronic communications Directive Directive 2002/58/EC Of The European Parliament And Of The Council Of 12 July 2002

All IoT system design must take the provisions of these directives fully into account, whatever the means used to capture the data.

Application design for privacy should be seen as a necessary requirement for helping to ensure effective, credible solutions that give confidence to users and campaign groups that otherwise have concerns over the use of RFID technologies. The European Commission consultation process on RFID revealed that 86% of respondents supported the need for a "governance model that is built on transparent, fair and non-discriminatory international principles, free of commercial interest".

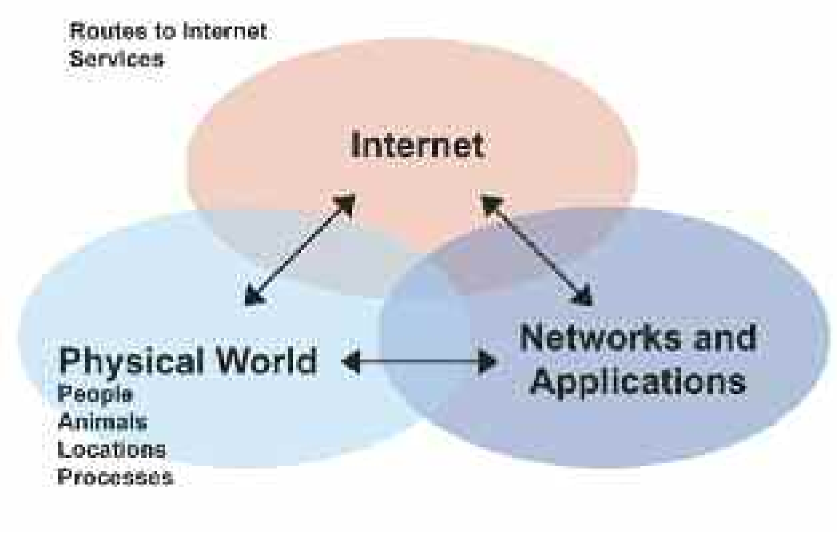
3.7 Applications and Service framework

Many of the applications being proposed for the Internet of Things, particularly in media-type publications, have more to do with technological forecasting than the attributes being proposed for the Internet of Things. Some, for example are concerned with enhancing some function, such as implantable sensory devices for medical diagnostics, rather than developments that exploit the networking and processing capabilities of an Internet-type infrastructure. Moreover, the forecasting is often fanciful in nature and without any indication of a migration path from current to future capability. While the object-associated technology is clearly of importance, in both existing and future applications, it is important in considering applications for the Internet of Things that the 'Internet' attributes are not only declared but are also justified.

The rationale for defining an application and service framework for an Internet of Things has to be one based on what is viewed as possible, since applications and services do not yet exist in any explicit tangible form. Islands of application may be identified that will clearly fit with the IoT concept but are not yet recognised within an explicit IoT infrastructure. Given the range of object-connectable data capture, network and communication technologies available for exploitation within an IoT, new applications, services and enterprise innovations are inevitable. But many of these technologies, if not all, can be applied in localized ways, without Internet or internet-type support, and achieve benefits that are radical in their impact. Indeed, these applications are characteristically those attributed to traditional AIDC application methodology.

So the question arises as to what characterizes an IoT application or service. Ostensibly, it is features such as connectivity, global reach, access and coupled functionality representative of the Internet. And, whereas the Internet applications and services rely upon human-promoted communications via computers or computer-based mobile platforms such modern mobile phones, IoT applications and services will extend the capability to other platforms and human-independent functionality in its primary form. Increasingly IoT applications are also likely to be characterised by greater use of embedded processing capability and larger, more complex networks linked to other networks. Given these features the opportunity may also be seen for extending AIDC process enhancement applications to harness benefits of data acquisition, information sharing and increased functionality through IoT architecture. Indeed this is a useful starting point in developing a sector to prospective applications characterised by process enhancements along process-defined pathways. These pathways may be internal to a company, between companies, along and between nodes in supply chain, between supply chains and so forth. The between components can now be readily accommodated using mobile platforms of identification and communication. This concept of extended process functionality through IoT type structures is considered in more detail in section 3.7.2, simply because it also requires consideration in respect of ICT principles and the building of such principles to underpin IoT application methodology.

Integration with the evolving Internet is seen as an important and essential feature of the IoT, and may exploit the conventional Internet offerings such as the world wide web to link services and extend capability. For example a conventional web site might offer object-connected software support services that would be downloaded and implemented through an integral or separate IoT domain. Services may exploit direct linkage between data carrier reader and the Internet. Already camera-equipped and RFID reader-equipped mobile phones are being used to read data carriers on objects, such as posters, the IP identifiers so derived yielding access to information on particular web sites. The camera-equipped devices generally work with matrix code data carriers printed or applied to particular objects.



Other types of identifier carried in the same or different types of data carrier may be resolved to point to particular IP addresses depending upon the application software. Using appropriate IP addressing edge-implemented object-connected applications, including networked structures, may exploit Internet connections to derive application support information, share information or generate new information and knowledge.

The Internet may also be accessed indirectly through an application host or network to serve an IoT need. This is likely to involve identification resolver techniques to accommodate legacy identification systems and to facilitate appropriate routing to the Internet level for discovery and other functional requirements.

Interfacing with the physical world, through the exploitation of AIDC and other object-connected edge technologies requires consideration of the core principles involved in understanding the nature of object space and object connections and in identifying objects and in acquiring and exchanging data / information, as well as engaging in physical actuation and control functions. The latter may be conveniently referred to as object-connected ICT.

3.7.1 Object Space and Object Connections

With ‘things’ or objects being the very focus for the Internet of Things there is a foundation requirement in underpinning the concept to consider the nature of objects, their life-cycle usage or operational characteristics, and the advantages that may be gained in grouping or networking objects in various ways to satisfy identifiable functional requirements. Life-cycle in this context relates to the series of changes, handling operations and so forth that the object or objects receive over their period of existence from origin, creation or essentially the point at which they are first identified to the point of obsolescence or disposal.

The principles outlined here concerning objects are already being applied to some extent in areas such as logistics where objects may be grouped and nested within other objects (packages, containers, pallets and so forth) for storage, transport and distribution purposes. However, a more general analysis of objects is likely to reveal a more substantive and meaningful foundation for developing the Internet of Things.

Object-space is the term that is being used here to depict the almost endless range of tangible physical entities that can be regarded as objects or things. In attempting to achieve some level of categorisation as a basis for considering applications within the Internet of Things two principal categories of objects may be identified; animate and inanimate objects. Each of these categories may be sub-divided into object sub-categories that are essentially fixed in location and objects that are essentially moveable when considered in relation to the attention they receive over their respective lifecycles. Fixed and mobile categorisation has implications with respect to communication protocols and devices that are adopted in realising applications.

Within each of these categories object sizes may range from the very small to the very large (microchips to super tankers for example). While objects may be generally considered to exhibit greater complexity or component parts with increasing size, this is not always the case. A micro-chip, for example, may be considered to have comparable complexity to a super-tanker. However, the micro-chip is usually considered as a single component for functional purposes over the life-cycle of the object, while the super-tanker will be regarded as an instantiation of an item class composed of many components.

The size, complexity of form and distinguishable components, state of being, lifecycle characteristics including object spatial-temporal movements and associated derivatives, object grouping, connectivity needs feature in the principles for defining functionality in applications and services. The principles extend to the choice of different data carriers and identifiers that can be used for identifying and managing objects in both the real and virtual world of objects. The Internet of Things as defined within CASAGRAS is clearly concerned primarily with physical real world awareness; the virtual aspect can also be readily accommodated.

The object-connected categorisation of technologies presented in section 3.2, and re-presented here with a column on the outline foundations for applications and services. While generic in nature it is likely that the framework will evolve as new technology, principles and certainly standards come into being. Considered in the context of object-connected ICT the framework provides a uniting set of physical interface propositions.

Object-connected Technology Framework and foundations for applications and services design

Object - connected Technology	Categories	Interface Requirements	Standards	Inter - communication capability
Animate, natural feature technologies	Anatomical and bio-dynamic (Physiological and behavioural)	Technique- and device-specific issues	Standards required to rationalise data transfer and integration (eg with smart cards)	Unique biometric identification in human - oriented services and applications, and potentially other animate object applications Potential for integration with smart card and other AIDC technologies
Inanimate, natural feature technologies	Different categories emerging – natural and fibre-assisted techniques	Technique- and device-specific issues	Standards required	Unique identification of objects, having wide potential in anti-counterfeiting applications and security and financial services. Potential for integration with other AIDC technologies
Data carrier, simple read-only identifier technologies	Linear bar code, Two-dimensional codes, composite codes, magnetic encoding, electronic encoding including RFID	Various interface protocols available	Strongly supported by technology and interface standards	Wide range of existing and potential secondary identifier (unique and type-based) applications and services, across all sectors of industry, commerce and services
Data carrier, portable data file, read-only technologies	Two-dimensional codes, composite codes, electronic encoding including RFID	Various interface protocols available	Strongly supported by technology and interface standards	Wide range of existing and potential secondary identifier (unique and type-based) applications and services, across all sectors of industry, commerce and services
Data carrier, read-write technologies	Electronic encoding including RFID, contact and contactless smart cards	Various interface protocols available	Strongly supported by technology and interface standards	Wide range of existing and potential secondary identifier (unique and type-based) applications and services, across all sectors of industry, commerce and services – offering lower costs, extended process capability and flexibility through reuse of data carriers
Communication-based, read-write data carrier technologies	Electronic encoding, location-determining and data transfer devices	Various interface and communication protocols available – RFID, WiFi, ZigBee, Bluetooth, NFC etc	Supported by technology and interface standards	Networked communication between object-based structures a design attribute, offering prospects for networked applications from personal to international wide area applications and services
Sensor-based data capture technologies	Electronic based platforms for wired and wireless capture and communications	Various interface and communication protocols available	Supported by technology and interface standards – others, including RFID-based standards, in prospect	Both single and networked communication between object-based structures a design attribute, offering prospects for networked applications from personal to international wide area applications and services
Intelligent data capture and communication technologies	Electronic, smart, decision-based functionality	Various interface and communication protocols available	Further protocols and standards required	Both single and networked functionality, offering prospects for intelligent networked applications from personal to international wide area applications and services

3.7.2 IoT and Internet Applications and Services

In considering applications and services within an Internet of Things it is important to distinguish solutions that clearly depend upon Internet-type functionality as distinct from localised solutions exploiting conventional control and processing capabilities. Given the nature of object space and the evolutionary diffusion of embedded processing capability into the physical world, opportunities may be seen for applications that range from personal level services, through domestic, corporate, public and city level, regional, environmental to national, European and international services and applications.

Bearing in mind the integration with the existing and evolving Internet, various types of application may be seen that exploit object and human interface communications as well as object-to-object communications. The various categories of application or service may thus be depicted as:

1. **Object-to-Internet-to- human (eg object initiated service that results in an email to a human respondent)**
2. **Human-to-Internet-to-object (eg human communicates via Internet to activate a control device in the home)**
3. **Object-to-Internet-to-object (eg object activated control service via the Internet that results in an object or systems activation, control event or information update, possibly with a human interface to allow monitoring of events)**
4. **Object-to-dedicated IoT infrastructure-to-object (eg similar to 3, but exploiting a dedicated infrastructure and domain features to support a new range of object-oriented applications and services, possibly with human interfaces as appropriate for interactive functions)**

To achieve an applications and services infrastructure for the IoT requires appropriate attention to the identifier considerations and proposals contained within section 3.4.and how they may be used to access Internet-based services and other, discovery-type, services. Within the IoT an architecture service oriented architectural (SOA) structure (see section 3.3) is likely to be used in order to realise a cooperative services facility, analogous to the world wide web.

Through use of appropriate technologies or their integration into network structures the opportunities can be seen for applications and services that extend from the personal network level through domestic, corporate and regional networks to wider and wider structures offering increasingly broader reach and functional capability.

There are many networks: in the home, in and between businesses, within the built environment in utilities and services, environmental, national and international, servicing international collaborative services in relation to the movement of goods, people and information. The range is virtually unlimited. However, there has to be a justification for linking networks to distinguish an IoT from isolated networks.

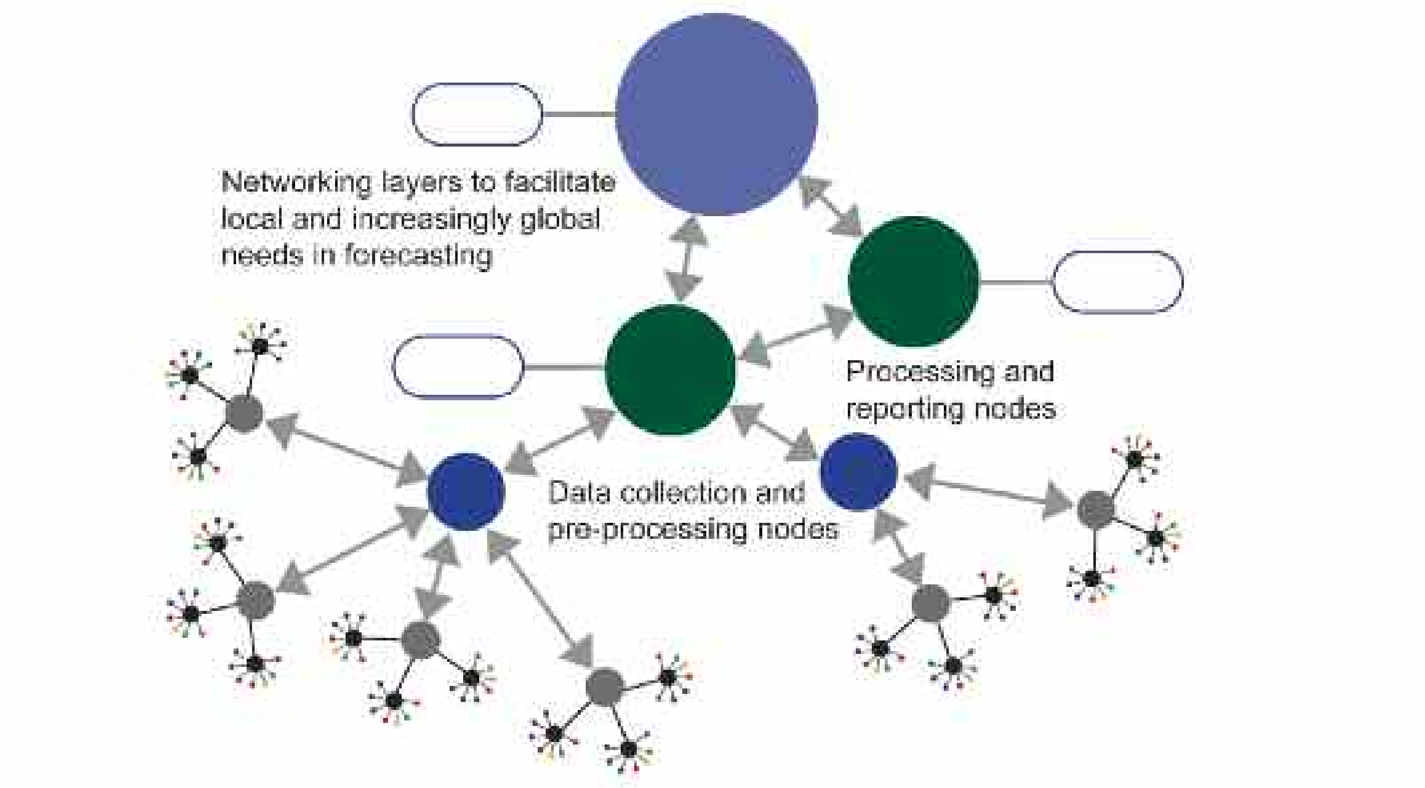
Layered Sensory and processing Networks

An immensely significant dimension to the consideration of physical objects within an Internet of Things is that of sensory capability, wherein object identification platforms are also endowed with sensors of various kinds to allow sensing of quantities relating to the object itself or the environment in which it is situated. Nodes equipped with sensors will undoubtedly constitute one of the largest if not the largest category of nodal devices for use in applications and services comprising the Internet of Things. With developments in nanotechnology and integrated electronic device designs the scene is set for revolution in sensor platforms capable of sensing and communicating sensor quantity values for a wide variety of physical, chemical and biological quantities. RFID sensor platforms are expected to feature significantly in these developments.

One example that illustrates sensory capability and the justified linking of networks is the linking of meteorological data collecting stations, for weather forecasting purposes, wherein a set of sensors constitutes a node delivering data (pressure, temperature, humidity, wind direction and speed and so forth, together with nodal location and radio-control time stamp) to a pre-processing node which them passes pre-processed data for a given region to a further processing node serving a collection of regions and so on to achieve global reach and serving global weather predictions. Each node may display sensory data and provide some rudimentary forecasting (typical of home weather stations). Two-way communications, wired or wireless, depending upon requirements, facilitates the communication of processing results, throughout the network, with particular nodes serving to provide displayed predictions. Some nodes may even serve actuators or controllers in order to effect a particular control function in response to particular conditions. For example, forecasting of local flooding prospects may automatically activate flood barriers.

With increasing granulation on the distribution of nodes the facility may be provided for more localized weather predictions, serving the needs of precision agriculture, exterior event planning, environmental management and exterior maintenance scheduling.

Layered Networking for IoT


Networking layers to facilitate local and increasingly global needs in forecasting
Processing and reporting nodes
Data collection and pre-processing nodes

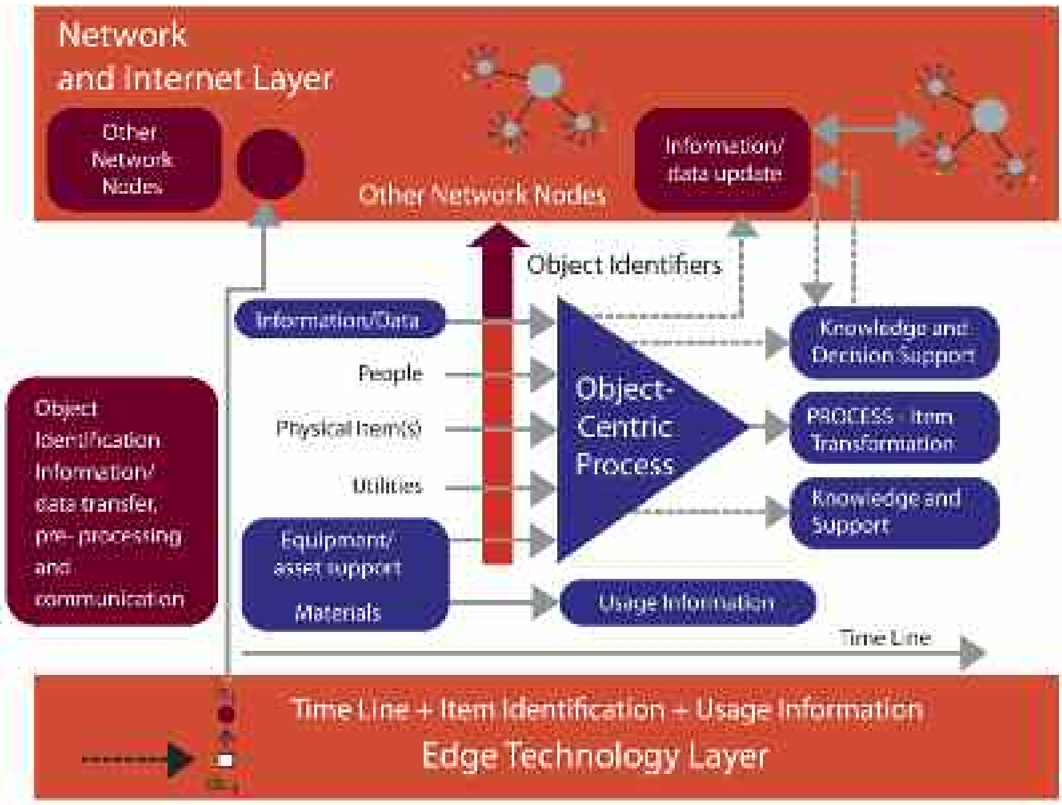
The same sort of layered network structure may be exploited for other services and applications, such as environmental monitoring and control functions, with higher level nodal reach being justified for research on wider environmental issues, such as energy and emissions studies, and knowledge-sharing purposes. Herein lies a rich opportunity for applications and service developments, impacting upon virtually all sectors of industry commerce and services as well as domestic support applications.

In considering the object-connected technologies in relation to both applications and services it is also necessary to consider the life-cycle characteristics. They comprise the totality of events and data handling activities throughout the history and processing of the object, some of which may be planned and some incidental. It also includes the instances of actual connectivity within a networked or other system-supported infrastructure. It is unlikely that objects within such structures or indeed within the wider Internet of Things will be available for connection on-demand; their timely presentation to a reader will often determine the time and the period for which they are connected. Moreover, vagaries or uncertainties in connection will, in certain circumstances, demand local or object-connected caching of data and synchronisation on achieving connectivity.

Extended Process Functionality, Pathways and Layered Networks

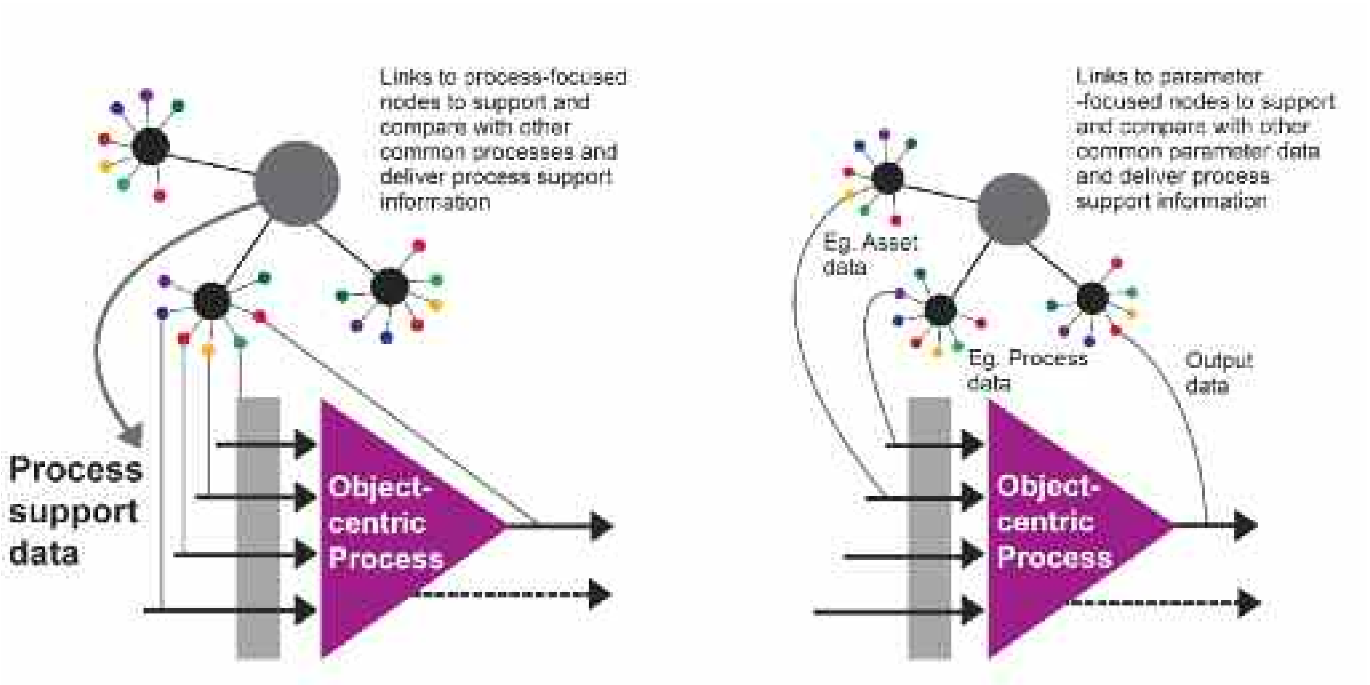
A grouping principle for objects or things that is particularly relevant to the structuring of applications and services within an IoT concerns the fundamental nature of processes, be they in industry, commerce or services, and extends to the domestic environment. Processes invariably involve a range of object types that can be conveniently grouped into people, assets, materials, utilities, locations, data and information, the latter being in either physical or virtual form. Process-based identification of these grouped entities may be exploited to achieve a range of object-linked benefits, particularly when handled through background networking structures and applied along process-linked pathways. This process-based multiple-identification approach is conveniently referred to as extended process functionality (EPF), described in more detail below as part of underpinning object-connected ICT.

Extended process functionality (EPF) exploits the use of multiple-identification for distinguishing and managing ‘things’ or objects in business and other processes, with background functionality involving the grouping and automatic management of like objects and associated information identified through their carrier identifiers. Processes invariably involve a range of physically distinguishable input components in addition to some primary input entity upon which the process operates to achieve a particular output. Thus, in a manufacturing process, for example, the primary input to a machining process may be a metal cylinder that is then machined to yield a particular component. The process requires a range of support inputs to achieve the required output and can include, for example, materials (lubricating oil), assets (machine and tools), utilities (power source) and operators (machinist).



By identifying these process inputs, and linking to date-stamp and other time-line information, the prospect is the presented for generating and exploiting background functions relating to business activity and development and can include, for example, automatic generation of management support information, materials and asset usage statistics, information for asset maintenance and, through appropriate networking, derive, share or process information. Information can constitute a very significant component in both the input and output of a process and again the use of identifiers can assist in making more effective use of information and the way in which it is managed.

The background processing of identifiers and associated information may be achieved by exploiting nodes and processing hubs. In this respect the process inputs and output can be viewed as equivalent to the sensor feeding nodes in the layered networking example illustrated on previous page.

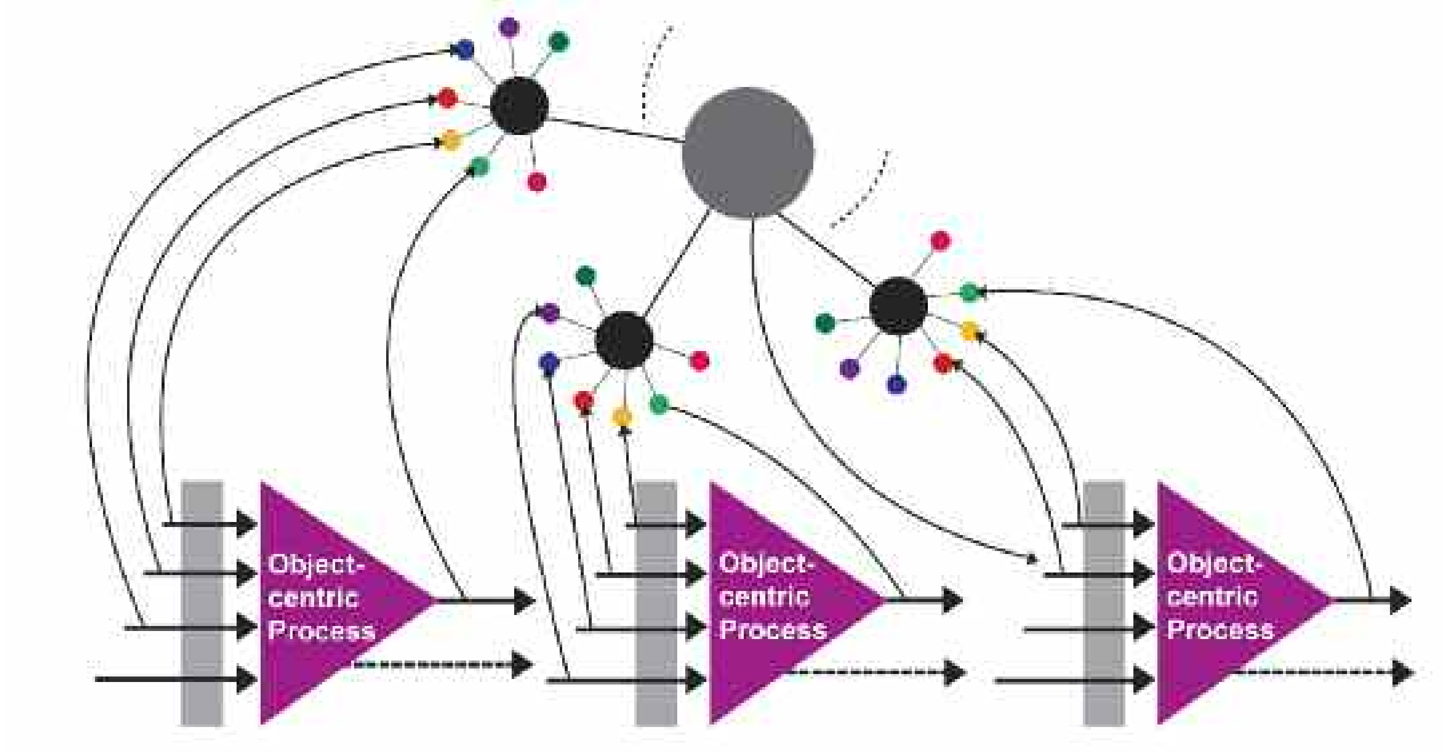

Links to process-focused nodes to support and compare with other common processes and deliver process support information
Process support data
Object-centric Process
Links to parameter -focused nodes to support and compare with other common parameter data and deliver process support information
Eg. Asset data
Eg. Process data
Output data
Object-centric Process

Thus, in the example above materials identifiers and associated information (possibly acquired from other nodes) may be fed to processing hubs along with similar information from other process points, the pooled data being used to automatically derive status information on available materials, materials usage statistics, re-ordering information and automatic re-ordering events, information for process development and so forth.

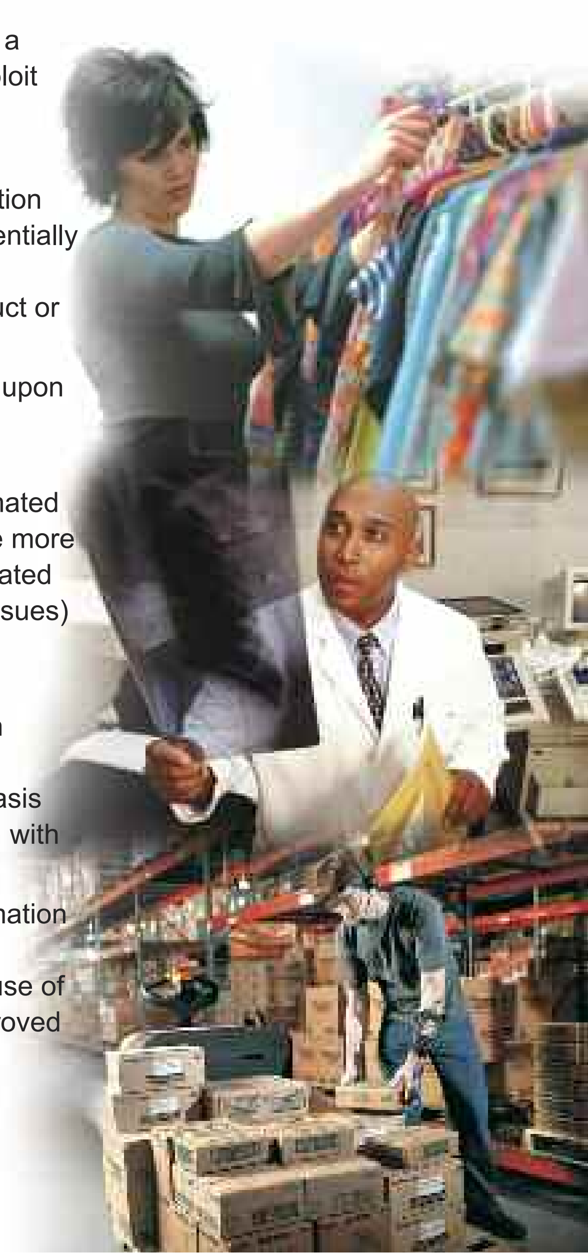
While such functions are not entirely new the extended process functionality allows scalability of functions, deriving, for example, industry level statistics and 'number crunching' analyses at levels that could not be considered at more local levels. The value of such 'number crunching' and associated data mining has been demonstrated [9] in a number of application areas such as healthcare, evidence-based medicine, legal and a commercial decision making, environmental management and management of common pooled resources, to name but a few.

By considering common pathway structures determined by interlinked processes or nodal points in supply chains with respect to this background layering and communications capability still further potential can be seen for IoT applications and services, wherein information and knowledge can be accessed, transferred and or shared to achieve greater functionality.
Using this capability, applications may be considered for a wide range of commercial and industrial sectors that exploit both intranet and Internet structures, including:

[9] Ayres, I (2007) Super Crunchers – How anything can be predicted, John Murray (Publishers).



Using this capability, applications may be considered for a wide range of commercial and industrial sectors that exploit both intranet and Internet structures, including:



Manufacturing and Production – For example, production line support and auto-synchronization of distributed, potentially global, production feasibilities where sub-assemblies or components are being produced to satisfy a target product or products being assembled at a different location.

Assembly – For example automated assembly drawing upon components and sub-assemblies being produced and delivered from distributed, potentially global, facilities.

Supply chain logistics – For example, exploiting automated background data, information and knowledge to facilitate more efficient and effective logistical function, including automated responses to traceability (including cross-supply chain issues) demands and problems.

Retail – For example, exploiting automatic background information gathering (potentially global) and analysis on products and customer preferences, including costs, availability, characteristics, warnings and so forth as a basis for enhancing procurement, decision support, interaction with suppliers and enhanced services to customers.

Healthcare – For example, exploiting background information gathering and data analyses to improve patient pathway process and practitioner support (including access and use of evidenced based medicine) healthcare support and improved patient care

Hotel and leisure - For example, enhanced process support to gather information on materials and other resources supporting hotel and leisure services functionality and indicators of performance.

Forensics – For example, exploiting background systems for enhancing chain of custody for evidence from scene of crime to court-room and automated gathering of information to facilitate enhanced analysis of evidence.

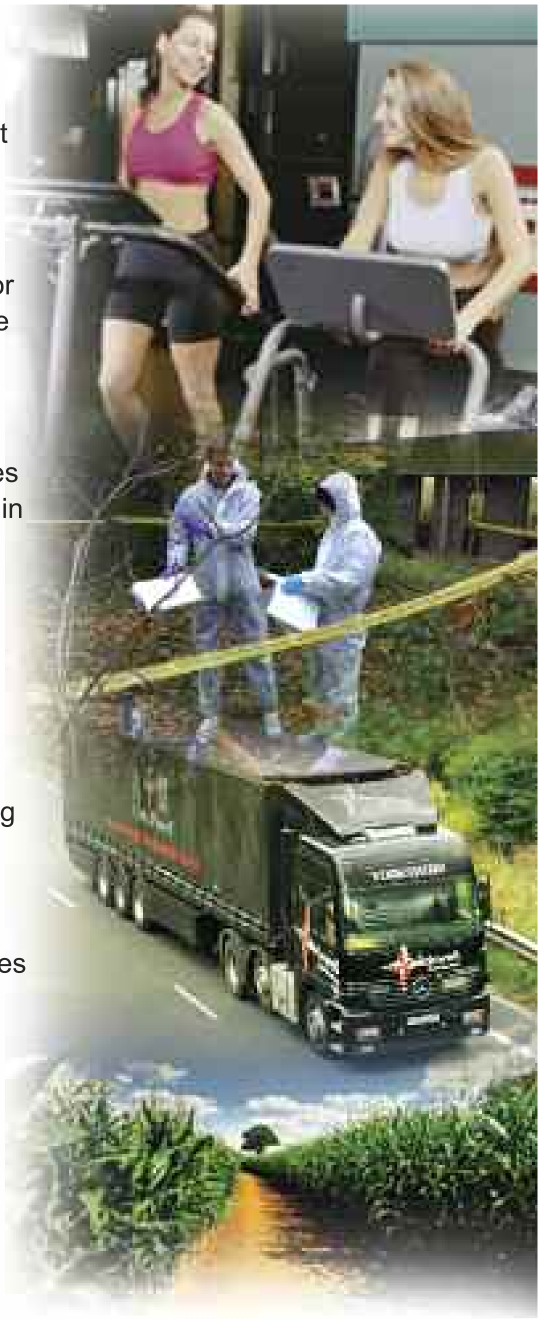
Transport and distribution - For example, enhancing the information base and processing to support dynamic changes in transport allocation and distribution schedules and routes in response to real-time factors impacting upon transport and distribution performance.

Construction - For example, exploiting background automated services for design support, including IoT structures and services being designed in to serve in enhancing automated functionality and linkage with other services serving the built environment.

Field maintenance - For example, automated data gathering from network sensory systems as a basis for planned maintenance and automated fault handling.

Precision agriculture - For example, exploiting evidence-based services for developing precision agricultural processes and procedures, automated data gathering and background processing based upon shared algorithms and performance assessment.

Environmental management - For example, exploiting networked data gathering analysis and use in managing environmental issues such as flood prevention through automated activation of flood barriers.



The list goes on. The challenge is to position the principles into an appropriate methodology for IoT applications and service design and development and to apply them to the various sectors of industry, commerce and services.

Up to now the attention has been directed to the sensory and process-support possibilities that could exploit an IoT structure. Services and access to services is another important functional part of the framework. As indicated earlier the service oriented architecture (SOA) is likely to feature significantly in IoT developments. These services may be designed to support a range of domestic, public and commercial needs and accessed through appropriate nodes either through intervention or through automated nodal structures in response to application or service needs.

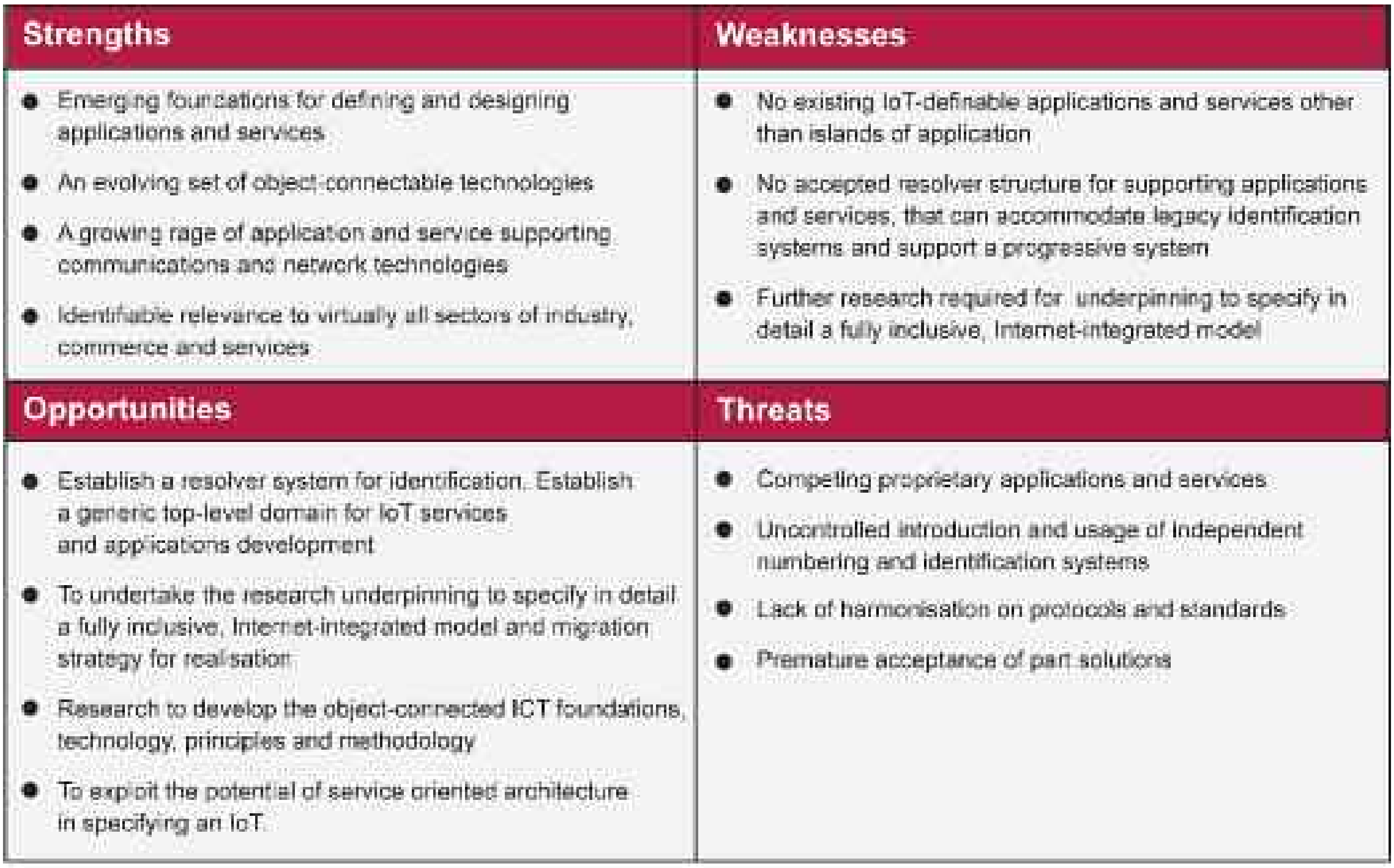
The scope for applications is almost limitless and given an ‘Internet' infrastructure that supports independent cooperative service developments the prospect is presented for on-going application growth in which innovation and enterprise are prominent features.

Simply on the basis of these key features, including object-space considerations, an effective framework can be seen to be emerging as a foundation component for the Internet of Things. The work is clearly required to define, extend and exploit such a framework. The need too can be seen for underpinning this framework with object-connected ICT principles.

3.7.3 Object-connected ICT

Object-connected ICT is essentially concerned with the positioning of automatic identification and data capture (AIDC) and IoT support principles within mainstream ICT. Its relevance to the IoT concept is fundamental, as it deals with the principles of identification and of carrying and transferring data / information between objects and object-connected devices. Outline principles are presented in Annex A – An Introduction to Object-connected ICT. By extending and attending to these principles in the context of processes and procedures and IoT capabilities and applications and services methodology can be developed that draws upon the attributes appropriate to needs and thus provide a foundational dimension to design.

3.7.4 SWOT Analysis - Applications and Service framework



Strengths	Weaknesses
● Emerging foundations for defining and designing applications and services ● An evolving set of object-connectable technologies ● A growing rage of application and service supporting communications and network technologies ● Identifiable relevance to virtually all sectors of industry, commerce and services	● No existing IoT-definable applications and services other than islands of application ● No accepted resolver structure for supporting applications and services, that can accommodate legacy identification systems and support a progressive system ● Further research required for underpinning to specify in detail a fully inclusive, Internet-integrated model
Opportunities	**Threats**
● Establish a resolver system for identification. Establish a generic top-level domain for IoT services and applications development ● To undertake the research underpinning to specify in detail a fully inclusive, Internet-integrated model and migration strategy for realisation ● Research to develop the object-connected ICT foundations, technology, principles and methodology ● To exploit the potential of service oriented architecture in specifying an IoT	● Competing proprietary applications and services ● Uncontrolled introduction and usage of independent numbering and identification systems ● Lack of harmonisation on protocols and standards ● Premature acceptance of part solutions

3.8 Structure and Governance for the Internet of Things

Structure and associated governance for the Internet of Things presents an important set of demands requiring international cooperation to deal with them. Lessons learnt from the developments in the Internet can provide a valuable pointers to how it might be achieved and without the problems encountered fort he Internet itself.

3.8.1 Lessons in Governance from the Internet

The evolving structure of the Internet brought with it the need for governance. The phenomenal growth of the world wide web in the early 1990’s and the subsequent integration of the Internet as a vital part of the economy and society led to a United Nations call for a World Summit of the Information Society (WSIS) directed at discussing the governance of the Internet as a global critical infrastructure,[10] culminating in the Working Group of Internet Governance (WGIG) and the Internet Governance Forum (IGF) which continues to promote discussions on the Internet. The WGIG provided a working definition for Internet governance, stating:

[10] Benhamou, B (2007) A European Governance Perspective on the Object Naming Service, Proceedings of the Portuguese EU Presidency conference on RFID: The next step to The Internet of Things.

"Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision making procedures, and programmes that shape the evolution and the use of the Internet. It should be made clear however, that Internet governance includes more than Internet names and addresses, issues dealt with by the Internet Corporation for Assigned Names and Numbers (ICANN): it also includes other significant public policy issues, such as critical Internet resources, the security and safety of the Internet, and developmental aspects and issues pertaining to the use of the Internet" (WGIG 2005).

The WGIG is an international body comprising members from government, industry, civil society and academe (research).

In recognising three stakeholder groups, government, private sector and civil society, WGIG suggested a division in roles for these stakeholder groups wherein:

Government - should create an environment for encouraging developments in ICT and develop, as appropriate, laws, regulations and standards, foster the exchange of best practices and engage in oversight functions.

Private sector – to promote industry self regulation and the exchange of best practices, develop policy proposals, guidelines and tools for policy makers and participate in national law making and foster innovation through its own research and development.

Civil society – to mobilize and engage in democratic and policy processes, network building and consider other views.

WGIG has also concluded that:

"No single government should have a pre-eminent role in relation to international Internet governance and that all relevant stakeholders should be involved in a multilateral, democratic and transparent way".

The Internet itself continues to need the guidance and direction of the IGF and through its deliberations will impact the conceptual approach that governments will take concerning the evolution of the Internet. Governments will invariably draw upon the IGF concepts in developing policy, law and controls within their jurisdiction. It is therefore reasonable that they will also draw upon such concepts in seeking a governance platform for the Internet of Things. This may be considered even more so when viewing the Internet of Things as an integration with the existing and evolving Internet. The global nature of the exercise demands an international, IGF-linked, platform structuring governance platform for the Internet of Things.

A range of issues will need to be accommodated in realising such a platform. The European Commission consultation process on RFID revealed that 86% of respondents supported the need for a "governance model that is built on transparent, fair and non-discriminatory international principles, free of commercial interest". While the core of the Internet, the governance structure, has not been subject to legislation, countries around the world, and within Europe, have introduced laws to ensure that Internet usage does not conflict with national laws and international rights and conforms to the norms and values of societies in general.

Issues of legislation will undoubtedly arise with respect to the Internet of Things, particularly where concerns arise that are of a privacy and security nature. With respect to RFID concerns have been expressed over openness and neutrality of database structure that are used to hold unique identifiers. This is also of direct relevance to the Internet of Things and global coding. Ethical and secure systems management is required with processes that are interoperable and non-discriminatory.[11]

[11] Wolfram, G et al, (2008) "The RFID Roadmap: The Next Steps for Europe", Springer.

3.8.2 Governance for the Internet of Things

These considerations provide lessons for considering the governance requirements for the Internet of Things.

With the scale data traffic being proposed for the Internet of Things and the associated prospect of an emerging cooperative service infrastructure that could possibly emulate the growth potential of the world wide web public policy issues are likely to present significant governance considerations for which no one country could be seen to have authority. Social and economic dependence points to the need for a regional based approach. Benhamou views the Internet of Things as an emergent critical resource and advocates the need for different countries and regions to progress work on different options to meet the governance needs.

In view of the latent requirement for integrating the Internet of Things with that of the Internet it is important that proposals for governance and other issues are considered in cooperation with relevant authorities and organisations involved with parallel developments of the Internet. Within Europe the European Future Internet Assembly is an example of such an organisation in which one of its aims is to develop the tools and approaches harnessing the potential of the Internet of Things.

A further aspect of governance requiring attention is the need to consider whether a registration authority is required for identifiers and the management of a global scheme for resolving them.

All this begs the question as to whether the Internet of Things should be governed separately from the Internet or as part of the Internet governance. This is a question requiring further research and consideration.

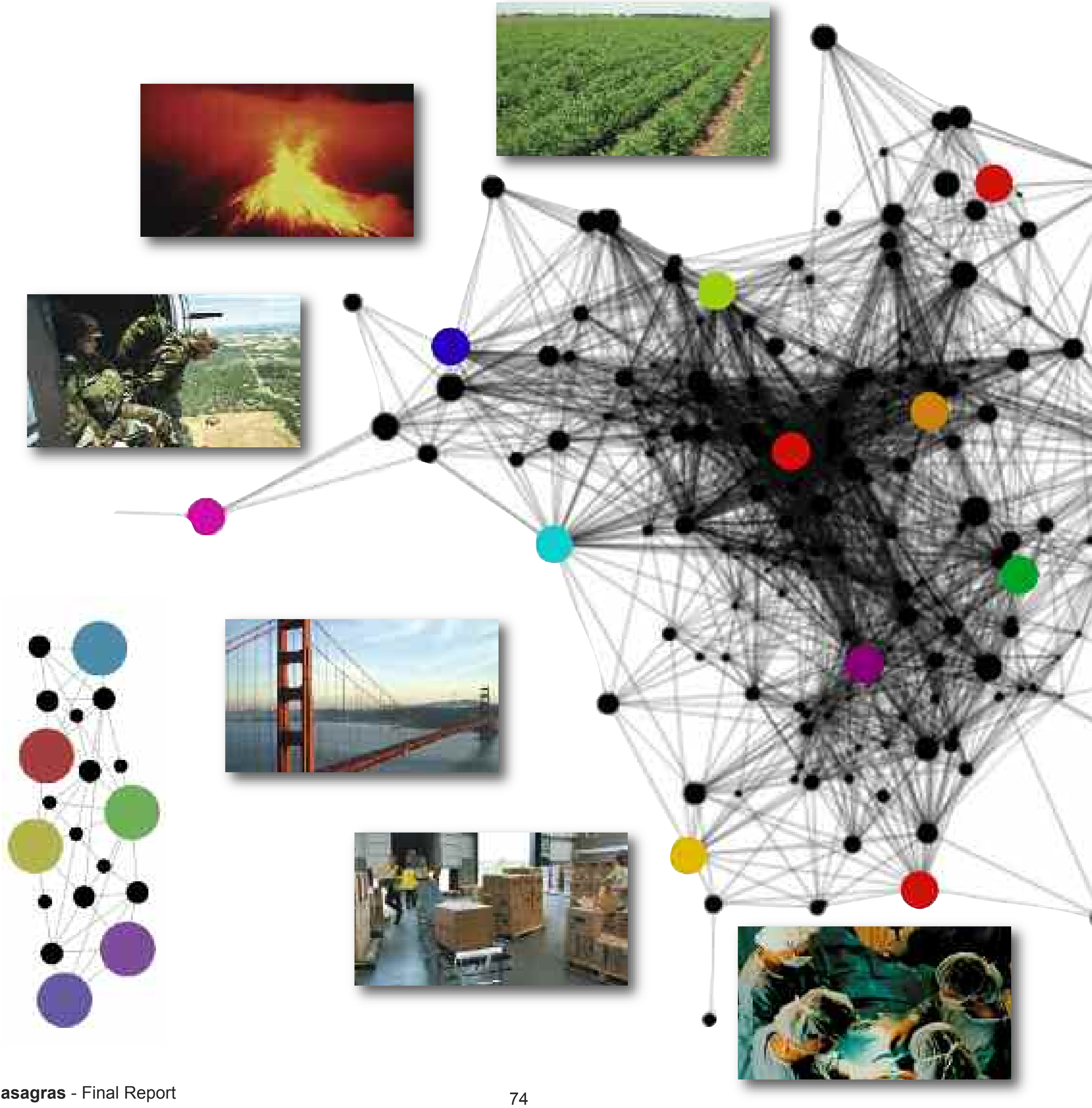
Given the nature and status of these disparate considerations the obvious recommendations in respect of governance for the Internet of Things are:

- To establish the basis upon which the IoT developments with respect to governance will integrate with those being pursued for the Internet through the Working Group of Internet Governance (WGIG) and the Internet Governance Forum (IGF).
- To establish an international IoT Development and Governance Forum and undertake rapid research into the issues for ensuring and agreeing appropriate and effective governance, including the revenue and registration schemes that will be needed and the political framework that will be necessary to facilitate appropriate international collaboration. This should also include the respective roles of governments, private sector and civil society in shaping the policy, shared principles, norms, rules and decision making declared by WGIG with respect to governance (WGIG 2005).
- To agree through international partners an initial cooperative structure for the IoT and initiate an international programme of applications and services development, including the need for a generic top level Internet domain as a platform for research and development and as a basis for supporting a co-operative development of the IoT structure, applications, services and governance.
- To establish clear cooperative foundations with respect to privacy, security and safety, and the role of governance in developing and maintaining such foundations.

In view of the multi-dimensional nature of the governance issues the need may be seen for an overarching programme of research and development geared to accommodating all the necessary socio-economic, business and technical dimensions, including the protection of such a network against attack and abuse.

3.8.3 SWOT Analysis - Governance for the IoT

Strengths	Weaknesses
● Internet experiences to draw upon ● Large body of knowledge on governance issues	● Further research required for underpinning to specify in detail a fully inclusive, Internet-integrated model and a model for governance
Opportunities	**Threats**
● Opportunity to strengthen cooperation on governance through follow-up initiatives	● Lack of international cooperation

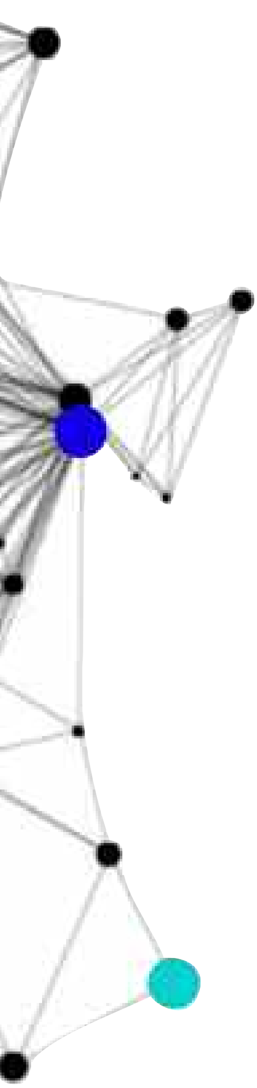


CASAGRAS
an EU Framework 7 Project

RFID Final Report

and the Inclusive Model for the
Internet of Things

4 CASAGRAS Conclusions & Recommendations



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. Our 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 is 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. We have worked 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 cooperation 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.

Other recommendations can be proposed which address the details of the SWOT analyses in this report and they can be accommodated in next step proposals. 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.

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

4.1 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.

4.1.1 The foundational features

The foundational features relate to:

1. 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.

2. 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.

3. 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.

4. Foundation principles for direct Internet connection applications and services.

5. 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.

6. Attention to harmonised and non-harmonised standards in respect of regulatory control and issues of interoperability.

7. Establishment of a central, global library of regulations regularly updated to satisfy design and support needs.

8. Attention to social and economic issues, including privacy and security of personal information and their significance with respect to IoT applications and services development.

9. Governance and the need to establish a model that is built on transparent, fair and non-discriminatory international principles, free of commercial interest.

10. 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.

4.1.2 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:

1. 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.

2. Development of the architecture and infrastructure for direct object-to-Internet applications and services.

3. Exploitation of Service Oriented Architecture (SOA) and associated network architecture for IoT services design.

4. Development of universal data appliance protocol (UDCAP) for plug-and-play exploitation of conventional AIDC technologies and other object-connectable edge devices.

5. 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.

6. 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.

7. 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.

4.1.3 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:

1. Development of standards-compliant RFID devices and readers.

2. Lower cost, lower power sensor and processing platforms, to support the design and realisation of sensory networks.

3. Development of location and positioning technologies to support IoT applications and services.

4. Development of object-connectable communications platforms, including near field communication structures.

5. Lower cost, higher performance energy harvesting and other powering techniques to support the development and exploitation of IoT wireless devices.

6. Biometric-based interfaces for IoT applications and services.

7. Privacy and security support technologies, including cryptographic devices based upon natural featureidentification (physical one-way function devices).

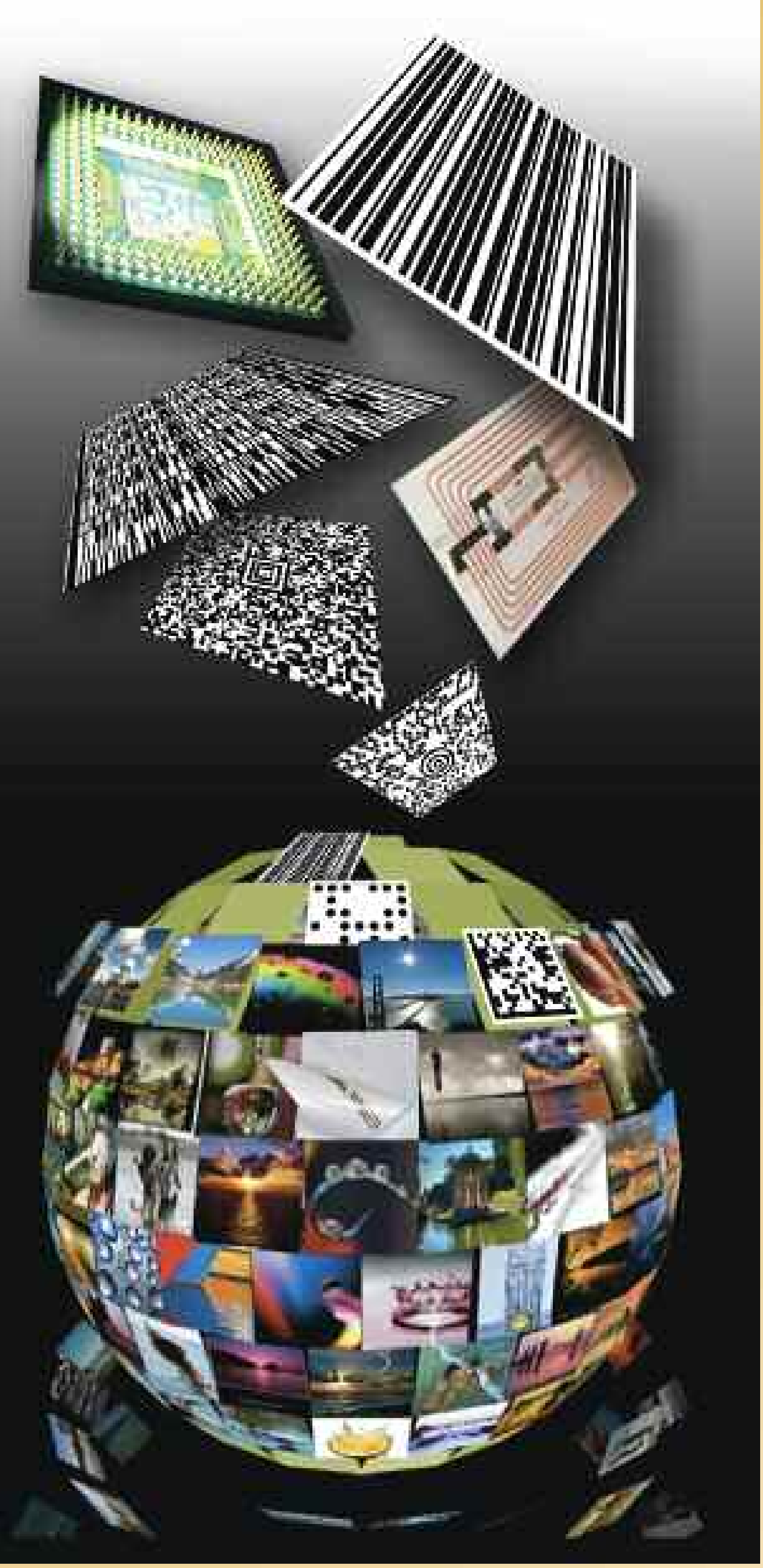
8. Intelligent embeddable processing and communication devices to facilitate automatic nodal functionality, including developments to support automated network management, self configuration and self-repair.

9. Physical natural feature identification readers and IoT interfaces for exploiting natural feature identification.

10. Middleware and other software developments, including intelligent processing platforms to support IoT-functionality and services design.

4.2 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.

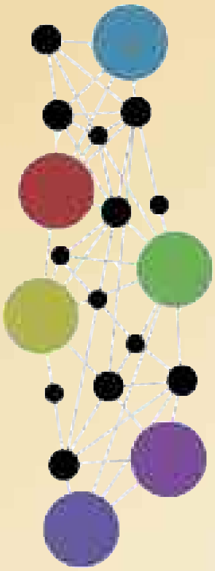
However, there can also be seen a need for rationalising this and subsequent investment to better utilise its potential.

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 assist initiatives will be critical in taking the IoT concept to effective reality.

1. 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.
2. 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
3. The development of a universal or federated data capture appliance protocol to accommodate migratory inclusion of object-connectable technologies.
4. 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.
5. The development of the rules for governance of the IoT with attention to social and economic issues including privacy and security
6. 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.
7. International cooperation on pilot developments and promotional initiatives directed at enhancing inclusion of national bodies in cooperative developments.
8. 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 we need to:



A) Agree on a definition of the Internet of Things that can be used as a popular point of reference.

B) Reduce the number of overlapping and potentially conflicting projects.

C) 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.

D) 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
an EU Framework 7 Project

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

Annex A

CASAGRAS, RFID and the Internet of Things in context

CASAGRAS is a project within Framework Programme Seven: FP7 – Information and Communications Technologies: ICT.[1] The FP7 ICT Work Programme 2009-2010 defines the priorities for the calls for proposals to be launched. The priorities of FP7 and Specific Programme decisions are in line with the main ICT policy priorities as defined in the i2010 initiative. They reflect the input received from the Programme Committee and Advisory Group, the European Technology Platforms and a series of detailed consultations with the main stakeholders.

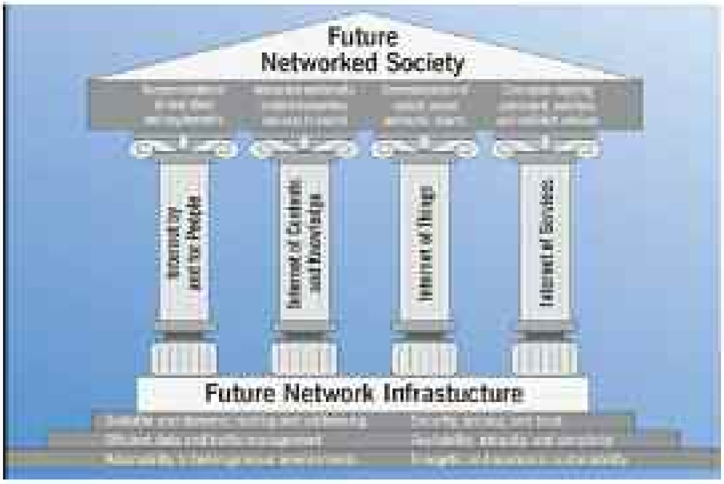
The ICT Work Programme under FP7 is divided into seven 'Challenges' of strategic interest to European society, plus research into 'Future and emerging technologies' and support for horizontal actions, such as international cooperation:

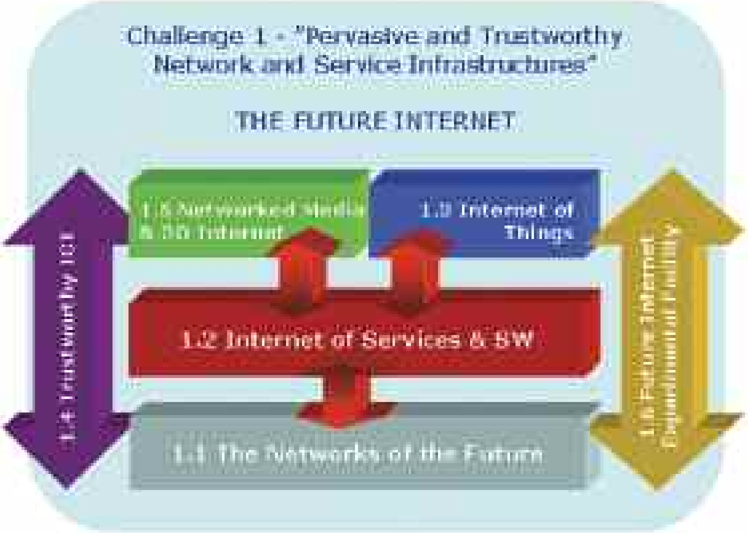
- **Challenge 1** - Pervasive and Trustworthy Network and Service Infrastructures
- **Challenge 2** - Cognitive Systems, Interaction, Robotics
- **Challenge 3** - Components, systems, engineering
- **Challenge 4** - Digital Libraries and Content
- **Challenge 5** - Towards sustainable and personalised healthcare
- **Challenge 6** - ICT for Mobility, Environmental Sustainability and Energy Efficiency
- **Challenge 7** - ICT for Independent Living, Inclusion and Governance
- **Future and Emerging Technologies (FET)**

In CASAGRAS and EC DG INFSO (DG Information Society and Media) D.4 Unit (D4 - Networked Enterprise & Radio Frequency Identification) the focus is on ICT Challenge 1 – Objective 1.3:

ICT Challenge 1: Pervasive and Trustworthy Network and Service Infrastructures

In CASAGRAS, our Future Internet context is the Future Internet Assembly (FIA) http://www.future-internet.eu Real World Internet (Internet Of Things) cluster of FIA http://rwi.future-internet.eu/index.php/Main_Page . We also work with the European Technology Platform (ETP) EPoSS http://www.smart-systems-integration.org RFID/IoT Working Group.


Future
Networked Society
Internet by and for People
Internet of Contents and Knowledge
Internet of Things
Internet of Services
Future Network Infrastucture


Challenge 1 - "Pervasive and Trustworthy Network and Service Infrastructures"
THE FUTURE INTERNET
1.5 Networked Media & 3D Internet
1.3 Internet of Things
1.2 Internet of Services & SW
1.1 The Networks of the Future
1.4 Trustworthy ICT
1.6 Future Internet Experimental Facility

[1] http://cordis.europa.eu/fp7/ict/programme/home_en.html

The Future Internet Assembly was formed on the initiative of the European Commission as an outcome of the Future Internet Conference that took place in Bled, Slovenia on 31 March - 2 April 2008. It is a cooperative cluster of different European research and industrial partners that intends to define scenarios of future Internet and specially the Internet threads and opportunities.

In the FP7 Work Programme, inside ICT Challenge 1, CASAGRAS is focusing on Objective 1.3 Internet of Things http://cordis.europa.eu/fp7/ict/enet/home_en.html. During the 2009-2010 FP7 ICT Work Programme, remaining FP6 and FP7 projects (from Call 1 and Call 5) are grouped into two clusters managed by EC DG INFSO Unit D.4:

- Future Internet Enterprise Systems (FInES) http://cordis.europa.eu/fp7/ict/enet/ei_en.html
- Cluster of European Research Projects on The Internet Of Things (CERP-IoT) http://www.rfid-in-action.eu/cerp

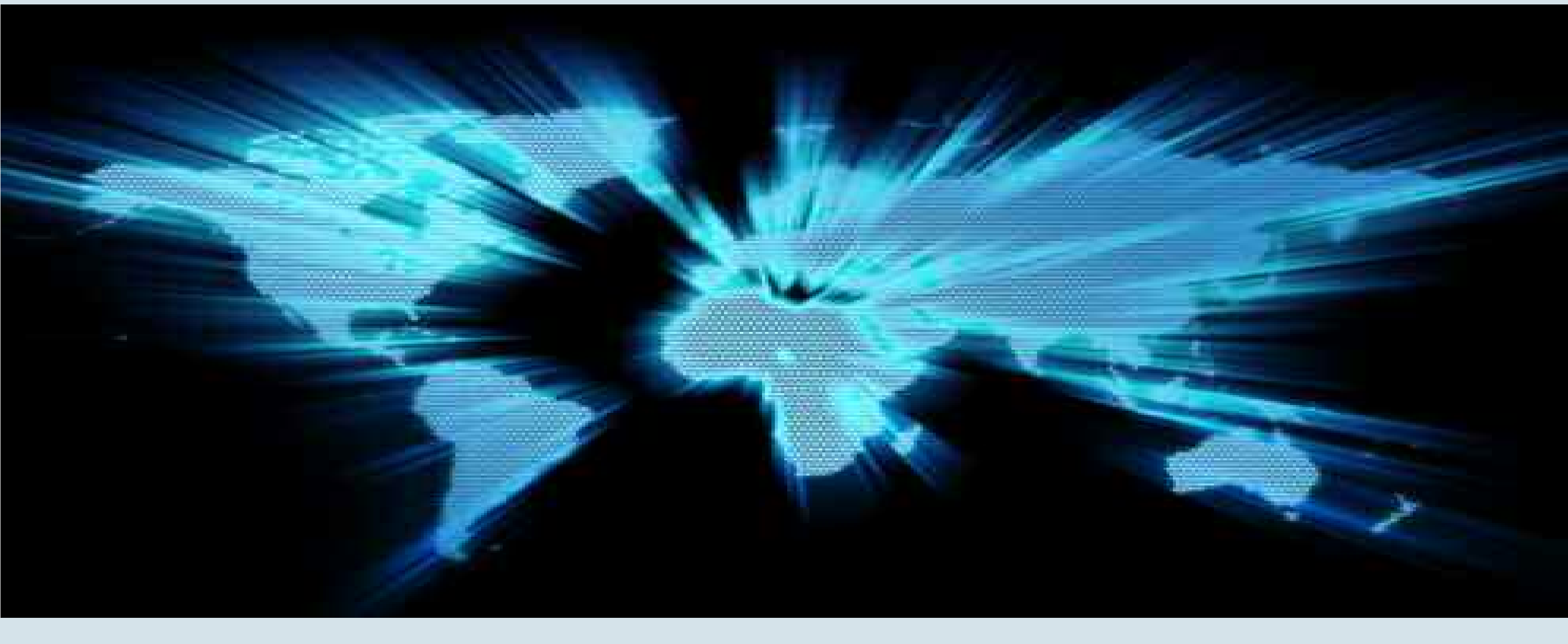
CASAGRAS related EC activities and RFID and IoT Funded Projects & Coordination Actions (Clusters)

The Objective 1.3 “Internet of Things and Enterprise environments” has 3 target outcomes we could split as follow amongst the 2 clusters:

- Architectures and technologies for an IoT [CERP-IoT]
- Future Internet-based Enterprise Systems [FInES]
- International cooperation and coordination [CERP-IoT]

CASAGRAS (with GRIFS) is working with the CERP-IoT cluster:

- At the request of the European Commission (EC) and the GRIFS project, Emilie Danel from GS1 is taking care of the CERP-IoT Dissemination activities including the selection of European events to attend and eventually to have a physical presence in cluster/EC stands for CERP-IoT members/representatives attending the events.
- The EC decided to publish a cluster Book (FInES and CERP-IoT) in electronic format in 2009 and pape formatr Q1 2010. This task is coordinated by Harald Sundmaeker (CuteLoop).
- The EC requested CERP-IoT Coordinator (Patrick Guillemin) to prepare a CERP-IoT Strategic Research Agenda (SRA) to be presented during EC FP7 Call 5 infoday in September 2009 and officially presented at the CASAGRAS final conference in London in October.



The Strategic Research Agenda (SRA) context is FP7 work program 2009-2010 (Challenge 1, Objectives 1.3 essentially but also considering Objectives 1.2 and 1.1) involving (amongst others) EC DG INFSO D.4 Unit, CERP-IoT members, FInES cluster, FIA/RWI and ETP EPoSS. This SRA/Roadmap for the Internet of Things (IoT) beyond 2015 will be the result of collaboration between the members of research projects that have been funded by the EC. The research challenges and objectives will reflect the experience of the contributors of the SRA in the cluster book printed by the EC. FIA/RWI rejoined the CERP-IoT cluster in July 2009 to collaborate on the CERP-IoT SRA development.

Key issues. These relate to standards, regulations, governance and the practical requirements in respect of the associated enabling technology and infrastructure; the present insufficiency of international collaborative effort, including the lack of definition and specification for the IoT; and the need to accommodate other enabling, object-connected, 'edge' technologies and principles than those attributed to RFID.

The EC funded and created an "EU REG" RFID Expert Group (June 2007-March 2009) and successfully facilitated the creation of a low funded RFID Thematic network (ICT PSP Call2) called RACE networkRFID http://www.race-networkrfid.eu/ .

European Union is excelling and leading RFID/IoT research and innovation with explicit international collaboration already established with USA (Lighthouse Project, CASAGRAS, GRIFS), China (MIIT, CESI/CASAGRAS, ETSI, GRIFS), Korea (CASAGRAS, GRIFS), Europe (FIA, FInES, CERP-IoT, RACE networkRFID, CASAGRAS, GRIFS) and Japan (CASAGRAS, GRIFS, DG INFSO D.4).

The EU REG participated in the delivery of:

- EC policy document (Staff position paper) on the Internet of Things
- RFID Mandate M 436 (CEN, CENELEC, ETSI, EC DG ENTR and DG INFSO)
- European Commission Recommendation on the implementation of privacy and data protection principles in RFID-enabled applications (com(2009) 3200 final).
- IoT Communication on IoT 11 May 2009

The EC launched on 8 July 2009 an informal RFID stakeholder group to follow the implementation of EC Recommendation com(2009) 3200 final. FP7 Call5 will bring research projects addressing the issues. The clusters (FInES, CERP-IoT) are requested to identify a Strategic Research Roadmap to address the issues beyond 2015.

What are the other contexts and collaborative actions needed?

There is a need to agree on a common European/International IoT/RWI framework to allow stronger collaboration. In Europe we need convergence between the different FP7 ICT Challenge 1 & Objectives 1.1, 1.2 and 1.3. This seems to be on the right track with the collaboration on developing an EU Strategic Research Agenda where FIA/RWI, ETP EPoSS, FInES and CERP-IoT clusters are working together. The result of this collaboration should be visible in the published cluster book and final conference of CASAGRAS ("Living in tomorrow's world of the Internet of Things" planned in London on 6 and 7 October 2009) and FIA (23-24 November 2009 in Stockholm)

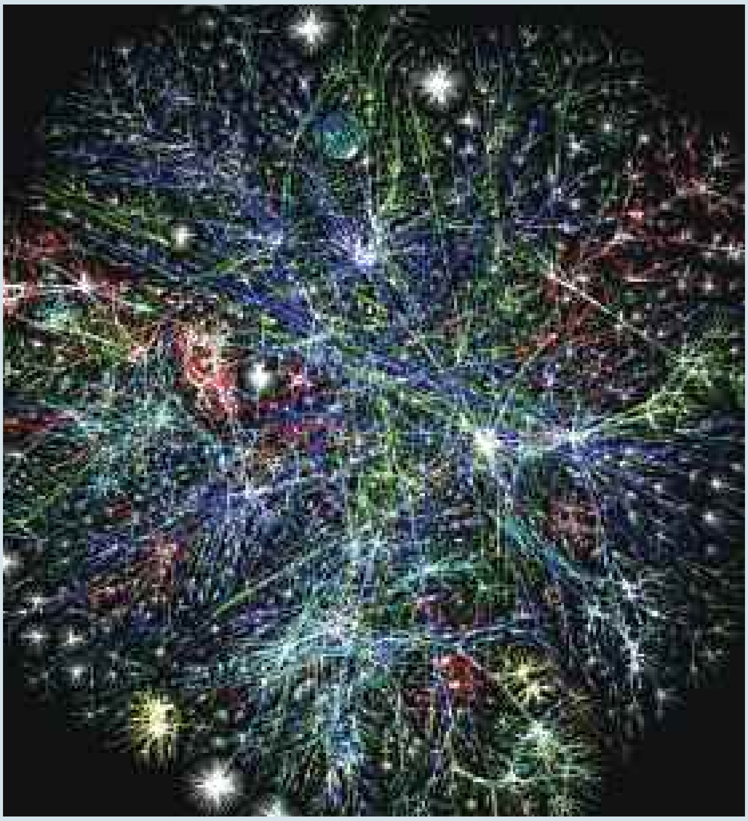
Other identified "Future Internet"/"Internet Of Things" related initiatives will follow:

- GENI and FIND, USA
- Future Internet Forum, Korea
- Next Generation Network Forum, Japan
- Future Networks, China
- ITU-T Future Networks focus group (strong presence of Japan and Korea)

Latin American countries (Brazil), India, Russia, Australia could also be added using FP7 Call 5 Supporting Actions that includes such international collaboration objectives in addition to support to the clusters.

Annex B

An Introduction to Object-connected ICT



Anthony Furness, *Technical Director, AIM UK*

A body of knowledge is now emerging that also provides a foundation for developing object-connected processes and constitutes a new and important sector of mainstream ICT. It embraces the automatic identification and data capture (AIDC) technologies and those of data communications. It also provides a set of principles for planning, designing, developing and applying data carrier systems that go beyond simple 'licence-plate' solutions. This emerging sector of ICT (Object-connected ICT) will have increasing impact upon object identification and management and a significant role in developing the Internet of Things. Object-connected ICT embraces and extends the foundations for AIDC.

By way of definition, Object-connected ICT may be described as:

The body of knowledge, techniques, principles, applications methodology and technologies used for automatic or semi-automatic identification, data capture and data transfer in management or other process support requirements with respect to tangible physical objects, including assets, people and locations.

Object-connected ICT extends the boundaries of supporting technologies to include other object-connected data capture technologies and associated principles. Sensory, security, locating and local communication technologies add to the range, with principles for exploiting and integrating technologies providing added dimension and capability to the applications, innovation and enterprise potential that can be achieved. There is a need for positioning AIDC and, more significantly, the object-connected extension of AIDC within mainstream ICT as one of the most significant technology drivers for object-based business, enterprise and Internet development. Unfortunately, it remains largely unrecognised within both the theory and the practice of ICT. The reason for this is largely historical. AIDC has been generally promoted through industrial channels as a collection of technologies rather than a sector of ICT dealing with item management.

The collective principles for these technologies have not been formally introduced into mainstream ICT education and training, or into mainstream ICT literature. Consequently rising generations of ICT practitioners and information-based service providers have been deprived of a significant foundation in information-based technologies. This is a situation that has to change, and more so as developments in AIDC and associated technologies demonstrate increasingly radical and revolutionary potential, not least within the development of the Internet of Things. It is a natural underpinning adjunct to the Internet of Things and while it has not been possible to include an introduction to the subject within the pages of this report "An introduction to Object-connected ICT" can be obtained through the AIM UK website, **www.aimuk.org** . It is hoped that this will serve as a catalyst for others to contribute to the development of this important sector of ICT and its foundational role in the Internet of Things. A call will be made later in the year for contributors to a book on Object-connected ICT and the Internet of Things.

Annex C

Ontology for Identification

Anthony Furness, Technical Director, AIM UK

Any tangible physical entity, or items as we shall now refer to them, may be represented by what may be called a state characteristic ($\hat{S}$). This characteristic comprises a set of quantities that characterises the item, or some aspect of the item, and its status with respect to prevailing conditions, and with respect to location and point-in-time. Symbolically, this can be expressed as

$(q, \zeta, t) \in \hat{S}$;

where q, represents the intrinsic features or other attributes of the item that may be exploited in identifying, managing or transforming the item in some way, as in a process of some kind. The terms, ζ and t, represent the position in space (location) and time respectively. Change or variability in q with respect to these terms ($q = f[\zeta, t]$) may often be exploited as appropriate in process functionality. The features represented by q may also be functionally dependent upon prevailing conditions, such as temperature and humidity and may therefore constitute a variable with respect to these quantities too, and have to be considered as such.

1.1 Primary Identification

In seeking to exploit the state characteristic of an entity for identification purposes it is important to derive a feature set that is stable with respect to time, location and other dependent factors. It is also important for image-based identification to derive a set that exhibits rotational, scalable and translational (RST) invariance.

Where an item, or part of an item, exhibits static or stable features over the period for which it is to be considered these features may, depending upon the number and degrees of freedom that the features exhibit, be used to identify the item. As such the set of identification features will be a subset, q_{id} , of q.

$(q_{id} , q, \zeta, t) \in \hat{S}$ $\qquad q_{id} \subseteq q$

Here qid represents a natural item identifier that may be exploited in identifying, managing or transforming the item in a process function. While the terms ζ and t, are again included in the symbolic representation for identification purposes qid should be independent of ζ and t. It is also necessary when considering a feature set (q_{id}) for identification purposes that the features should be readily accessible by appropriate sensing or information capture techniques. Biometrics are representative of this class of identifiers.

In these stark theoretical terms it may seem that such notation and techniques are somewhat remote from practical value. In reality, a number of these natural feature identification techniques are in current use. By way of example, the seemingly random matrix of fibres that form the micro-surface structure of a sheet of paper can be exploited for identification purposes, the fibres determining the amount of back scatter variation when scanned with a low-power laser beam. The signal derived in this way, analogous to a bar code scan, yields a 'signature' (q_{id}) that can be expressed in digital terms (sequence of bits) and used to uniquely identify the sheet of paper.

The state characteristic is intrinsic to any item and where a sub-set can be used to identity the item the identifier can also be linked to a body of knowledge or information about an item that exists or is generated to facilitate understanding, handling, processing or management of that item. This is very much a generalisation. The extent to which this characteristic or its components parts are exploited depends upon practicalities and economics.

The practicalities relate to the granularity or resolution to which it is necessary to identify items and the means available and reasonable for identifying such entities.

Natural feature identification distinguished in this way may, for convenience, be considered as primary identification. Moreover, the techniques can be categorised with respect to the features or properties that are exploitable for identification purposes. So, for primary identification purposes features may be of physical, chemical or biological origin and derive from either static or dynamic phenomena.

1.2 Secondary identification

The alternative to natural feature identification is to use a data carrier in the form of an attendant physical entity, such as a tag or label, which can be embedded-in, attached-to, or accompany an item. The carrier is used to carry and provide an identity, typically in the form of a machine-readable number or alpha-numeric string stored within it. Identification in this form may be conveniently referred to as secondary identification.

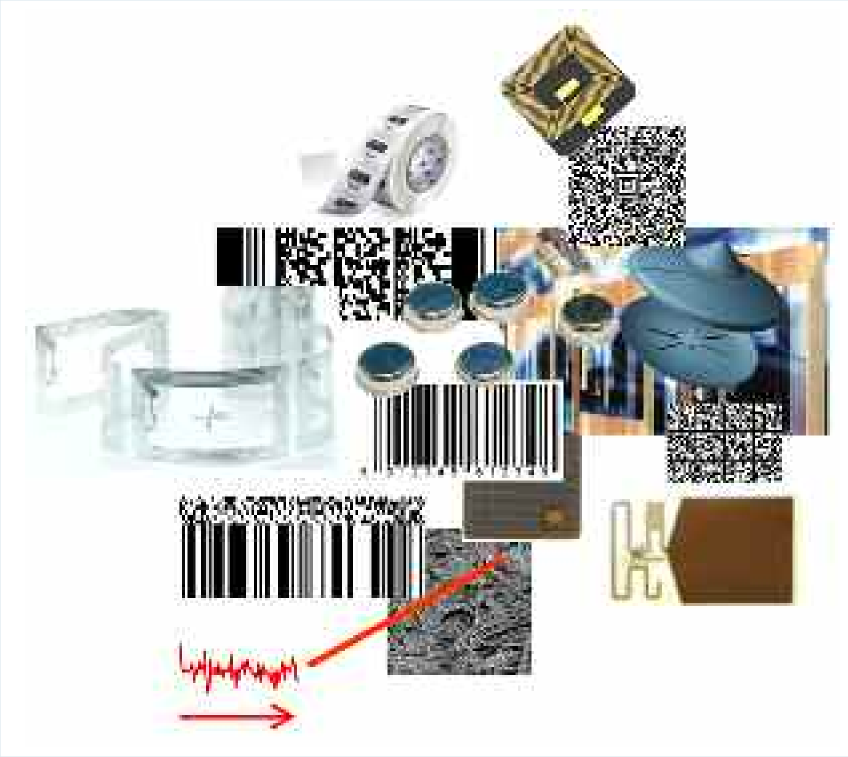
Using this approach to item identification, the item-attendant data carrier is linked in state terms to the item to which it is attached, and both assumes the identity of the item and shares the influences of time and location experienced by the item. So the combination of item and item-attendant data carrier can now be represented essentially by a combined state characteristic:

$(ID_{dc}, q_i, q_{dc}, \zeta_i, t_i) \in \hat{S}$ Where dc denotes the data carrier and i the item.

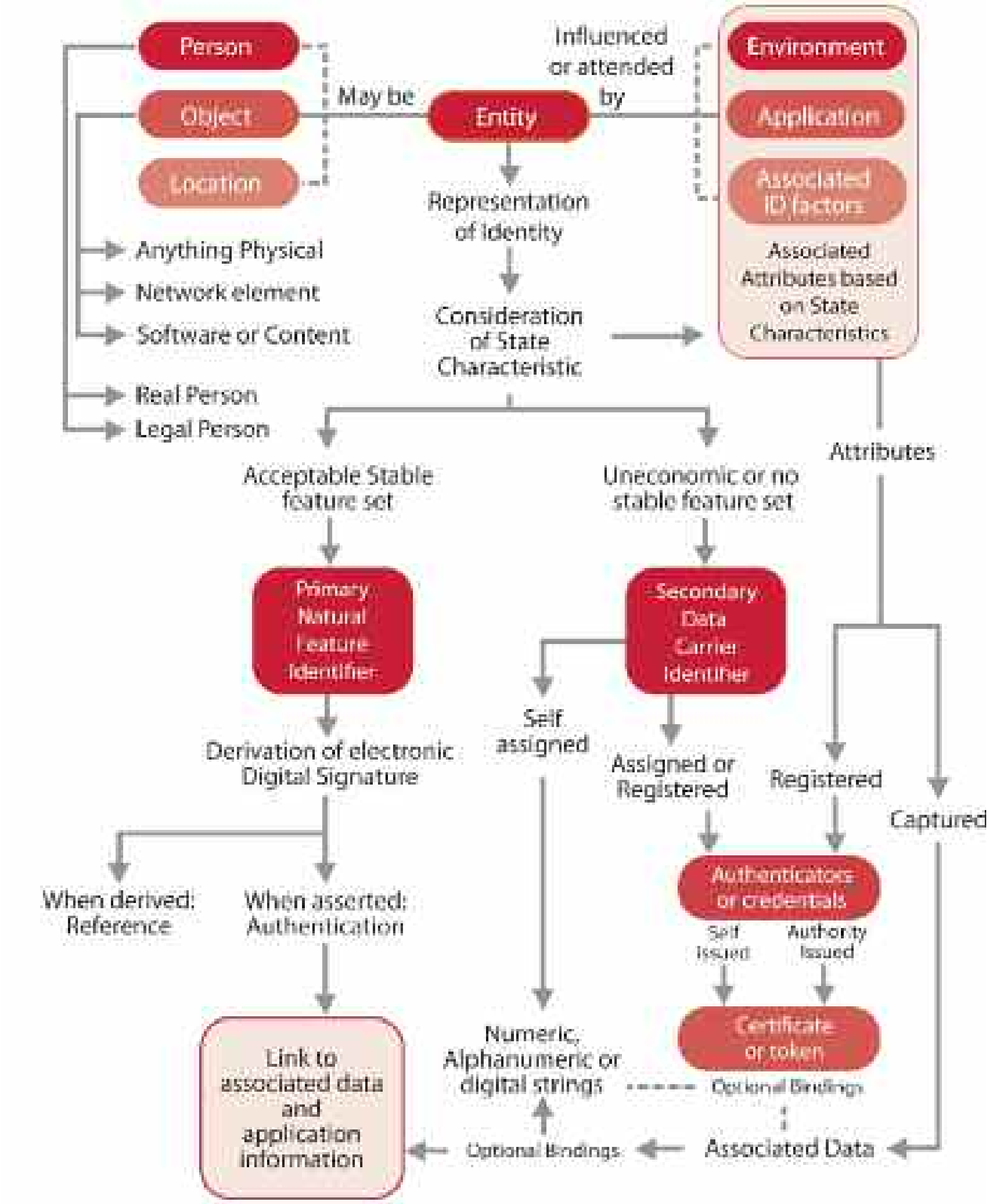
While the data carrier itself will also exhibit intrinsic features (q_{dc}) they would not generally be exploited within a process function. However, they will have relevance to application needs with respect to features of durability and effectiveness of supporting data carrier functionality.
It must also be recognised that the data carrier may also be capable of carrying additional data or information to that of the item identifier but of relevance to the item concerned. Where this capability is defined the combined state characteristic will include the additional data or information component:

$(ID_{dc}, D_{dc}, q_i, q_{dc}, \zeta_i, t_i) \in \hat{S}$ where D_{dc} represents this additional data or information component.

A range of item-attendant data carriers are available, with differing form factors and attributes to suit a wide range of applications.
These carriers include linear bar code symbols, two-dimensional coded symbols, contact and contact-less magnetically encoded carriers and both contact and non-contact semiconductor structures, including radio frequency identification (RFID).



Schematically the foundations for identifying an entity can be as shown below.

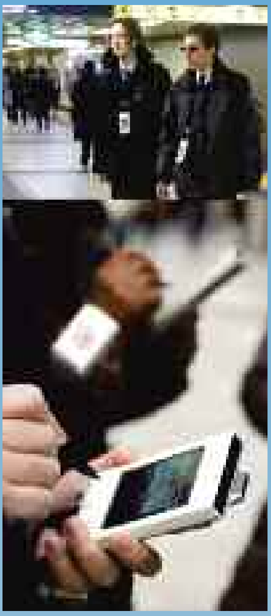

Person
Object
Location
May be
Entity
Influenced or attended by
Environment
Application
Associated ID factors
Associated Attributes based on State Characteristics
Anything Physical
Network element
Software or Content
Real Person
Legal Person
Representation of Identity
Consideration of State Characteristic
Attributes
Acceptable Stable feature set
Uneconomic or no stable feature set
Primary Natural Feature Identifier
Secondary Data Carrier Identifier
Self assigned
Derivation of electronic Digital Signature
Assigned or Registered
Registered
Captured
When derived: Reference
When asserted: Authentication
Authenticators or credentials
Self Issued
Authority Issued
Certificate or token
Link to associated data and application information
Numeric, Alphanumeric or digital strings
Optional Bindings
Optional Bindings
Associated Data

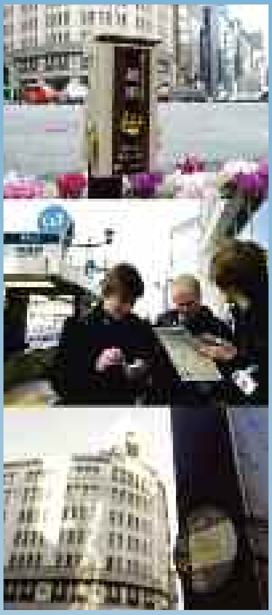
While RFID is used as a secondary identifier and data carrier platform further types of devices may also provide the facility for sensory functions, using appropriate sensory and data storage or transfer components. This introduces a dynamic data capture feature with respect to the combined state characteristic, wherein the data component of the data carrier becomes a function relating to the sensor or sensors used for data capture and any data communication process that operates upon the data content:

$D_{dc} = f(\delta, D_s)$ where δ represents the sensory function and D_s the data storage feature.

Dynamism can also be distinguished for the intrinsic features of a RFID data carrier as a result of its radio functionality, giving rise to a ‘radio signature’ characteristic of a particular carrier. Thus qdc may be considered to comprise a static and a dynamic term (q_{dcs}, q_{dcd}).

A pictorial flavour of the application potential for the Internet of Things





Useful Contacts and reference points

CASAGRAS
www.iot.eu.com

GRIFS
www.grifs-project.eu

Cluster of European Research Projects on The Internet Of Things (CERP-IoT)
http://www.rfid-in-action.eu/cerp

Future Internet Assembly (FIA)
http://www.future-internet.eu

Real World Internet FIA
http://rwi.future-internet.eu/index.php/Main_Page

European Technology Platform (ETP) EPoSS
http://www.smart-systems-integration.org

Future Internet Enterprise Systems (FInES)
http://cordis.europa.eu/fp7/ict/enet/ei_en.html

RACE networkRFID
http://www.race-networkrfid.eu

The Old Vicarage,
All Souls Road,
Halifax,
West Yorkshire,
HX3 6DR, UK
Tel: +44 (0) 1422 368368
Email: ian@aimuk.org
website.www.iot.eu.com