
WHITE PAPER

SMART NETWORKED OBJECTS

&

INTERNET OF THINGS

V1.0 13 12 2010

TABLE OF CONTENTS

EXECUTIVE SUMMARY	4
Vision.....	5
CHALLENGES OF THE DESIGN AND INTEGRATION OF OBJECTS.....	10
Energy management at object level	10
Packaging, integration into materials, sensor (and actuator) integration.....	11
Deployment and sensors (actuators) calibration.....	12
Communication devices.....	13
Trust, security and robustness	14
Reconfigurable hardware & software, co design and integration.....	15
CHALLENGES OF THE MASSIVE SECURE AND FLEXIBLE NETWORKING OF OBJECTS...	17
Communication protocols & information routing in a network with heterogeneous environment.....	17
Quality of service (QoS) standards convergence, provisioning, dimensioning, scalability, models and control.....	19
Intermediation substrate.....	21
Geolocation and privacy	21
CHALLENGES OF THE SERVICE MANAGEMENT	23
Local data fusion.....	23
Distributed information processing & heterogeneity management.....	23
Ambient and cooperative intelligence.....	25
ANNEXE 1 : INDUSTRIALS SCENARIOS	30
ANNEXE 2 : COMPETENCES CLASSIFICATION	44
ANNEXE 3 : CONTRIBUTEURS & CONTACT POINTS.....	45

EXECUTIVE SUMMARY

The continuous progress in microelectronics and networking techniques make it now possible to envisage networks formed by the interconnection of smart 'network enabled' objects and the secure and efficient deployment of services on top of them. This is the vision of the Internet of Things. We now see the deployment of a new generation of networked objects with communication, sensory and action capabilities (wireless information transport networks, RFID, WSN, etc.) for numerous applications. But the interconnection of objects having advanced processing and connection capabilities is expected to lead to a revolution in terms of service creation and availability and will profoundly change the way we interact with the environment. In short the physical world will merge with the digital/virtual world.

This vision "from simple connected objects as sensor networks to more complex and smarter communicated objects as in the envisioned Internet of Things" however needs to implement a pluridisciplinary approach for new technologies, concepts and models (IC development, energy management, communications systems and principles, embedded systems and packaging, data acquisition and processing, field experimentation) and supposes to solve a number of scientific, technical and business challenges. Actually, scientific and technical challenges require different competencies:

- ✓ challenges linked to the integration of smart autonomous interconnected objects (sensors, actuators, processors etc.) under really strong energy, sustainability and environment (physical and chemical medium) constraints
- ✓ challenges linked to the massive (trillions of objects could be interconnected) secure dynamic and flexible networking and the concept of ubiquitous service provision.
- ✓ challenges linked to the fusion of the data obtained by the sensors, network and service management, the distributed data treatment and ambient intelligence.

Finally the application and business cases should be studied beforehand in a close collaboration between the academic and industry worlds since the technical solutions that will be adopted significantly vary from one application to another. In addition, the analysis of the acceptability of the society, the governance related issues, the standardization and the interoperability of these emerging smart objects and Internet of Things applications has to be addressed.

To address the technical issues a joint initiative between Carnot Institutes (ESTIA, FEMTO, IEMN, IT, LAAS, LETI, LIST, LSI, MIB, STAR et UT) and industry (Orange, Alcatel Lucent, Thalès, Schneider Electric, Airbus and Auchan) has been launched. The industrial partners of this initiative played a key role in defining ambitious application scenarios in various fields (home networks, smart and green cities, logistics, aeronautics) that were used to structure the work of the group.

The objectives of the initiative are to analyze the technical and applicative challenges linked to smart networked objects and the Internet of Things, raise the awareness of academics industry and public authorities on this topic and prepare collaborative projects in response to current calls (FP7, ITEA, National ANR projects, Competitively clusters etc.)

The present white paper summarizes the main findings of this initiative.

There is a worldwide consensus, both in industry, academy and public institutions in charge of supporting R&D, on the major socio-economic impact that the Future Internet will have. There are several views on what the Future Internet will be (see for example Euro-FGI Vision, An overview on future communications, D. Kofman, Institut Telecom, December 2007), but they globally refer to the fact that we are going to see the ubiquity of personalized services, the generalization of location and context awareness and of services composition, the global mobility of those services across technological, administrative domain and terminal borders, the extension of the network through advance networking paradigms like ad-hoc, mesh and vehicular networks, the merge of the real world with the digital one through technologies like wireless sensor and actuator networks (WSANs), next generation RFIDs or robots setting the cornerstone for the so called Real World Internet. This merge relies in particular on technological breakthroughs in the following two areas: **(1 Hardware)** advanced microelectronics for smart autonomous communication enabled objects (sensors, actuators, processors, memories, batteries and energy scavenging, transceivers (RF interfaces, base band circuits, ...)), packaging that are affected by the environment and the operation mode, **(2 Models & Software)** innovative distributed intelligences and human-machine interaction approaches that are constrained by flexibility (configuration, plug and play, ...), scalability (trillions of objects could be interconnected), security/privacy, business models, law and ethic. Finally, the complexity of the interactions between the hardware technologies, the software protocols and the environment from different domains often require co-simulation tools to have an evaluation of the system operation before making a prototype.

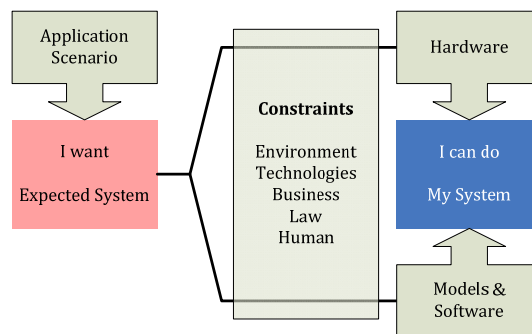


Figure 1: How to build a system

In a close future, it is expected that these smart objects will significantly go beyond present 'simple' sensors and RFID. They will be in particular based on cheap and small devices including sensor and actuator capabilities, advanced signal and information processing, one or several communication interfaces and networking capabilities, which can be embedded in most types of environments and systems, including existing communication terminals, vehicles, clothes, medical/body and most consumer electronic appliances. These systems offer an augmented perception of the reality to a local or distant user or smart entity which can act accordingly. Thanks to the integration with the Internet, users will be aware of conditions in distant places and will be able to control a remote single or a group of objects, mechanisms and environments. Recently,

this concept of Ambient Intelligence has been rehabilitated and the term NED (Networked Embedded Devices) has been used to identify this large diversity of devices with computing and communication capabilities, capable of self-discovery and coordination for the provision of an integrated experience (see for example Real World Internet, Position Paper, Future Internet Assemble, M. Presser et al. , December 2008).

The Future Internet architecture will therefore consist of a core and two rings: the core will be composed of the evolution of the present Internet infrastructure (core and convergent fix-mobile access), the first ring will be composed of a new generation of terminals with networking capabilities and therefore the possibility of participating to spontaneous and self-organized networks, the second ring, based on these smart, active and sensitive systems and technologies will allow the merging of the real and digital worlds.

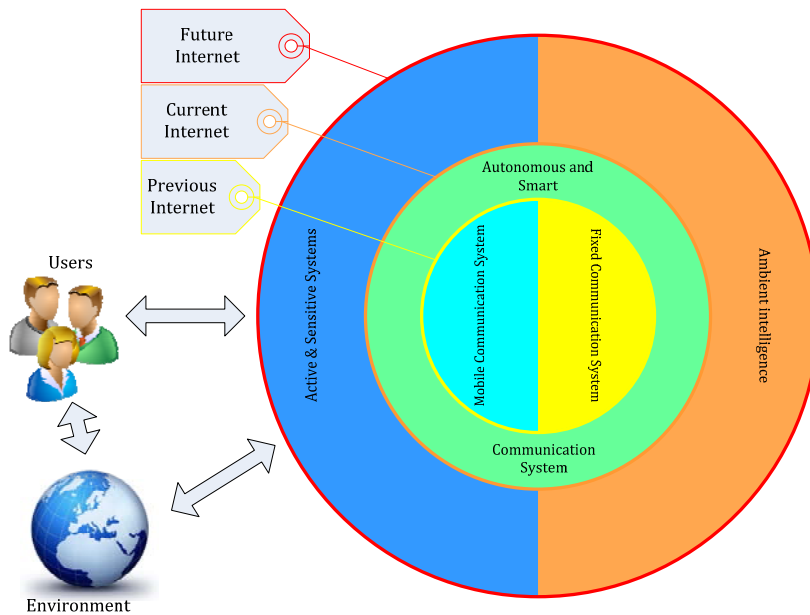


Figure 2: Future internet – one entity itself?

The present initiative

The present initiative focuses on the technologies and architectures that will enable the second ring as well as in its inter-working with the rest of the global architecture, paving the way towards the Real World Internet. Very significant economical, industrial and societal impacts are expected. The initiative has been launched by relevant Carnot Institutes (LETI, LAAS, IEMN, LSI, TELECOM EURECOM) and industrial leaders (Orange, Alcatel Lucent, Thalès , Schneider Electric, Auchan, Airbus) in order to provide a coherent R&D framework for contributing on the design of the Real World Internet and demonstrate its impacts in selected application areas. Some other Carnot institutes have joined this initiative like UT, MIB, LIST, ESTIA, and more are welcome !

The initiative will cover the technological and architectural aspects of various innovative systems that are key enablers of the Real World Internet. The work will be structured

along several application scenarios provided by the industrial members that will be used to give specifications and usage scenarios and to demonstrate the results. It will be carried out in specific projects of different nature: national projects, -Carnot-Fraunhofer projects, European projects (FP7, ITEA, CELTIC...), Competitivity clusters, industrial partnerships etc.... with a large integration effort included in selected application platforms:

- ✓ Ubiquitous services and mobility
- ✓ Industrial processes and logistics
- ✓ Wholesale and retail commerce
- ✓ Transportation and aeronautics
- ✓ Intelligent buildings and homes
- ✓ Personal, medical and leisure services

Table 1 : This table gives the main characteristics of interconnected objects for some typical applications

Application	Power source.	Transmitter Receiver	Size	Cost	Quantity	Network characteristics	Distant Interaction mode	Challenges
Smart home	Mains	PLC Rates: Tx rate : a few kbps Rx : a few kbps Range <50m	<20 cm ³	< 1€	>100 millions	Service discovery Self-configuration Network discovery	Interrogation download	Service discovery
Smart home	Mains or battery	PLC or microwave Rates: Tx : a few kbps Rx : a few bps Range < 100m	<10 cm ³	<0.5€	>10 Millions	Self-configuration Spontaneous network Network coding	Activation Interrogation	Power efficiency Adressage et routage
Smart and green cities	Battery or photo voltaic	Microwave Rates: Tx : 100 bps Rx : a few Range < 1km	<10 cm ³	<0.5€	>10 Millions	Self-configuration Réseau spontané Network coding	Activation Interrogation	Power efficiency Adressage et routage (mesh)
Smart home /surveillance	Mains or battery	Microwave/optical Rates: Tx : 100 kbps Rx : 1 kbps Range < 500m	<20cm ³	<10€	>100 millions	Réseau spontané Network coding Centralisé/Distribué	Command Activation Data transfer	Security Self-configuration
Smart and green cities / surveillance	Battery	Microwave/optical Rates: Tx : 100 kbps Rx : 1kbps Range < 5km	<20cm ³	<10€	>100 millions	Réseau spontané Network coding Centralisé/Distribué	Command Activation Data transfer	Security Self-configuration

The interface between the real and digital worlds requires the capacity for the digital world to sense the real world and to act on it. The initiative will contribute to the design of smart networked objects as new generation of sensors and actuators responding to the requirements related with the fact that those capabilities have to be embedded in a large diversity of devices, sometimes with reduced computation, memory, size, energy capacity and specific packaging regarding some application constraints. A research effort will also be provided on the architectures of the devices that will embed those functionalities and that will for instance perform signal processing, distributed information processing and aggregation. Evolved SoC solutions will be designed.

Challenges around the necessary intelligence embedded in these systems will be described and considered together with the communication capability of their interactive components. Special effort will be provided on exploring the network architectures (ad-hoc, WSANs, robot swarms, etc), as well as exploring the corresponding protocols. Self-organization and self-management are critical in this environment and new networking principles, including addressing, naming and identification paradigms, adapted routing solutions, mobility solutions and self-discovery of elements and services and location capability are just a few of the core requirements of those new networking paradigms. The initiative will also focus on the inter-working of the various heterogeneous systems, including the merge with cellular networks and the network and services management. Security solutions will be jointly designed with networking solutions; there is a requirement here for adaptable and self-organized security architectures.

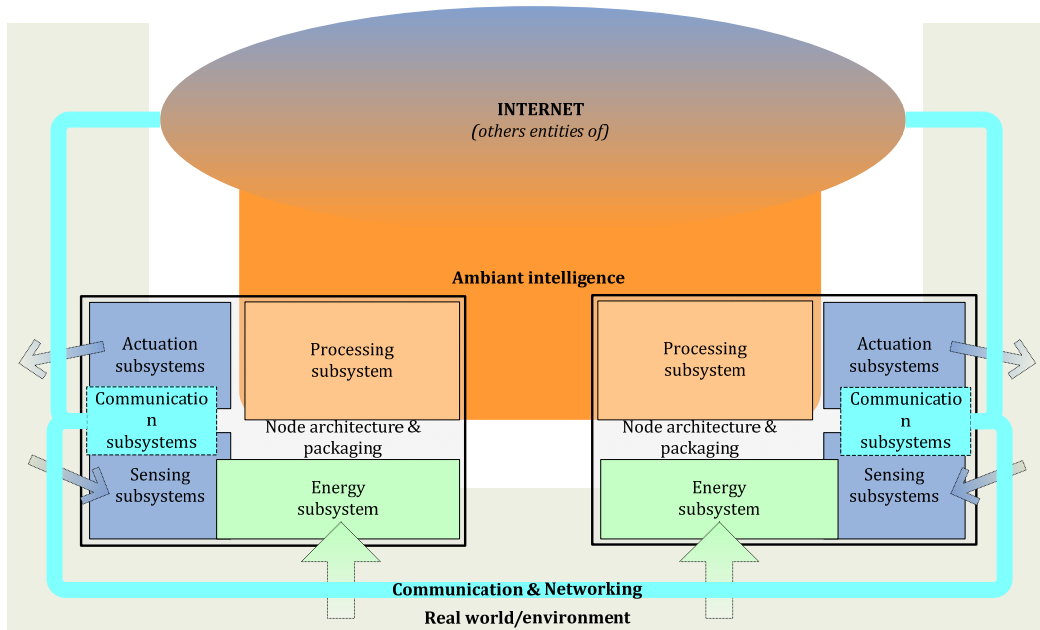


Figure 3: A local view of objects connected to the internet of things and their three main challenging domains: Technologies - Communication - Intelligence

The partners will contribute to the design of the required models simulators, softwares, including the operating systems, as well as on the solutions for dynamically updating the software elements. This activity will include the design, formal verification and on board test of the required real-time distributed systems. Specific HMI's will also be designed. Advance service architectures, with the required middleware and specific solutions for elements and services discovery will be proposed

CHALLENGES OF THE DESIGN AND INTEGRATION OF OBJECTS

This part is divided in 5 sub topics dealing with the technology approach:

- Energy management at object level
- Packaging, integration into materials, sensor (and actuator) integration
- Deployment and sensors (actuators) calibration
- Communication devices
- Trust , security and robustness (related to network criteria her - should be replace by “robustness, reliability and integrity”
- Reconfigurable hardware & software, co design and integration

Energy management at object level

In recent years, multiple applications, involving networks of a relatively large number of wireless nodes, have been considered. Each node would perform sensing, data processing and wireless transmission of information. Consequently, these nodes need to be self-powered, many of the advantages of wireless sensor networking being likely to be lost if external (i.e wired) power sources were used. This constraint has to some extent curtailed the proliferation of wireless networks.

Therefore restricting ourselves to internal power sources, batteries, either primary (disposable) or secondary (rechargeable), offers a high energy density, at low cost. Unfortunately improvements in energy capacity have been much slower than in other areas such as the performance of integrated circuits. As a consequence the percentage in size and weight devoted to the battery in a miniaturized device has dramatically increased. Moreover, there are other drawbacks associated with the use of batteries:

- ✓ environmental concerns in the case of lost sensors
- ✓ economical aspects associated with the replacement of primary batteries
- ✓ and even unpractical change of batteries for networks embedded in materials or for biomedical implants. Power generation using (micro) fuel cells also suffer from this last drawback.

Fortunately, at least primary batteries can be eliminated through the use of environmental energy capture, raising the theoretical possibility of infinite lifetime. Energy capture is the solution for long term, deploy and forget, wireless networks. For energy capture, two principles may be considered, called energy harvesting (continuous source) and energy scavenging (intermittent source). However, availability of energy is then bounded by physics limits, and for such a self-powered network, energy is therefore a critical issue, and the global design (sensing, signal processing and communication) must use energy as one of the major specifications or starting points. In other words, power management methods and technologies are critical enablers. Consequently this is a rapidly growing area for innovation, while still lacking of true industrial system integrators, no more focusing on only one aspect of the total node.

Energy harvesting and mainly scavenging sources (unlike batteries or fuel cells) are not energy reservoirs, and consequently are characterized by their power density only. They are a mean of capturing the environmental energy such as light, thermal or

electromagnetic flux, or mechanical movement. This hard-won primary energy has then to be efficiently converted into usable electrical power. This implies both the design of transducers, which must fit the always-specific environmental conditions, and a proper impedance matching between the transducer output and the load, whatever the load nature is, in order to maximize the energy transfer. If needed, any electronic low-power conversion circuit should switch itself off if the captured power falls below its own requirements. Obviously, all other electronic devices must also follow a low-power design and operating principles.

Another step in powering solutions would be managing several energy sources, with compatible technologies and with substantial power ratios.

The other side of powering is autonomy. To be autonomous, the system has to get a perfect energy management in order to optimize powering and also performance. This aspect becomes crucial for a system with several power sources and energy storage solutions. "Intelligence" is then embedded in the system in order to manage all the constraints. Like powering, autonomy has existing solutions which have to be adapted or even redeveloped to be compliant with micro and nano systems.

On another aspect, for some activities, the network must be active while its surroundings do not offer any energy (equipment is switch off, night-time...). Then part of the energy previously captured would have to be stored. Storage can practically be achieved either through secondary batteries or (super) capacitors. The former nevertheless suffers from some of the drawbacks of primary batteries, and also needs an electronic circuit to control the charging profile, this circuit negatively impacting the power dissipation.

Finally, the design of an energy-efficient wireless sensor node requires a global (holistic) approach taking into account the different aspects of the energy consumption. For this goal, the challenge is the development of a co-simulation framework that includes accurate energy models for the analysis and the optimization of the power usage in the sensor node.

Opportunistic Energy (harvesting energy techniques) would be also addressed, with new challenges about energy efficiency optimisation procedures. This topic would be intrinsically linked to part 3 "sensors monitoring through network", but would also required specific investigations on new coding schemes for instance, in order to converge toward an improved bit/hz/s/DC consumption ratio.

Packaging, integration into materials, sensor (and actuator) integration

Integration inside materials require to make technological breakthrough in the domain of micro-system **packaging and its compatibility with the host matrix**: Generally speaking, a micro-electronic system requires cares in handling: there are often mechanically fragile and physical sensitive to electrostatic discharge and environment chemical agents. Consequently their insertion into a host medium implies many problems.

The material can be the site of mechanical straight: those straights can be concentrated on inserted objects leading to high level of stress (by analogy with stress concentration around holes) at the sensor/medium interface, or in the opposite case, could be

redistributed elsewhere in the host medium implying apparition of weak points. Such phenomenon may also alter default materials properties. This aspect should be carefully investigated, at least by mechanical design and tests. In plastics materials more pernicious problem could appear: once a micro-object has been incorporated inside a hot plastic material during the processing, it may induce redistribution of residual stresses during the cooling phase, and lead to objects with final shapes out of specifications. The way of insertion into plastic matrix is a challenging problem. Usual industrial process like extrusion or moulding implies high temperature (typically between 200 and 400°C) and pressure level such as 200 bars. The micro systems will have to overcome these difficult conditions by presenting an appropriate packaging or at least a pre-coating to be compatible with industrial production lines.

In the worst cases, the host material inside which we want to integrate sensors could sometime be a chemically aggressive medium: concrete or cement material is a typical example with $\text{pH} > 12$. A direct contact between the medium and the dices would lead to corrosion problems and diffusion of moisture inside the system. In such case, a packaging will be necessary.

Definition and specification of an appropriate packaging is a challenging task because it should consider interface compatibility between medium and packaging material and in the same time the packaging may not alter the micro system's performances. There are no general rules of design as the types of sensors and targeted medium can be diverse from one application to another.

Similar challenges exist for the integration of actuators into the environment.

Integration on silicon and integration technologies within specific environments (textiles, buildings, ..) and contribution to the implementation of new materials and topologies/architectures of sensors.

Deployment and sensors (actuators) calibration

The calibration phase is fundamental to obtain useful measurements. Since the sensors are the mean through which ambient intelligence systems "assess" the environment and elaborate their operating strategy, the measurements must be reliable. Similarly, since actuators are the "arms" of such intelligent systems, it is crucial to know precisely their behaviour

The calibration process has for purpose to identify the imperfections of a measurement like bias, drift, noise level, and to correct it. Such imperfections may generate erroneous measurement or dispersions that should be minimized. Ideally, the calibration should be a factory process. However, some sensors need in-situ calibration, Embedding sensors in materials can also alter the characteristics (response) of a particular sensor in a way that is not necessary known at the time the sensor is produced. It is also likely that the expected low production cost of the sensors will prohibit the cost of a factory trimming and calibration. Therefore, methodologies that can be applied to a few high end sensors are usually not scalable, and new automatic self-calibration techniques must be developed.

The deployment of the sensing infrastructure raises also key issues. In order to perform a cost-effective deployment of such a massive infrastructure, the sensing system must

be able to perform a self-assessment once deployed, namely, estimate its “shape” (where are the sensors? how could they be linked together? how redundancy and resilience establish themselves?). Such process involves key technology like self and cross localization and self and cross testing.

Communication devices

When a system is integrated into a new material and environment, the communication must use a modality which is adapted for the information transport throughout its one. Integrated sensing system may include the possibility to transfer data from one point of the network to another one. An integrated sensing system communicates through complex materials with conductive structure and different material layers. Lots of R&D efforts are dedicated to develop low power transmission system and protocol. Investigations focus on power consumption, size, transmission, and performance in order to fit with sensor integration needs. The reliability of the radio link is essential in certain applications (vehicular, medical, safety etc.), which requires a system level approach to guarantee it through e.g. coding, diversity, cooperation, networking. It is obvious also that antenna development takes a great part in the transmission performance between micro systems. In addition radio signals may be exploited towards the accurate or approximate localization of wireless communicating devices, which opens the way to many location related applications or services.

Though in specific cases other modalities like wireline (PLC for instance) or optical can be used, wireless in the 100s MHz to 1 GHz region is the most versatile and was extensively studied in the past. The conclusion still held that in a majority of applications, the wireless sensor node communication part is the main contributor to the overall power consumption, much beyond the sensor subsystem and the micro-controller subsystem when any. Nevertheless, if the power consumption in active mode is less and less the primary source of energy depletion since the sensor node generally spends more than 99% of the time in sleep mode where it shall consume some 100s nA to afford several years lifetime, it still has an impact on the power management and energy source selection and design. Low cost, low size, disposable and/or bio-compatible batteries tend to have a peak current capability below the actual instantaneous needs of the radio when transmitting or receiving, therefore the active power consumption reduction objective still holds.

The wireless communication subsystem also has to deal with strong packaging and integration constraints as highlighted previously. Though the radio IC itself occupies a limited size, laws of physics for antenna design lead to size-efficiency tradeoffs, pushing the selection of the operating radio frequency to higher values, less suitable to low power and low leakage operation for the radio IC. The bulk of wireless communicating sensors is therefore now in the 800 MHz to 2.4 GHz area, benefiting from unlicensed – but crowded bands.

The vision for disruptive solutions either consist in optimizing each building block of a “classical” approach in a cross system / cross competence manner, thus needing a very close cooperation among researchers of broad domains, especially to set up modeling and design flows, or to analyze in depth specific application requirements and to tailor a

solution to these requirements thus avoiding general purpose approaches, at the expense of hard cost optimization due to the absence of critical market mass.

Finally, tenability and reconfigurability are strongly expected for such future smart objects and sensors, and investigation on emerging nanotechnologies are strongly expected. In particular, new research activities dealing with « bio-compatible » sensors and new actuators with new physical dimensions considering environment (fluidic, thermal, piezo,...).

Trust, security and robustness

Traceability of safety requirements is a real need in the context of critical system validation and certification. One has to prove that hazards have been identified and that related safety requirements have been correctly implemented. For now, the traceability analysis during certification is usually done manually by experts, parsing large sets of documents. Thus, certification is sometime more expensive than the development of the system itself. Despite recent progress in hardware technology, pervasive and ubiquitous services remain relatively few and their functionalities are still far from what could be expected. One of the major reasons is due to the fact that they are not trusted. To increase trust, one should guarantee that any service:

- ✓ behaves as expected, without any error (functional correctness)
- ✓ is free from conditions that can cause injury or death to users, damage to or loss of equipments or environment (safety)
- ✓ is protected against malicious adversaries to intrude or hijack the service (security).

This type of systems offers new challenges in terms of validation. Indeed, for practical use of such services, it is essential to be able to add services dynamically, so that they can be adapted to the different configurations and user needs. Combinatorial explosion due to the multiplicity of services remains a hard problem. Moreover, since services are likely to interact¹, a final validation should be done after deployment (on-line validation).

Smart devices can potentially be accessed in a large number of ways by unauthorized personnel. Hardware level as well as software level / network level techniques must be developed in order to ensure the suitable degree of security, according to the targeted application requirements.

Autonomous systems are complex. They include a large number of software controlled sensors (cameras, sonars, etc.) and actuators (motors, wheel, arm, claw, pumps, etc.).

In addition, they integrate advanced features, based on data collected from these sensors and actuators to provide high level services (stereoscopic correlation, environment modeling, travel planning, obstacle avoidance, navigation, etc.). These features are implemented in general as software components.

¹ A new service can change the behaviour of pre-existing ones, break them, or even crash the system. This is a well known problem in the telecommunication industry known as the “feature interaction problem”.

In addition to this complexity, these systems are critical, and the software of these autonomous systems must also manage the uncertainty and temporal constraints. Time constraints are critical because the system interacts with other dynamic systems in a dynamic environment. The uncertainty is due to the fact that the environment and its interactions cannot be completely and accurately modeled. In particular, safety of operation should be considered as a major concern. Indeed, most autonomous systems can be a potential danger to people. The software components of autonomous systems must provide robust capabilities to meet the operational uncertainties. Nevertheless, uncertainty is often the source of unexpected events and interactions, and can put the system into an unpredictable state. From a software perspective, a mechanism must be provided to ensure that these situations are under control and does not lead to catastrophic consequences for the system and / or the environment.

The objective is to develop an environment to assist the design of autonomous systems based on software components. It should allow:

- 1) the construction of complex autonomous systems from heterogeneous software components (synchronous, asynchronous, real time);
- 2) the provision of a complete encapsulation of functional and extra-functional properties and the development of the foundations and methods to ensure the composability of components;
- 3) the prediction of the main characteristics of the system such as performance, robustness (temporal and safety) from the characterization of system components with no combinatorial explosion.

Reconfigurable hardware & software, co design and integration

In addition to the embedded processing capabilities which are required by each application, advanced communicating objects, since they will be inserted in ad hoc networks, will have the ability and resources to reconfigure themselves :

- ✓ the insertion of objects within a spontaneous network should ideally occur in a transparent way without any external action. To be able to do this the object should have the ability to scan its environment and detect neighboring communicating object in order to reconfigure itself according to the required communication protocols (detailed in the dedicated paragraph). The need for high flexibility and reconfigurability requires advanced algorithms development to control the object. The techniques are formally similar to the ones currently used in cognitive radio systems.
- ✓ on the other hand some nodes could play different roles depending on the evolutions of the ad hoc networks they are inserted in. They could be used as relays, or play the role of a central station for a sub network which could control and synchronize the spontaneous network and collect and steer the collected information
- ✓ the object should have enough embedded processing power to steer its resources especially linked to energy management.

These algorithms should run on an embedded digital processor. However a « software » approach induces two overheads: silicon area and energy budget. The latter is especially significant for autonomous objects. The energy budget of a programmable IC is between 10 times (DSP) and 100 times (microprocessor) larger than that of a dedicated IC. This

means that a significant part of the reconfigurability and intelligence of the object should be implemented in the hardware layer (ASIC, dedicated functions, tradeoff between sensor and environment functions). The optimization of the processing architecture will not only be based on low power processors but should also use reconfigurable algorithm integration.

This reconfigurability addresses all components and should combine analog and digital circuits. Indeed reducing the energy consumption while keeping flexibility will largely rely on the development of reconfigurable analog components. For instance new analog functions such as energy scavenging should be addressed in the early phase of hardware architecture design. The hardware architecture should also use emerging techniques such as 3D integration including the RF part, and sometimes sensors (actuators) and energy management systems.

A key challenge for future nodes will be the implementation of reconfigurability and flexibility while keeping an acceptable energy budget. This will rely on optimized hardware integration largely based on reconfigurable analog circuitry.

CHALLENGES OF THE MASSIVE SECURE AND FLEXIBLE NETWORKING OF OBJECTS

This part is divided in 4 sub topics dealing with the communication and the networking design approaches considering the identified requirements at both the objects and the networking levels but also the security and the privacy aspects :

- Communication protocols & information routing in a network with heterogeneous environment
- Quality of service (QoS) standards convergence, provisioning, dimensioning, scalability, models and control
- Intermediation substrate
- Geolocation and privacy (link to the service management challenge also)

In the context of Internet of Things, multiple heterogeneous technologies will be available from the connected objects to the network. It will be important to investigate then the synergies between these heterogeneous technologies in order to better tackle different functionalities in this network either classical functions such as routing, mobility, security, or new ones more related to the objects connectivity such as intelligent connectivity of the smart objects such as using cognitive radio, or other new techniques. Cross layer approach will be of major interest. Other approaches will have to be investigated as well...

The Internet of things is not only an evolution of the current internet to interconnect new « nodes » i.e. objects but it also involves new communication paradigms specifically designed for these objects. In any case, issues linked to connectivity, efficient data transfer, easy access to services etc. will be essential. Constraints will not only be linked to the limited embedded resources in the objects, but also to the heterogeneity of the devices, to the scalability in terms of number of connected objects and to security. The overall architecture of the Internet of Things is also an open question: should the objects be integrated in an all IP convergence scheme and implement light IP like protocols stacks (e.g. 6Lowpan, see also the IPSO: IP for Smart Object Alliance) or should they be connected to local sub networks with different communication techniques with some specific gateways such as semantic gateways interconnecting these sub networks to the access and core IP based networks ? At the time being, we cannot answer this question, we need to investigate both approaches, and try to solve several research issues.

Communication protocols & information routing in a network with heterogeneous environment

Objects can be heterogeneous in various respects: nature and functionalities, properties (fixed, mobile), type of resources, communication modes (synchronous, asynchronous, multi hop, broadcast) and medium, types of applications.

Appart from investigating the possible synergies between the heterogeneous technologies, It is important first of all to classify the heterogeneous connected objects based on their functionalities, their properties whether they are fixed or mobile, what are their resources; as for computing, memory and energy, their communication capabilities whether they offer synchronous or asynchronous communication, broadcast or ad hoc communication, and their usability for which type of application.

Regarding the functionalities of the heterogeneous connected objects, we need to identify and classify the new functionalities that will generate new traffic to be transported in the network. As for the current existing objects we can mention the new functionalities that are identification for object tracking, sensing and actuating for environment monitoring, and so on. It will be then of major interest to analyze the new traffic model and its requirement toward the network.

Based on the connected object characteristics, the communication model to be designed to connect these objects will definitely be adaptive to the limited resources and the heterogeneity of these objects, it will also have to face the high density and the scalability of the network connecting these objects. In the process of connecting these objects, identifying, addressing and naming these connected objects will send us back to the time when IP addressing was designed to offer scalable connectivity of heterogeneous networks. However, IP is greedy in terms of resources; and these are scarce in the projected connected objects. Designing scalable, resource and energy aware identification and addressing plan is one of the major issues in the path to efficiently connect objects. Adapting IP addressing plan as proposed by the IETF in 6LOWPAN working group and designing new addressing but also mapping to IP to allow interconnectivity with IP networks will also have to be investigated.

Considering that the identification and addressing of the connected objects is solved, then the bootstrapping and the auto-configuration and neighbor discovery of the connected objects in order to set up the connectivity and maintain the network of objects have to be designed. Again these processes have to be energy and resource aware.

Now, considering that the connected objects have well configured their addresses, they have to be capable to transmit and forward the traffic from one object to another reaching the right destination in a reliable and scalable fashion. Here, we will have to investigate the existing relaying models such as broadcasting, IP routing, ad hoc routing, delay tolerant routing, and so on, and again energy and resource aware are of major importance, but also the mobility of objects, and here object location and tracking might be used for efficient traffic relaying. Note that, two approaches will be confronted; the first one is supporting the end to end traffic transmission; similarly to the IP approach, and the other one will use gateways but special ones such as semantic gateways that will interconnect sub networks of objects to the rest of the network and will understand and translate the communication from one sub network to another.

In fact, in the network communication design, we will investigate in parallel the communication model design of the network connectivity between objects and the communication model of the connectivity of an object or a network of objects to another network such as Internet. In the first case; this might come up with a new communication model based on new paradigms such as autonomic communication or any emerging future networking, or it might adapt the existing communication model such as the internet model. In the second case, as mentioned earlier, researches will follow the existing investigations as in the IETF or IPSO regarding the adaptation of the existing IP model to extend the connectivity to these new nodes; aka objects, or design specific gateways for protocol and traffic semantic translation to interconnect these objects to the targeted network; aka Internet to offer design and access to new services

built upon these objects and accessed through the All IP converged network. This last scenario is attracting mobile telecommunication stakeholders.

Finally, the designed communication model either between objects or from the objects to the network as Internet will have to integrate the necessary credentials and security mechanisms again energy and resource aware to insure information confidentiality and also privacy.

Quality of service (QoS) standards convergence, provisioning, dimensioning, scalability, models and control

Nowadays we are experiencing a novel evolution of internet. Billions of Internet-enabled equipments will provide digital intelligence and connectivity for almost every commercial and industrial products and appliances, extending the Internet into most aspects of our lives – this is the concept of the pervasive Internet. The Internet is now progressively evolving towards a global communication infrastructure supporting new real-time services in addition to traditional document-retrieval applications.

With the Internet getting more and more present in our daily activities, network outages or even significant degradations of the quality of service become more critical. To avoid network congestions and the resulting service degradations, Internet Service Providers need to **properly dimension the core network** and trunk lines giving the subscriber's access to the Internet. In the current competitive context, they cannot afford installing excessive amounts of capacity and therefore need efficient capacity planning methods. The goal of such methods is to ensure a healthy network that can grow to meet future needs.

The evolution of the present networks towards all-IP solutions, to the internet of the things, is taking different forms, as the traditional telcos are migrating towards Next Generation Networks from the ITU and ETSI recommendations, whilst Internet Service Providers develop their IP networks towards multi-service networks, relying more on the IETF specifications. The main features of Next Generation Networks are a separation of functions (content, service, transport) and the use of a packet network that support multiple services, with openness and convergence at the IP layer.

In order to be open and to be capable of carrying multiple flows and different services, that should be now able to connect all kinds of equipments in the world, including all set of sensors, with interactivity, it is necessary to ensure that a minimum set of properties related to QoS is fulfilled. For instance, throughput, maximum delay, jitter and loss should be properly designed or guaranteed for a large number of end-to-end sessions devoted to multimedia.

Mechanisms for ensuring QoS would allow ISPs to support new services and Network Providers to build for QoS paths. However, QoS can lead to complex problems in IP networks, although legacy voice telco networks were specifically designed to provide a guaranteed level of QoS, in contrast to the current Internet which provides only "Best Effort" connectivity.

Packet loss, latency and jitter are the main QoS parameters describing the network performance and hence quality characteristics of IP-traffic. Three fundamental

strategies and approaches exist to handle QoS in the internet, which are quite different in their principles, mechanisms, architectures, deployment and difficulty:

✓ The first one assumes that underlying networks are able to provide the requested QoS : nothing has to be done in the internet architecture related to QoS. It is the simplest technical solution based on the assumption that, whatever traffic is sent, the network infrastructure and equipment will always provide a sufficient QoS. This means that the network has to be upgraded and improved, as and when needed, in such a way that the network always provides the necessary QoS for everyone. This assumption comes from experience to date that networking hardware technology continues to improve in-line with demand. This is a statistical and long term solution, implemented by Traffic Engineering, with the hope to be able to guarantee that almost all links will be under-loaded most of the time. Then, by performing monitoring over sufficiently short timescales, links which approach their full utilization capacity will have to be detected and upgraded. Of course, research in monitoring, traffic engineering, topology optimization and on-time upgraded deployment, is needed.

✓ The second recognizes that the present networks cannot provide QoS in all cases, but it assumes that enhancements to the current internet can be added to provide an acceptable QoS; this approach starts from the present “Best- Effort” Internet and develops different optimization mechanisms to provide a better QoS. As a few existing networks cannot guarantee QoS, improvements are needed, and so corresponding new designs and solutions have to improve the current Best-Effort Internet by introducing optimization solutions. This approach will satisfy the user QoS requirements in some cases, but, the result of the optimization mechanisms will always depend upon the maximum capabilities of the QoS in the underlying networks. Here again, as a consequence, there is a statistical solution, less expensive, but also a subject to contention problems. In order to minimize these problems, network providers can perform monitoring to adequately define their acceptable utilization capacity before upgrading them. Therefore, in our vision, research in new or optimized mechanisms, protocol, and architecture (e.g. respectively ECN, etc, DCCP, etc, proxys, etc), and (partial) comparison models is needed.

✓ The last target proposes to build a new network architecture that must be able to provide any requested QoS to the network users. The users will be granted the QoS they request. The design of such solution is not an easy task since it would require to use IP and, at the same time to be as general and open as the present Internet. Moreover, it is necessary to be able to monitor and manage all Internet requests and resources. Clearly, designing, developing and deploying such a solution leads to a high complexity, first to define a solution, and second to show that the cost of its deployment is reasonable. In particular, signaling is needed to pass the necessary information between elements in order to reserve resources, perform admission control, route packets to certain paths, prioritize traffic and use the relevant transport protocol, as signaling enables information transfers between users and different Autonomous Systems (AS) or within ASs, while not actually providing functionality for prioritizing the use of the resources in the network.

The degree of difficulty increases for each of these approaches, the most difficult being the last one, that has to be as general and as open as the present Internet, while at the same time being able to guarantee answer to all requests and to master all resources. In

our vision, proposition for novel solutions can be done in the domain of QoS architecture, user Quality of Experience and preferences, control plane, QoS protocols, inter-domain signaling and synchronization, multi-technology abstractions and mappings, host-to-host reservation optimization, scalability, full architectural models, and classes of services deployment.

Intermediation substrate

A prerequisite for the deployment of various services originating from communicating objects based on heterogeneous technologies and interconnected in a heterogeneous way is an “intermediation substrate” that will enable self discovery, connectivity, information exchange between objects – networks - and - users as well as the traceability of transactions which will be required in a trusted environment.

This will require solving a number of technical issues among which:

- ✓ Self discovery of object capabilities at various semantic levels (user services, protocols) etc.
- ✓ Interoperability between heterogeneous protocols based on various technology environments (buildings, infrastructure, telecom networks etc.)
- ✓ Technical solutions to handle end to end trust chain (through different operators having an administrative responsibility to manage the objects); this would guarantee to the user the reliability and trustworthiness of the services, protection of sensitive private data, easy and secure authentication mechanisms and traceability of operations.
- ✓ Combining applications with different critical levels (for instance security and entertainment applications running on the same object), while taking into account the limited embedded processing capabilities.

Architecture studies should also be carried out, in particular the issues between centralized and distributed architectures. The applications will require the objects to be mobile keeping connectivity through operated network infrastructures and, when required, through spontaneous ad hoc networks between objects.

Geolocation and privacy

Geo-privacy (also sometimes called locational privacy) is an emerging field which can still be considered to be in its infancy. However, it becomes more and more important due to the recent multiplications of ubiquitous systems which integrate geolocation capacities which may thus leak information about the movements of the mobile node. The main purpose of geo-privacy is to prevent an unauthorized entity from learning the past, current and future geographical location of an individual (today this problem extends to with smart phones and computers). Methods for preserving the geo-privacy can be classified according to at least three important dimensions:

- ✓ The moment and the place of the protection: for instance, we might be interested in protecting the privacy of the user of a geolocalised system when he is *online* (physically connected) or *offline* (in the case of future access to recorded mobility traces).

✓ The goal of the protection: it might be important to offer a strong privacy guarantee for each individual involved in the geolocalised application or simply for a group of persons or even at a more global level.

✓ The type of technique used: preserving the spatio-temporal data of an individual can be done through various types of techniques ranging from the perturbation of the geolocalised data through sanitization to the applications of cryptographic primitives and secure multiparty computation or even to the use of access control mechanisms (for instance if the access to the geolocalised data is done through a server that can monitor queries).

Studying geoprivacy can be done through inference attacks, privacy and utility metrics, sanitization methods or access control mechanisms.

An inference attack takes as input some geolocated data, possibly together with some auxiliary information, and produces some additional knowledge. For example, an inference attack may consist in identifying the house or the workplace of an individual. Because inference attacks can be used against collected data (offline context) or against some geolocated application to infer private information online, they can also be used to evaluate the level of protection that a particular dataset or system offers to its users.

Another way to quantify privacy consists in using more generic metrics such as measuring the entropy within a dataset or computing some global statistics. Despite several propositions found in the literature, the problem of defining relevant privacy metrics for geolocated data is open for now. For instance, is an individual hidden inside a crowd gathered in a small area really more protected in terms of privacy than an individual alone in the middle of a large area such as a desert? Or should we rather define privacy according to how much the behavior of an individual is indistinguishable of the behaviors of other (or a group of) users?

It is worth noting that privacy protection methods may have an impact on the utility (and therefore usability) of geolocated data and systems. Indeed, if too much information is removed via sanitization, if the cryptographic primitives used for protection are costly or if the access control mechanisms impact performance and reachability, the overall utility of the system is impaired. This often leads to a trade-off between privacy and utility. Therefore, it is important to be able to assess the utility of the overall system and henceforth to measure the impact of the privacy-protecting methods on the utility. A sanitization process adds uncertainty to the data and removes some sensible information so as to protect the geolocated data of an individual. Pseudonymization which replaces the common identifier of an individual by either a randomly generated pseudonym or the "unknown" value is a first step of sanitization but as such it is often not sufficient to protect the privacy of individuals. Examples of more advanced sanitization methods include downsampling, perturbation, aggregation; spatial cloaking and mix-zones just to name a few.

By using cryptographic primitives, ubiquitous systems can perform computations which depend on their geolocated data in a secure manner such that only the output of the global computation is learned (and nothing else). Access-control mechanisms can be used to control how an external entity accesses the geolocated data of individuals within a system. By auditing queries, it also can decide whether or not it should disclose more information since this could cause a privacy breach.

CHALLENGES OF THE SERVICE MANAGEMENT

This part is divided in 3 sub topics dealing with the service approach:

- Local data fusion
- Distributed information processing & heterogeneity management
- Ambient Intelligence
- Environment and tools for service creation composition and orchestration, user interface

Local data fusion

Data fusion is an information processing technique that aims association, combination, aggregation, integration and blending of multiple data sources, representing a variety of knowledge and information, in order to provide a resulting information better than that obtained from all sources each considered separately.

The problem of aggregation and the simultaneous use of data and information from multiple sources can be found in many fields of application often associated with the need of observing an environment from sensors more or less reliable, more or less accurate, and more or less effective. But in fact, the term data fusion extends to larger areas. It includes the combination of all sources of knowledge, whether from sensors, navigation systems, various databases (map data, documentaries, digital terrain models, rules of expertise) or even analysis or previous data fusion.

In the sequel, we consider fusion of multiple sensors data. Depending on the application, the relevance of information provided by various sensors is related to the coverage of the observed environment. How to place different sensors so that information resulting from the data fusion is optimal? Optimizing the coverage of an environment through a network of sensors is a crucial issue. This question remains strongly linked to communication, sensing, computing and energy capabilities of the deployed sensors.

Distributed information processing & heterogeneity management

❖ Distributed information processing

Increasing the number of sensors allows getting a finer mesh of the observed environment. This increase is associated with a significant increase in the amount of data to be processed. Processing these data can be considered either at a central node or in a distributed mode at different sensors. Another approach is to group together the sensors in several clusters; each one headed by the sensor with the most available computational resources. Such an approach allows better management of energy resources in the network. Tree architecture can then be dynamically adopted.

Two levels of data fusion can be considered: fusing the decision or the measurements. In the first case, the sensor shares with its neighbors or with a central node a local decision while in the second case they share their measurements. In terms of communication cost, the transfer of raw measurements is generally more expensive than a decision. In the case of sufficiently dense networks a hybrid approach may be considered allowing a

trade-off between the cost of communications and the quality of the estimate or of the decision.

When the decision is taken at a central node, the local errors are usually easily detected and removed. However, the existence of a central node creates a bottleneck at the network level. Depending on the application, it may be necessary to use highly decentralized processing. Such an approach is more suited to scaling and more tolerant to the addition or deletion of a node or to dynamic changes in the network.

Furthermore, the development of a data fusion process in a sensor network must consider the asynchrony between sensors, possible loss of packets especially in the case of wireless communication and local disturbances. The data fusion algorithms need to be insensitive to packet losses, or at least be able to adapt efficiently when the data loss is partial or total.

❖ Plug and play, self deployment, heterogeneity management

Tiny sensing devices are increasingly present in applications that now require higher Quality of Service with adaptability and re-configurability properties. However, the large number and heterogeneity of sensing devices make them difficult to manage with conventional management tools. Furthermore, the real-time nature of sensing systems imposes time critical management actions in these highly dynamic systems. Self-manageability is therefore an essential property for networked sensing systems. Several challenging key-points must be answered:

✓ Sensor deployment: problem has been faced for instance by the Telecom community. However, it seems that no work still exists on the optimal (the indicators have to be defined) deployment of a sensor/actuator network. Most of the time the sensor are positioned where they can be placed due to external constraints and not where they should be set according to application requirements; Building Information Models should be useful for taking such decisions.

Configuration and Automatic software deployment are important features for flexible sensing systems because the end user is neither a hardware expert nor a software specialist. The most we can ask to the user at this level is an interaction through a web browser. Ideally, we would expect that the system will auto-configure itself without human intervention, against dynamic changes in its environment. The update of device firmware, provisioning of new services or update of applications are necessary for extensible systems. Software management in autonomic manner without human intervention would be one step towards real autonomic sensing systems. For this purpose an event mechanism is needed in order to notify the actors who are involved on taking decisions on new software deployment or updating existing ones. The consortium has particularly pointed this need at the hardware and software levels in section “

Reconfigurable hardware & software, co design and integration”.

← Mise en forme : Puces et numéros

✓ Performance monitoring and maintenance of such sensor/actuator networks are essential. As sensors can be placed at locations that are hardly reachable, remote monitoring and maintenance gain a particular importance. For instance, when a set of sensors or actuators is suspected to be faulty, several scenarios can be envisioned. The first is the ideal case where the faulty part is replicated. However, this is not always

possible and graceful degradation could be an answer. Graceful degradation consists of not ensuring the full service but a degraded service (e.g. less input data, slower processing) that in some case could be enough to ensure that the system provides an acceptable alternative.

The overall goal is to provide a plug and play (PnP) sensing system. The user would come with its sensor on-the-shelf, plug to the system and the device would be self-discovered, self-configured, automatically updated with the latest firmware and monitored during all of its lifecycle. Autonomic computing domain² investigates similar issues, however the existing concepts should be rethought and adapted for resource constrained networked sensing devices having tough constraints including real-time constraints for instance with issues linked to security or system command.

Ambient and cooperative intelligence

❖ Ambient and cooperative intelligence

Today's networks are made of a large number of Network Elements (NEs) such as routers, firewalls, gateways, hosts, etc., each performing a set of elementary functions related to routing, security management, resource reservation, QoS management, etc. More sophisticated functions such as configuration of NEs, optimization of routing tables, troubleshooting, etc., are mainly managed in a centralized fashion often involving human intervention.

However, networks are more and more faced with rapidly changing situations and increasingly complex configurations which are harder and harder to be adequately managed in a centralized manner, because of timing issues (collecting and processing information takes time) and complexity issues (dealing with networks centrally/globally is increasingly complex).

The idea is to pilot the Internet of Things using tools coming from the artificial intelligence field. A platform, based on Distributed Intelligent Agents, permits to perform a number of management functions in a decentralized way, dealing locally with simpler situations in a more responsive way.

Each Distributed Intelligent Agent associated with an NE is capable of sensing and observing events and changes occurring locally. Agents communicate among neighbors to improve their knowledge of the situation in their neighborhood and to make consolidated/coordinated decisions within an area of the network.

The different characteristics of the agents are the following:

- ✓ Decentralization, it means that no agent has a global vision of the system and the decisions are taken in a totally decentralized way;
- ✓ Reactivity, an agent is a part of an environment and its decisions are based on what it perceives from its environment and on its current state. It takes a local view (also called situated view) of its environment.
- ✓ Pro-activity, it is the ability of setting goals and realizing them.

² P. Horn, "Autonomic computing: IBM's perspective on the state of information technology," IBM TJ Watson Labs, NY, 15th October, 2001.

✓ Sociability, it is the ability to distribute the intelligence between the different agents and to cooperate with other agents in the system.

By distributing Agents across the network, problems are dealt with locally, swiftly, earlier and are simpler to address compared to the resulting global problem handled in a centralized approach subject to latency; e.g. an agent can immediately change the configuration of its NE to react to a local load problem.

Beyond purely local problems, Agents cooperate among neighbors to deal with problems appearing in the neighborhood, e.g. a connectivity problem can be detected by several agents that can then cooperate to characterize the problem more precisely and provide a synthetic report to the network control center.

Each Agent maintains its own view of the network on the basis of information obtained (i) directly from local observation of its NE and (ii) indirectly for the rest of the network by exchanging information with its neighbors. This Agent-centric view of the network, focused on the Agent's close network environment, is called the Situated View.

The rationale for the Situated View is that events occurring in the neighborhood of an Agent are generally of greater importance for the Agent than events occurring in a remote part of the network. The fact that local events are known earlier and are more accurately documented in the Situated View makes it easier for the Agent to react rapidly and appropriately.

Agents regularly check for important changes appearing in their Situated View - and thus in the network environment as seen by each Agent - and may decide to automatically adapt certain parameters of their own NE or ask neighboring Agents to do so for their respective NEs. E.g. if an Agent detects locally a potential security problem, it can consolidate this information by checking similar information regarding its neighborhood in the Situated View and then decide to adjust a security policy and/or to trigger a security alarm.

The use of the Situated View drives Implicit Cooperation between Agents who "influence" each others via the knowledge that they are sharing. Implicit Cooperation is the primary mode of cooperation among. This mode of cooperation is simple, particularly robust and well suited for dynamically changing environments because it does not require the establishment of an explicit dialog and a strict synchronization between Agents.

What an Agent is capable of doing is defined as a set of Behaviours. Each of these Behaviours can be considered as a specialized function with some expert capabilities, able to deal with specific aspects of the work to be performed by the Agent.

Behaviours have access to the Situated View which operates within each Agent as a whiteboard shared among the Agent's Behaviours.

The activation, dynamic parameterization and scheduling of Behaviours within an Agent is performed by the Dynamic Planner. The Dynamic Planner decides which Behaviours have to be active, when they have to be active and with which parameters. The Dynamic Planner detects changes in the Situated View and occurrence of external/internal events; from there, it orchestrates the reaction of the Agent to changes in the network environment.

The elements described above come from the start up GINKGO NETWORKS and the platform proposed by the company. The platform provides simple decentralized ways to deal with a growing number of modern networks requirements which are harder and harder to respond to with traditional centralized systems.

- ❖ Environment and tools for service creation composition and orchestration, user interface

Ambient intelligence will impact all aspects of daily life constituting then a powerful driving force of innovations and development. Indeed, it is necessary to provide services and facilities that are appropriate in all circumstances, everywhere and every time both for individual needs and societal challenges including all activity domains. It is no longer just about increasing productivity gains of individuals and businesses, but also to develop technological artifacts that improve the welfare both at the individual and society levels, and hence to support the safeguarding of our planet. It is no longer just about producing computers (software and/or hardware) ready to use, but also to allow both citizen and companies to be the actor-architect of their own services, which can be unlimitedly (re) configurable, in compliance with safe protocols and other laws and mainstream values.

The challenges include:

- ✓ Mobility (with persistence and continuity of communication), moving (with the intermittent connection) of communicating things, information and learning of ubiquitous computing, the Telepresence of individuals or the presence of fragmented body;
- ✓ Identity and identity management of various objects, due to great number, knowing that above a given cardinal of sets, the identity of an object loses its effectiveness;
- ✓ The key properties of communicating things: safety, transparency of functions, non-intrusive, non-addictive with respect to the user;
- ✓ Multimodal Human-system interfaces, heterogeneous interactions in the assembly and the composition of different aggregates in the architectures of various systems, the negotiations;
- ✓ Integration, cooperation (spontaneous or opportunistic) or collusion and learning capacity, at all granularity levels, of niches that intersect; the management of such a complexity ;
- ✓ Cross-cutting aspects of uses taking into account the multidisciplinary approach.

Non-technical challenges include a broad spectrum:

- ✓ Conviviality: intuitive interaction, more general than ergonomics ;
- ✓ Psychological: reject phenomena of devices devoted to assistance to elderly ;
- ✓ Legal: safety of robots, intellectual property, the right of access to a digital entity, the right to forget in all the tracks recorded by these things, laws on physical objects;
- ✓ Ethics: respect for individual privacy, digital dignity in infrastructures for monitoring purposes ;

- ✓ Political: freedom of expression of citizens in semi-private spaces.

A services deployment environment includes three components. The first one is the assessment of these services in terms of technology and uses (see “Reconfigurable hardware & software, co design and integration”)

✓ Creation of services: machine to machine (M2M) systems are an unavoidable future. These systems are highly interactive; create links between mobile devices (PDAs, smartphones, sensors ...) and users to perform collaborative tasks in a context of pervasive and ubiquitous computing. Because of their intrinsic characteristics, they must rely on highly dynamic and self-configurable software architectures. For instance, if we consider the home automation field, the introduction of processors communicating in the home automation devices constitutes a mass of information and computing power in each house. In terms of energy, information and technical resources are potentially available for consumption optimization according to the ecological demands. In terms of comfort, safety and assistance (elderly, sick, etc.), societal needs are immense and growing. However, the available technologies can not achieve the home automation applications that meet expectations. One difficulty is that the configuration of each house is different, and the devices provide different services in their implementation, and use of multiple devices can introduce conflicts and indirect incompatibilities hardly identifiable.

The first challenge is to achieve high-level services as composite services built from all available services (atomic or composite), and verify that the current setting of the house provides services consistent with expectations.

The second challenge is the dynamical behavior that is inherent in this type of application: services are created, interconnected, and deleted during execution. This dynamicity responds to the constraints of the distributed application adaptability and the mobility of its users. For static architectures, models are proposed but these approaches are not usable and we should rely on formal and powerful modeling formalisms. For instance, Graph Grammars which treat the dynamic evolution of software architectures by graph transformation.

✓ **Access to services, interfaces, human machine interfaces (HMI):** The provided services must not only be accessible to the user but the latter must also be able to ensure its monitoring and control. We have to remain very attentive to the problems of use and ergonomics, especially through the design of user interfaces, since the human user must be in the loop control for systems to be accepted by users. The search for innovative solutions to human interface must allow users to be aware of the state of their system and of the motivation of the selected regulation scheme so that the system does not appear as a black box. The user must keep control, always be able to override the decisions of the system (except mandatory security constraints). And finally it makes them aware of their energy footprint, so they can, if possible, modify their behaviour owing to a real time feedback of their actions.

There are many kinds of HMI that can be divided according to the content of conveyed information and the interface devices. They must be adapted for use by people in the

building for example. We will consider different types of interfaces (traditional, tangible or multimodal), centralized or distributed, mobile, semi-mobile (some may be removable) or static.

Finally, the aspect strongly linked to the service orchestration is the usable quality of service which has been discussed in the section “Quality of service (QoS) standards convergence, provisioning, dimensioning, scalability, models and control” and the existence of “Intermediation substrate” to build and reach the appropriate services.

ANNEXE 1 : INDUSTRIALS SCENARIOS

Scenario smart Building – Schneider contribution



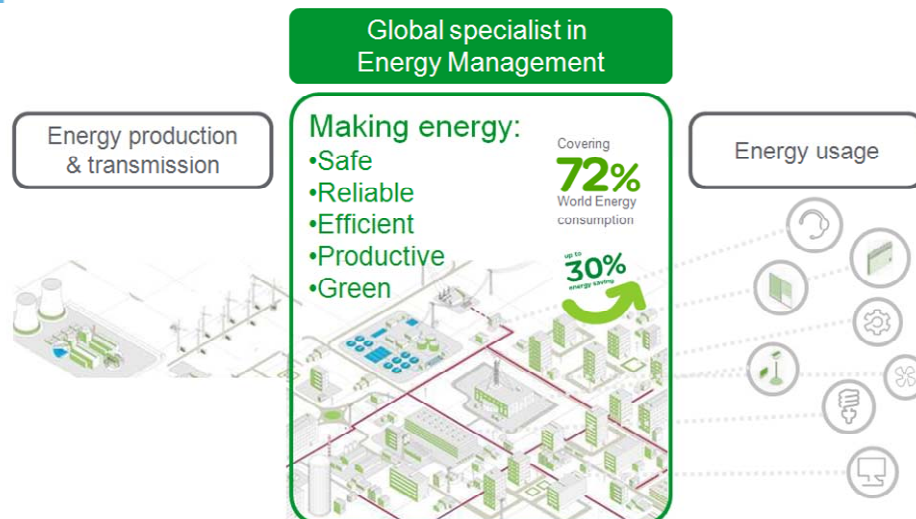
Inter Carnot Objet Communicant

Sylvain Paineau
Schneider Electric
Stratégie et Innovation
Partenariat R&D et Valorisation

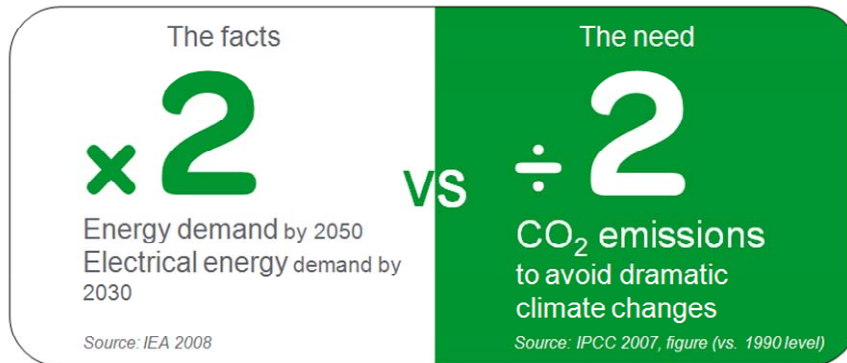
5 Mai 2010



Unique positioning



The energy dilemma is here to stay



Energy management is the key
to address the dilemma



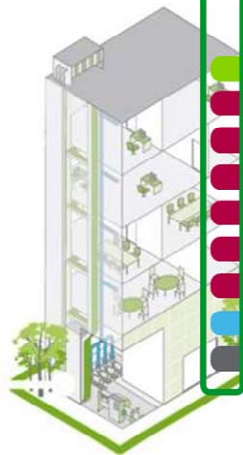
Energy Management brings a set of High tech to Building domain

- Energy is the key challenge for our planet
- Building provide a tremendous area for progress
 - Over 40% of energy consumed by buildings
 - Develop existing buildings towards acceptable levels of performance
 - Target very high performance levels for new buildings
- Beyond passive energy efficiency, 3 stakes
 - Optimize use of equipment and energies
 - Measurement and monitoring
 - Boost cooperation between players

Simple software integration

Interoperability and openness
to third party systems

EcoStruxure



- Renewable energies
- HVAC control
- Lighting control
- Energy monitoring & control
- Motor control
- Access control
- Security
- Critical Power & cooling
- Electrical distribution

Green: Make the connection of renewable energy sources easy, reliable and cost-effective

Efficient & productive:

- Measure and control energy, automate, provide relevant diagnosis
- Manage processes
- Make all the utilities of any Infrastructure more efficient

Reliable: Prevent from power outage & quality variance

Safe: Transform and distribute power safely

Autonomous Wireless Multisensors

■ Main requirements

- Enhance Energy Efficiency and comfort of occupants
- Address both New and Existing markets
- Fulfill the application constraints (Robustness, Long life time, Limited Maintenance)

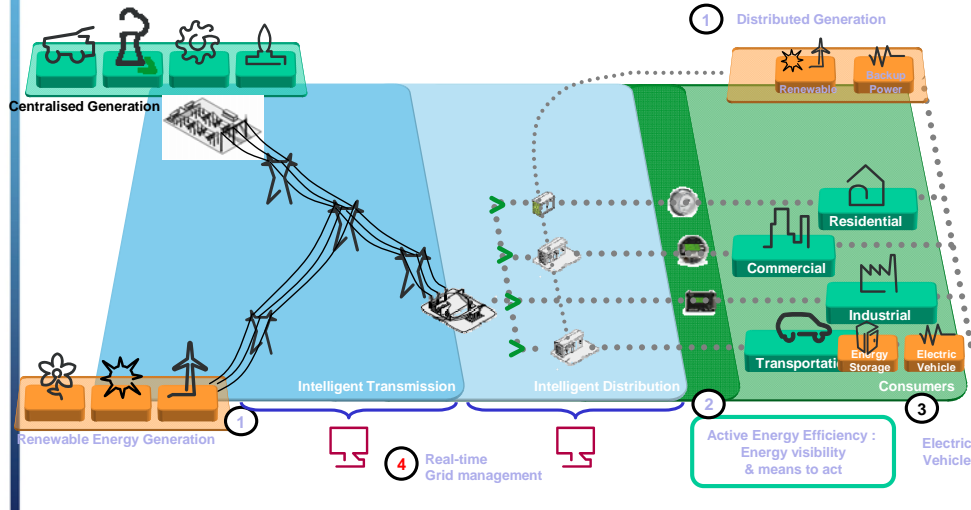
■ Main Characteristics of the Autonomous Wireless Multisensors



- **Ultra low power** wireless sensors platform
- **Mutisensors** (Temperature, Humidity, Light intensity and CO2 sensors)
- **No primary battery**
- **Solar cell** to power-up the sensor
- 802.15.4 wireless communication to comply with ongoing **Green Power Zigbee** Standard
- Can run more than **2 month** in total darkness making it particularly suitable for the application

Supply/demand of Energy started its transformation journey

A quick evolution towards Smart Grid



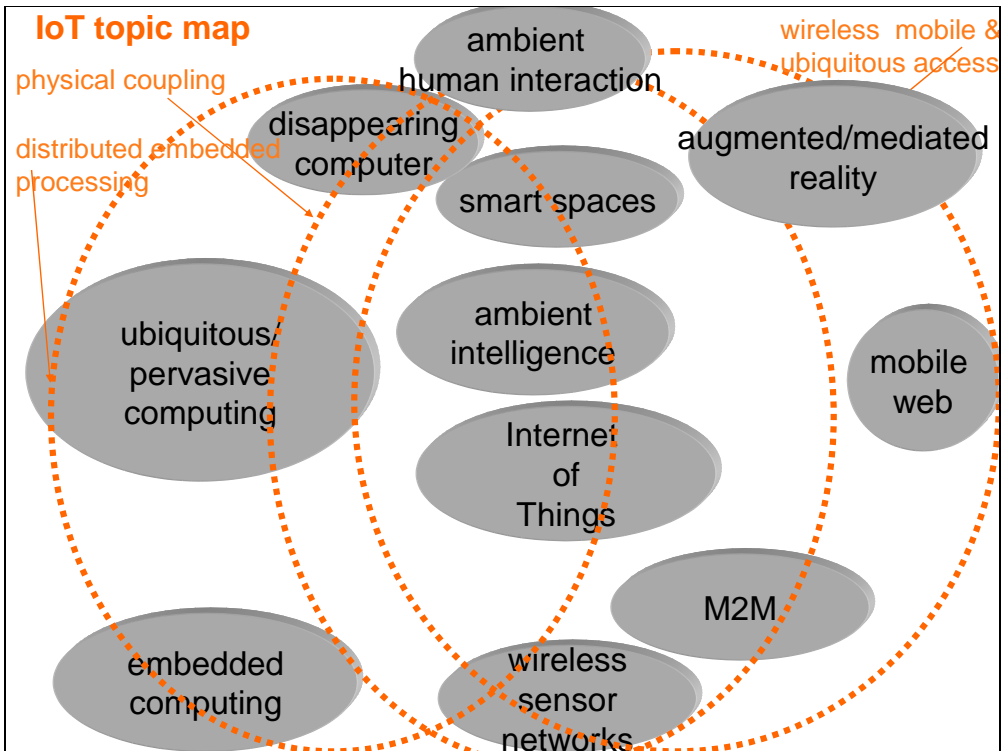
Make the most of
your energy™



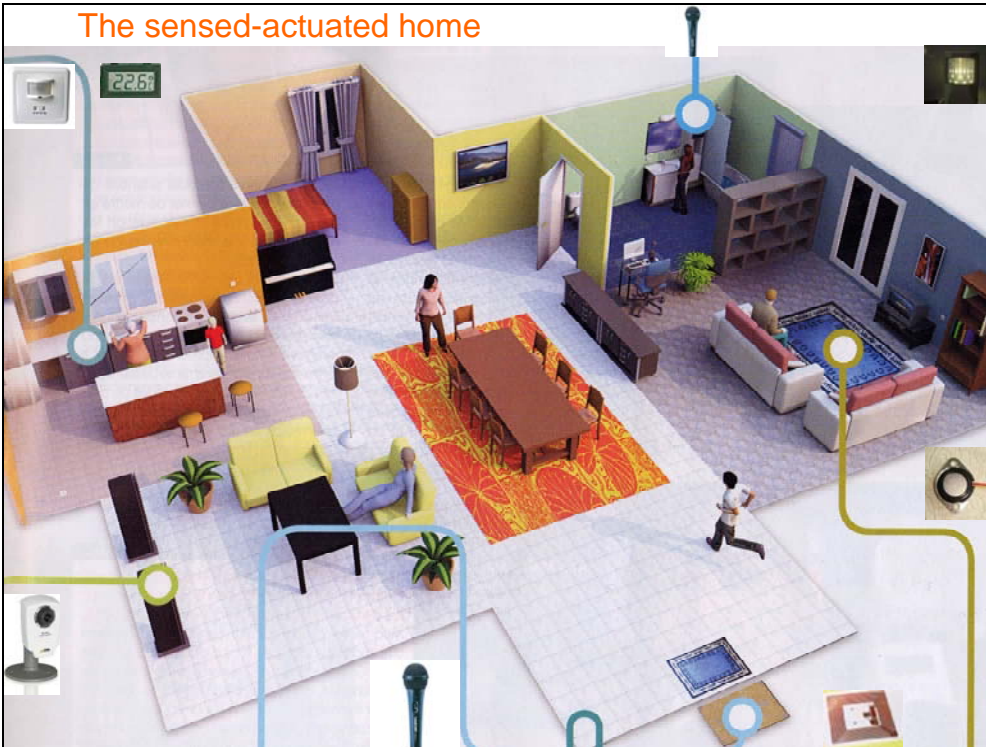
M2M & Internet of Things, from smart spaces to smart cities

*M2M & Internet des Objets, perspectives de recherche,
Orange Labs*
des espaces intelligents à la ville intelligente

Gilles Privat, Research & Development
05-05-2010, Rendez Vous Carnot, Lyon



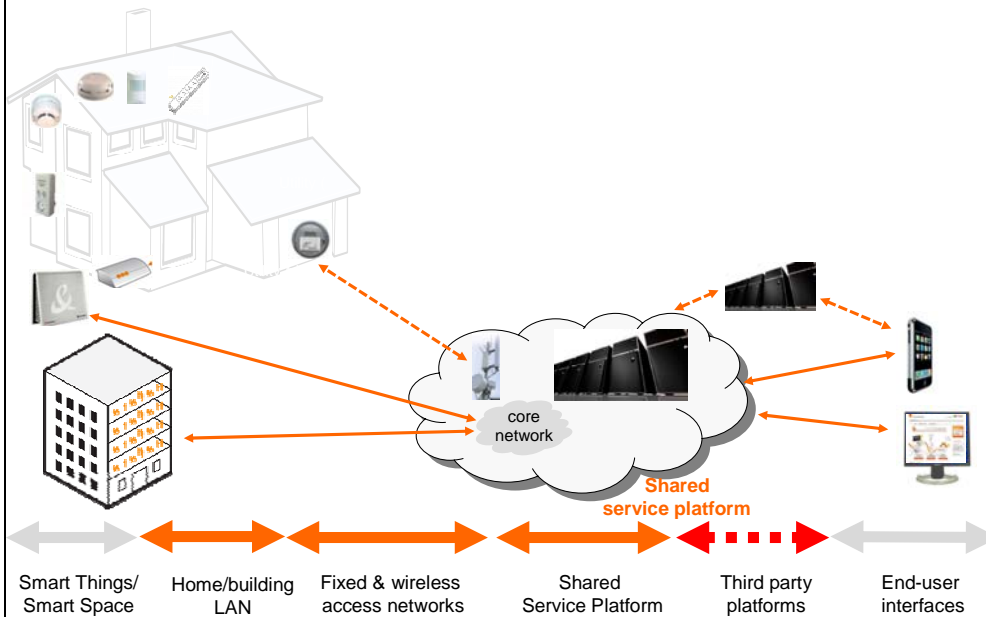
The sensed-actuated home



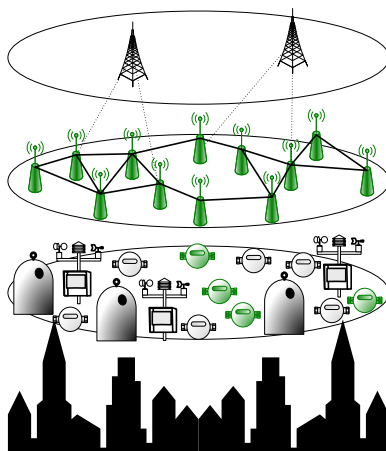
Common IoT/smart space services for the sensed-actuated home

- Home + network of federated sensors & actuators = "smart space"
- Coupled sensor-actuator system may be used for both *human interfaces* and *physical context interfaces*
- Relevant elements of context/content acquired by sensors :
 - State of environment
 - internal temperature, humidity, light, etc.
 - Status of users (present)
 - presence/location/identity of persons
 - level/nature of individual/group activity
- Managing the home as a smart space
 - beyond one-to-one device management and monitoring services
 - providing shared intermediate-level services on top of shared sensor/actuator & network infrastructure

End to end home/building services



Shared city-scale infrastructure for the supervision of physical networks



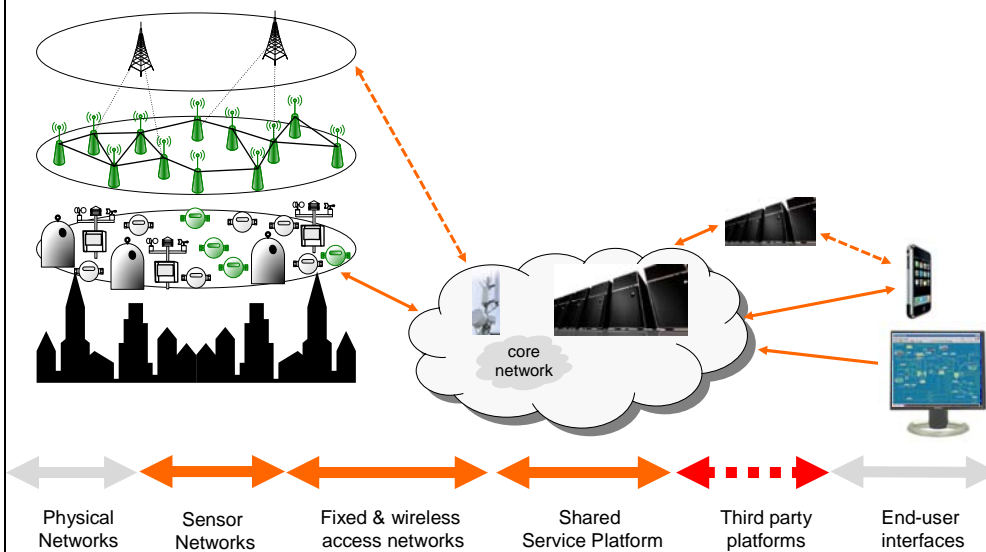
Physical networks

- transportation networks
 - public transit systems
 - car-sharing/bike-sharing networks
 - physical goods distribution networks
- electrical grid
- gas/water distribution network
- waste collection networks

Common data services

- supervisory control (loose coupling)
- distributed control (tight coupling)
- flow analysis
- data warehousing
- data mining

End to end city-scale services



IoT/M2M : reversing the content provision/aggregation dilemma

- no long-term value from commodity data transport (“bit-pipe” role), whatever the network
 - core networks already commoditized
 - operator-managed wireless access will inevitably follow
 - capillary networks are open
 - IoT/M2M is a boundless source of new “content”
 - complements and de-bottlenecks existing “media” services
 - content provision = owning and/or setting up sensors
 - content aggregation = extracting higher level information from raw sensor data, at a multiplicity of different levels :
 - fusion
 - classification
 - recognition/interpretation
 - mining
- ➔ more added value from aggregation than from provision!

Orange Labs - Research & Development –

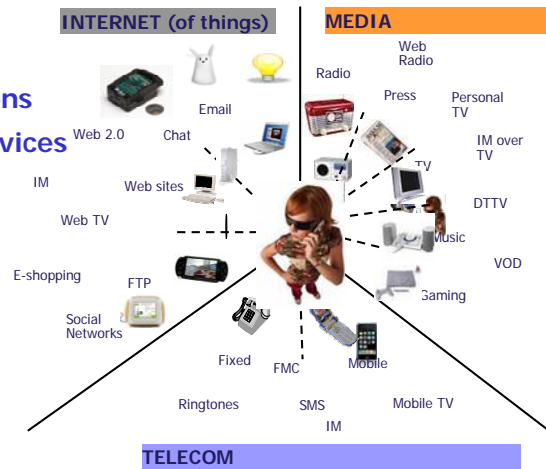
Communicating objects and mobile services

From Internet of things to web of objects

O. Audouin,
Director of External affairs
Alcatel Lucent Bell Labs France

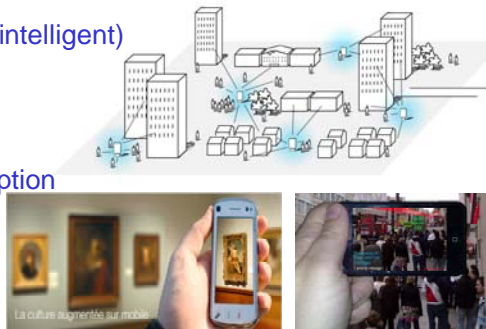


More **producer** than user
User-driven Innovation
Multiplication of connections
Immediate and Simple services
Social networks
Personalized services



Personalized interactions with the (intelligent)
environment (city, building)

- Guiding the user in the city
 - Enriched environment perception
 - Environment configuration
- with high level of automation



User-created content and applications

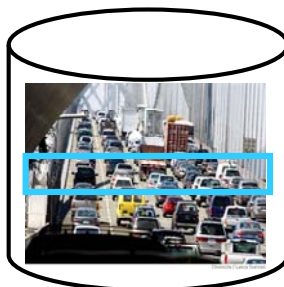
- Leveraging data and services brought by the objects
- « Mash up » with communication and web services



Supported by templates, smart objects and devices, users can instantiate an educational city-game with the click of a button, re-using the existing objects, devices and sensors in a city context.



Mary is walking around in Lyon, enjoying the atmosphere and, interacting with the city using her mobile device. She is presented with tourist information and local stories as she progresses her walk. She decides to create an interactive, entertaining but also educational city game for her children. She now enthusiastically touches city objects (buildings, furniture, screens, billboards, ..) and (inspired by the existing multimedia information) creates questions, hints, and media snippets for her children. Mary re-uses a public billboard that will display a movie of Mary when her children approach it in the summer. She uses existing city-game templates to re-use the Paris city security cameras to record the upcoming adventures of her family.

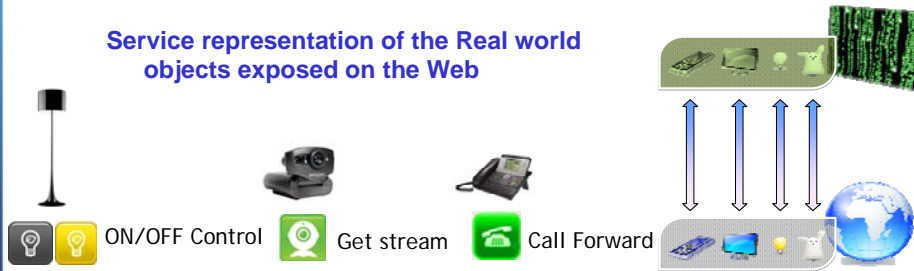


Time to free (web) services from the browser as we know it - and free Internet of Thing applications from their current silos !

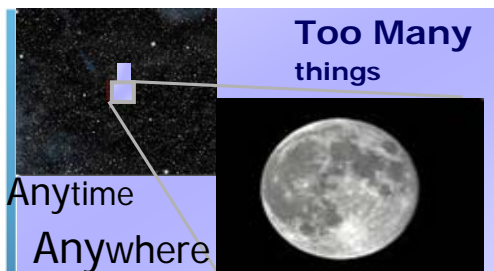
Invent new applications leveraging real-world object exposed using web technologies (smart environments)

Personalised and context aware service, Natural interfaces,
user-created applications

Service representation of the Real world
objects exposed on the Web



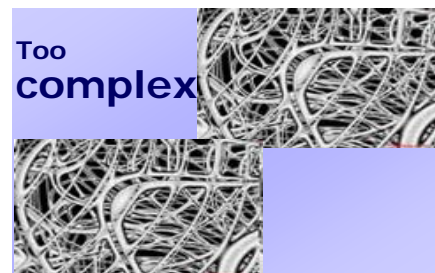
Intermediation: Interoperability, composition, end-to-end trust management



Anyway
AnyThing

- ☐ Easy and ubiquitous connection
- ☐ Hybrid infrastructure/ad hoc networks
- ☐ Agile and self-reconfigurable networks
- ☐ Security, privacy, trust

- ☐ 6 billions of persons -> 60 billions of objects
- ☐ Identification of objects and addresses
- ☐ Data volume
- ☐ Traffic diversity



Scenario « aeronautic » – Airbus

Over the last century, aviation has evolved to become a driving force for the global economy. To address the challenges related to the expansion of air traffic, to the dramatic increase of jet fuel price, to environmental concerns, and to security and safety, the aerospace industry is seeking technological and process innovations in aircraft design, manufacturing, operation, maintenance and traffic management.

In this context, Aircraft Health Monitoring (AHM) is one of the major challenges of R&D activities supported by aircraft manufacturers. This activity aims at proposing an innovative and comprehensive Global Aircraft Maintenance service for future aircraft customers, given the relative importance of maintenance costs for Airline Companies with respect to other types of costs such as customer services, flight operation, flight traffic, etc... At present, the main targets of AHM include the Airframe (Structure mostly), the Aircraft Systems and the Power plant (Main Engine and APU – Auxiliary Power Unit).

AHM focuses on the prediction of failures to prevent structure or system damages by anticipating the maintenance action necessary to avoid “events”. Such predictive service is especially relevant to the Structure Health Monitoring (SHM). SHM therefore consists in the monitoring mainly of corrosion, of cracks and of impact damages taking place during aircraft life. Particular attention is paid to SHM due to the fact that integration at aircraft level is not fully demonstrated yet, although SHM technology components have become available for a few years. SHM is expected to contribute to some aeronautic breakthroughs such as *Composite Airplanes* and *More Electrical Aircrafts*, the use of new materials and new systems requiring extended monitoring capabilities of their aging and performances. In addition, there is a potential direct added value for those of aircraft manufacturers which are both Aircraft integrators and Airframe manufacturers.

Wireless Sensor Networks (WSN) can meet the above goal by offering a cost-effective means for continuously monitoring the health of structures and systems. AHM by WSN, is therefore envisioned by major aircraft manufacturers. The wireless architecture is generally considered as a powerful tool to:

- decrease installation costs,
- decrease inspection costs,
- optimize safety margins in mechanical design,
- and consequently, is a means to reduce aircraft weight, fuel consumption and emissions of greenhouse gases.

One drawback to moving toward a wireless network installation is the poor reliability and limited useful life of batteries needed to supply the sensor nodes. Regarding AHM, in addition to the required lifetime (~ 15-20 years), batteries are prohibited since the wireless sensor node is often implemented in locations without temperature regulation (temperature encountered at high altitude are close to -60 Celsius, but can be very high in locations close to the engines) that could result in a drastically reduced yield and safety issues. This limitation has to some extent curtailed the proliferation of wireless networks in that area. However, the batteries can be eliminated through the use of environmental energy capture, raising the theoretical possibility of infinite lifetime, or at least a lifetime similar to that of the aircraft.

In addition to AHM, WSN may find potential applications in other various fields:

- in-flight tests: Airbus A380 carries about 500 km of cables and wiring to which an extra 300 km is added for in-flight tests,
- passengers' in-flight entertainment and services system: complex wiring between, on one side, passenger's armrest, individual screen and light, and plane systems on the other, is complex, heavy, expensive and hard to modify when needed for commercial purposes,
- logistical challenges: by helping managing cargo or aircraft equipment (galley, life vests...),
- active flow control through micro / nano sensors & actuators: active flow control, can offer significant improvements to aircraft wing, helicopter and wind-turbine rotor performance by suppressing detrimental effects of separated flow.

However, whatever the application, common implementation or industrialization requirements will be shared by the envisioned WSN. Firstly, most nodes, even if not actually embedded into aircraft parts (either inserted into metallic assemblies, or buried into composite materials) will not be easily and economically maintainable: this implies a total autonomy vs. energy (no battery replacement), a MTBF similar to that of most aircrafts mid-life before refit, upgrade or maintenance (16 years). Then it is worth to mention that industrialization will be a major concern whatever the design phase; that includes among other issues:

- robustness regarding harsh aircraft environment: temperature (from 500°C close to the engine exhaust, to -60°C far from the engine exhaust!), shocks, pressure change, radiations, fungus, sand & dust, humidity, icing, hail...
- compliance with D0254 and D0178B design standards, and more generally with various certification rules,
- compliance regarding RF regulations, robustness vs. EMC, EMI, ESD, lightning,
- compliance regarding "green rules" such as RoHS and REACH,
- management of obsolescence, recycling capabilities,
- while being preferably standard-based, low-weight, and exhibiting self-identification, auto-diagnostic and self-reconfiguring capabilities,
- not to mention functionality robustness of the network, security (*top priority* of all aircraft manufacturers) and safety for a few specific application areas.

ANNEXE 2 : COMPETENCES CLASSIFICATION

<div>1 : Node 2 : Network 3 : Distributed intelligence 4 : Design rules</div> <div>■ Core competence ■ Existing competence □ Knowledge / no competence</div>											
Challenges	ESTIA	FEMTO	IEMN	JIT	LAAS	LETI	LIST	LSI	MIB	STAR	UT
Design and Integration of Objects											
Energy management object level	■	■	■	■	■	■	■	□	■	■	■
Harvesting, Management, storage, consumption (1,2,3)											
Packaging, integration into materials, sensor (and actuator) integration (1)	■		■	■	■	■	■	■	■	■	■
Deployment and sensors (actuators) calibration					■	■	■		□	□	□
Communication Devices	■	■	■	■	■	■	■		■	■	□
Trust, security and robustness		■			■	■	■	■	□	□	□
Reconfigurable hardware & software, co design and integration	■			■	■	■	■	■	■	■	□
Massive Secure and flexible Networking of Objects											
Communication protocols & information routing in a network with heterogeneous environment (1)	□		■	■	■	■	■	■	■	□	■
Quality of Service standards convergence, provisioning, dimensioning scalability, Models and Control			■	■	■		■		■	■	■
Intermediation substrate				■			■		□		■
Geolocation and privacy (1,2,3)	■		■	■	■	■	■	■	□	■	□
Service Management											
Local Data Fusion (2,3)	□		□	■	■	■	■	■	■		■
Distributed information processing & heterogeneity management (2,3)	□		□	■	■	■	■	■	■	□	■
Ambient and cooperative intelligence				■	■	■	■	■	■	■	■
Information given by each laboratory											

ANNEXE 3 : CONTRIBUTEURS & CONTACT POINTS

ESTIA	Renaud BRIAND Guillaume TERRASSON	(contact point)
FEMTO	Gregory HAYE	(contact point)
IEMN	Charles ANSSENS Stéphane BEAUSSART Alexandre BOE François Xavier COUDOUX Patrick KENNIS Christophe LETHIEN Christophe LOYEZ Paul Alain ROLLAND Nathalie ROLLAND	(contact point)
IT	Hakima CHAOUCHI Serge GOURRIER Daniel KOFMAN Christian PERSON David SADEK Alain SIBILLE Djamal ZEGHLACHE	(contact point)
LAAS	Marise BAFLEUR Michel DIAZ Jean-Marie DILHAC Daniela DRAGOMIRESCU Marc-Olivier KILLIJIAN	(contact point)
LETI	Pierre-Damien BERGER Emilio CALVANESE STRINATI Levent GURGEN Suzanne LESECQ Hughes METRAS Eric MERCIER Laurent OUVRY François PACULL Jean-Benoît PIERROT Antoine ROBINET Marie-Noelle SEMERIA Dominique VICARD	(contact point)
LIST	Jean-Noel PATILLON Karine GOSSE Christophe JANNETEAU	(contact point)
LSI	Jean CAELEN Alain KIBANGOU Salvador MIR	(contact point)
MIB	Thierry TARIS Xavier DELORD Christophe MAGRO	(contact point)
STAR	Christophe MULLER Philippe PANNIER	(contact point)
UT	Dominique GAITI Pascal SALEMBIER	(contact point)