
LIVRE BLANC

OBJETS COMMUNICANTS

&

INTERNET DES OBJETS

VF1.0 – 21 06 2011



TABLE DES MATIERES

Résumé	3
Vision.....	5
Contexte de l'initiative	7
Défis de la conception et de l'intégration des objets	10
Gestion de l'énergie au niveau objet.....	10
Packaging, intégration dans les matériaux, intégration de capteurs (et d'actionneurs)	12
Déploiement et calibration des capteurs et des actionneurs.....	12
Dispositifs de communication.....	13
Confiance, sécurité et robustesse.....	14
Reconfiguration matérielle et logicielle, co-conception et intégration.....	16
Défis liés à l'interconnexion massive, sécurisée et flexible d'objets.....	18
Protocoles de communication et routage de l'information dans un environnement réseau hétérogène	18
Qualité de Service (QoS), convergence des standards, prestations, dimensionnement, modularité, modèles et contrôle	20
Substrat d'intermédiation.....	22
Géo-localisation et protection de la vie privée	23
Défis liés à la gestion des services.....	26
Fusion locale de données	26
Traitement distribué de l'information et management hétérogène	26
Intelligence ambiante et coopérative	28
ANNEXE 1 : SCENARIOS INDUSTRIELS	33
ANNEXE 2 : CLASSIFICATION DES COMPETENCES.....	47
ANNEXE 3 : CONTRIBUTEURS ET POINTS DE CONTACT.....	48

RESUME

Les progrès continus des technologies de la microélectronique et des réseaux de capteurs permettent maintenant d'envisager le déploiement de services sécurisés et optimisés distribués sur des réseaux d'objets communicants intelligents interconnectés : c'est la vision de l'Internet des Objets. Nous assistons actuellement au déploiement d'une nouvelle génération d'objets interconnectés dotés de capacités de communication, de détection et d'activation (réseaux de transport d'information sans fil, RFID, WSN, etc.) pour de nombreuses applications. Ainsi, l'interconnexion d'objets dotés de capacités avancées de traitement va conduire à une révolution en termes de création et de disponibilité de service et va profondément changer notre façon d'agir sur notre environnement. En bref, le monde physique fusionne progressivement avec le monde virtuel.

Cette vision englobant de simples objets connectés, tels les réseaux de capteurs, jusqu'à des ensembles d'objets communicants plus complexes et plus intelligents, comme l'envisage l'Internet des Objets, implique de mettre en œuvre une approche pluridisciplinaire des nouvelles technologies, des concepts et des modèles (développement de circuits intégrés, gestion de l'énergie, systèmes et principes de communication, systèmes embarqués et packaging, acquisition et traitement des données, expérimentation sur le terrain) et suppose de relever de nombreux défis scientifiques, techniques et commerciaux. En pratique, les défis scientifiques et techniques requièrent différentes compétences concernant :

- ✓ L'intégration d'objets intelligents autonomes interconnectés (capteurs, actionneurs, processeurs, etc.) avec des contraintes fortes en termes de consommation d'énergie, de durabilité et d'environnement d'utilisation (milieu physique et chimique) ;
- ✓ La taille gigantesque (des milliards d'objets peuvent être interconnectés) des réseaux communicants sécurisés, dynamiques et flexibles et le concept de l'ubiquité de la prestation de service ;
- ✓ La fusion des données issues des capteurs, la gestion du réseau et du service, le traitement de données distribuées et l'intelligence ambiante.

Il est essentiel de lancer des études préalables relatives aux applications et aux marchés en étroite collaboration entre les mondes académiques et industriels, car les solutions techniques qui seront adoptées pourront varier fortement d'une application à l'autre. De plus, l'acceptabilité sociétale, la gouvernance, la standardisation et l'interopérabilité de ces objets intelligents et applications de l'Internet des Objets doivent être pris en compte.

Pour aborder les questions techniques et apporter des solutions, les instituts Carnot sont à l'origine d'une initiative lancée en 2010 sur le domaine. Elle regroupe des instituts Carnot de l'alliance Carnot TIC-MNT (CEA LETI, CEA LIST, LAAS, LSI, STAR et Télécom & Société Numérique), des centres de recherche public (ESTIA, FEMTO-ST, IEMN, MIB et UTT) et plusieurs industriels (Orange, Alcatel Lucent, Thalès, Schneider Electric, Airbus et Auchan). Les partenaires industriels de cette initiative ont joué un rôle clef en définissant des scénarios applicatifs ambitieux dans des domaines variés (domotique, ville intelligente et verte, logistique, aéronautique) qui ont été utilisés pour structurer la tâche du groupe.

Les objectifs de cette initiative sont d'analyser les défis techniques et applicatifs liés aux réseaux d'objets intelligents et à l'Internet des Objets, de susciter une prise de conscience des universitaires, des industriels et des autorités publiques sur ce sujet, et de préparer des projets collaboratifs en réponse aux appels d'offres en cours (FP7, ITEA, projets nationaux ANR, Pôles de Compétitivité, etc.)

Ce Livre Blanc résume les principaux résultats de cette initiative.

VISION

Il existe un consensus dans le monde entier, tant au niveau industriel qu'académique et au sein des institutions publiques en charge des activités de R&D, sur l'impact socioéconomique majeur que préfigure l'Internet du futur. Différents points de vue ou visions existent (cf. « Euro-FGI Vision, An overview on future communications », D. Kofman, Institut Télécom, Décembre 2007), mais ils convergent tous vers le fait que nous nous dirigeons vers l'ubiquité de services personnalisés et la généralisation de la connaissance en termes d'environnement, de contexte et de composition de services, avec une mobilité globale de ces services à l'échelle technologique, administrative et jusqu'aux frontières des terminaux. L'extension du réseau au travers des paradigmes avancés de réseaux (réseaux *ad hoc*, maillés, réseaux véhiculaires) et la fusion des mondes réel et numérique grâce à des technologies comme les réseaux de capteurs et d'actionneurs sans fils (WSANs), les prochaines générations de RFID ou de robots autonomes intelligents, constituent la pierre angulaire de ce qu'on appelle l'Internet du monde réel ou « Real World Internet ».

Cette fusion se fonde notamment sur des ruptures technologiques dans deux domaines principaux : **(i) matériel** : solutions microélectroniques avancées pour objets communicants autonomes intelligents (capteurs, actionneurs, processeurs, mémoires, batteries et récupération de l'énergie, émetteurs/récepteurs – interfaces RF, circuits en bande de base, etc.), l'encapsulation ou le packaging et l'intégration de ces solutions au sein d'environnements fonctionnels et de modes de fonctionnement appropriés ; **(ii) Modèles & Logiciels** : avec des approches innovantes relatives à l'intelligence distribuée et aux Interactions Homme-Machine qui sont aujourd'hui limitées par la flexibilité (configuration, « plug & play », etc.), l'évolutivité (milliers voire milliards d'objets devant être reliés entre eux), la sécurité et le respect de la vie privée, les « business models », le droit et l'éthique. Enfin, la complexité des interactions entre les technologies « hardware », les protocoles logiciels et l'environnement de différents domaines requièrent inévitablement des outils de co-simulation permettant une évaluation du fonctionnement d'un système avant tout prototypage.

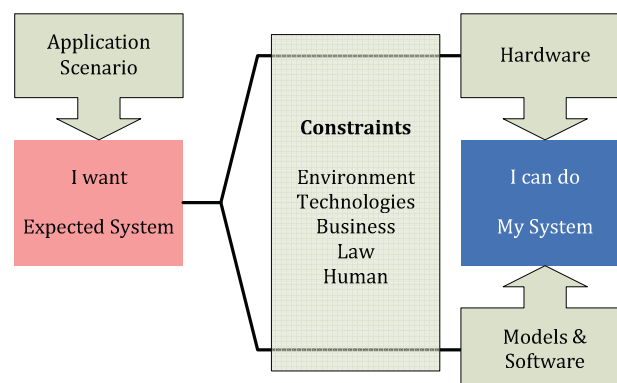


Figure 1 : Comment construire un système ?

Dans un avenir proche, on s'attend à ce que ces objets intelligents aillent bien au-delà des « simples » capteurs et modules RFID aujourd'hui utilisés. Ils seront notamment fondés sur des équipements bas coût, miniaturisés, intégrant des capacités de détection

et/ou d'actionnement accrues, suivant des techniques avancées de traitement de l'information, et supportant une ou plusieurs interfaces de communication en réseau. Ces sous-ensembles pourront être intégrés dans la plupart des environnements et systèmes fonctionnels, à savoir : les terminaux de communication, les véhicules, les vêtements, les appareils électroniques médicaux ou/et portés sur la personne et la plupart des appareils électroniques à usage grand public. Ces systèmes offrent une perception de la réalité augmentée à un utilisateur local ou distant ou à une entité intelligente qui peut alors agir en conséquence. Grâce à l'intégration au sein d'Internet, les utilisateurs seront informés de la situation dans des lieux éloignés et seront en mesure de contrôler à distance un actionneur isolé ou un ensemble d'objets, de mécanismes et d'environnements. Récemment, ce concept d'intelligence ambiante a été réhabilité et la terminologie NED (« Networked Embedded Devices » ou équipements intégrés dans le réseau) a été utilisée pour identifier cette grande diversité d'appareils dotés de capacités de calcul et de communication, capables de s'auto-identifier et s'auto-coordonner pour disposer d'une information collective intégrée dans le réseau (cf. « Real Internet World », Position Paper, Future Internet Assembly, M. Presser *et al.*, Décembre 2008).

L'architecture Internet du futur sera donc constituée d'un noyau et de deux anneaux (figure 2) : le noyau sera composé de l'évolution de l'infrastructure actuelle de l'Internet (accès cœur et convergence fixe-mobile). Le premier anneau sera composé d'une nouvelle génération de terminaux avec des capacités de mise en réseau et donc la possibilité de participer à des réseaux spontanés et auto-organisés. Le deuxième anneau, fondé non seulement sur ces systèmes intelligents, actifs et sensibles à leur environnement, mais également sur les technologies sous-jacentes, permettra la fusion des mondes réels et numériques.

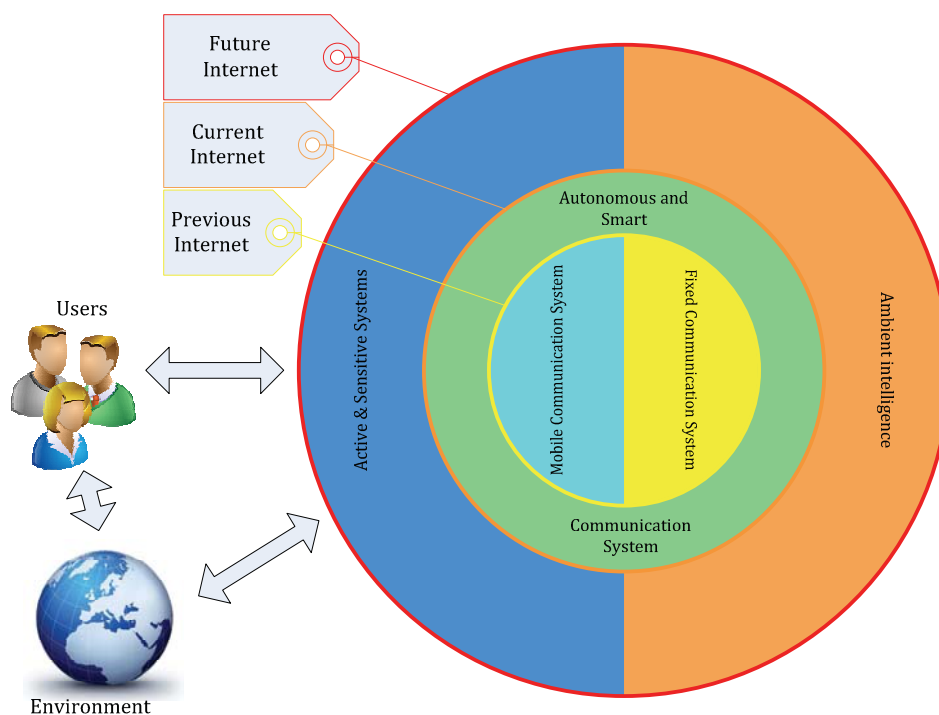


Figure 2 : Internet du Futur – une seule entité ?

Contexte de l'initiative

La présente initiative se concentre sur les technologies et les architectures qui permettront de donner naissance à la deuxième couronne, ainsi que son mode d'interopérabilité avec le reste de l'architecture globale, ouvrant la voie à l'Internet du monde réel (Real World Internet). De très importantes répercussions économiques, industrielles et sociétales sont ainsi attendues. L'initiative a été lancée en 2010 par plusieurs Instituts Carnot et centres de recherche publics reconnus dans le domaine (les instituts Carnot CEA LETI, LAAS, LSI, et Télécom & Société Numérique, et l'IEMN) et différents leaders industriels (Orange, Alcatel Lucent, Thalès, Schneider Electric, Auchan, Airbus) afin de fournir un cadre cohérent de Recherche & Développement pour contribuer à la mise en œuvre d'un « Real World Internet » et démontrer ses impacts dans les domaines d'application sélectionnés. D'autres acteurs ont rapidement adhéré à cette initiative : les instituts Carnot CEA LIST, et STAR et les centres de recherche ESTIA, MIB, et UTT. D'autres contributeurs et partenaires potentiels restent les bienvenus.

L'initiative portera sur les aspects technologiques et architecturaux de différents systèmes innovants qui sont des catalyseurs clés du « Real World Internet ». Les travaux seront structurés selon plusieurs scénarios d'application prévus par les industriels qui permettront de définir les spécifications et les scénarios d'usage et de démonstration. Les travaux seront réalisés dans des projets spécifiques de différentes natures : des projets nationaux, des projets entre instituts Carnot et instituts Fraunhofer, des projets européens (FP7, ITEA, CELTIC...), des projets de Pôles de compétitivité, des partenariats industriels, ... avec un effort d'intégration vers de grandes plateformes applicatives autour des thèmes suivants :

- ✓ Les services ubiquitaires et la mobilité ;
- ✓ Les procédés industriels et la logistique ;
- ✓ Le commerce de gros et de détail ;
- ✓ Les transports et l'aéronautique ;
- ✓ Les bâtiments et les maisons intelligentes ;
- ✓ Les services à la personne, médicaux et de loisirs.

Le tableau suivant liste quelques applications représentatives de ces thèmes et donne les principales caractéristiques et défis des objets interconnectés correspondants.

Tableau 1 : Principales caractéristiques d'objets interconnectés pour certaines applications typiques.

Application	Source d'énergie	Transmetteur Récepteur	Taille	Coût	Quantité	Caractéristiques réseau	mode d'interaction à distance	Challenges
Maison intelligente	Secteur	PLC Débits : Tx: qqes kbps Rx : qqes kbps Distance <50m	<20 cm ³	< 1€	>100 millions	Découverte du service Auto-configuration Découverte du réseau	Interrogation Chargement	Découverte du service
Maison intelligente	Secteur ou batterie	PLC ou Microonde Débits : Tx : qqes kbps Rx : qqes bps Distance < 100m	<10 cm ³	<0.5€	>10 Milliards	Auto-configuration Réseau spontané Codage de réseau	Activation Interrogation	Efficacité énergétique Adressage et routage
Villes intelligentes - Villes propres	Batterie ou photo-voltaïque	Microonde Débits : Tx : 100 bps Rx : quelques bps Distance < 1km	<10 cm ³	<0.5€	>10 Milliards	Auto-configuration Réseau spontané Codage de réseau	Activation Interrogation	Efficacité énergétique Adressage et routage (mesh)
Maison intelligente /surveillance	Secteur ou batterie	Microonde/optique Débits : Tx : 100 kbps Rx : 1 kbps Distance < 500m	<20 cm ³	<10€	>100 millions	Réseau spontané Codage de réseau Centralisé/Distribué	Commande Activation Transfert Données	Sécurité Auto-configuration
Villes intelligentes - Villes propres / surveillance	Batterie	Microonde/optique Débits: Tx : 100 kbps Rx : 1kbps Distance < 5km	<20 cm ³	<10€	>100 millions	Réseau spontané Codage de réseau Centralisé/Distribué	Commande Activation Transfert Données	Sécurité Auto-configuration

L'interface entre les mondes réel et numérique nécessite la capacité pour le monde numérique de percevoir le monde réel et d'agir en conséquence. L'initiative contribuera à la conception d'objets intelligents exploitables au niveau du réseau et correspondant à une nouvelle génération de capteurs et d'actionneurs permettant de répondre aux exigences multiples imposées par la grande diversité de dispositifs dans lesquels ils seront intégrés : capacités réduites en termes de puissance de calcul, de mémoire, de taille, d'exploitation et de stockage d'énergie et enfin d'intégration spécifique dans l'environnement compte tenu des contraintes propres aux applications visées. Un effort de recherche sera également porté sur les architectures des dispositifs qui intégreront ces fonctionnalités et qui, par exemple, effectueront un traitement du signal embarqué, un traitement de l'information distribué et offriront des possibilités d'agrégation de données. Des solutions avancées de SoC (System on Chip) seront ainsi conçues.

Les défis autour de l'intelligence nécessaire à intégrer dans ces systèmes seront décrits et étudiés de concert avec l'analyse de la capacité à communiquer des composantes devant interagir. Un effort particulier sera porté sur l'exploration des architectures de réseaux (*ad hoc*, WSANs, essaims de robots, etc.), ainsi que sur l'exploration des protocoles correspondants. L'auto-organisation et l'autogestion sont essentielles dans cet environnement et les principes conceptuels propres à ces nouveaux réseaux, à savoir

l'adressage, le nommage et l'identification des paradigmes, les solutions de routage adaptées, les solutions de mobilité et d'auto-identification d'éléments, de services disponibles et de capacité de localisation, ne sont que quelques-unes des exigences fondamentales de ces nouveaux paradigmes de réseaux. L'initiative se concentrera également sur l'interfonctionnement des différents systèmes hétérogènes, y compris la fusion avec les réseaux cellulaires et la gestion du réseau et des services. Les solutions de sécurité seront élaborées conjointement avec les solutions de réseaux. Ceci se traduira par une exigence d'architectures auto-organisées et à sécurités adaptables.

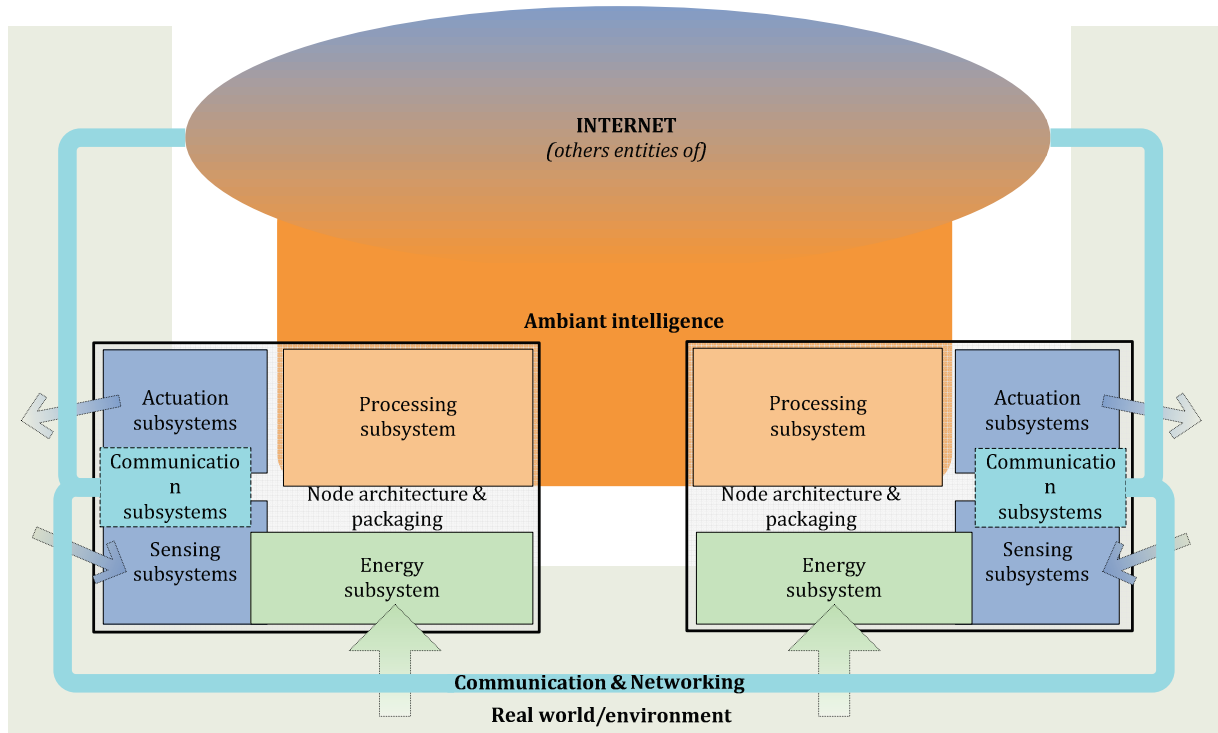


Figure 3 : Description des objets connectés à l'Internet des objets et les trois principaux challenges correspondants : Technologies – Communication – Intelligence.

Les partenaires contribueront à la conception des simulateurs de modèles qui seront requis, des logiciels, notamment les systèmes d'exploitation, et des solutions de mise à jour dynamique des éléments logiciels. Cette activité comprendra la conception, la vérification formelle et le test sur carte des systèmes distribués temps réel étudiés. Des interfaces Homme-Machine (IHM) spécifiques seront également conçues. Des architectures de services avancées, comprenant les composants logiciels (middleware) et les solutions spécifiques pour l'identification des éléments et des services disponibles, seront également proposées.

DEFIS DE LA CONCEPTION ET DE L'INTEGRATION DES OBJETS

Cette partie est divisée en six points relatifs à l'approche technologique :

- ✓ Gestion de l'énergie au niveau objet ;
- ✓ Packaging, intégration dans les matériaux, intégration des capteurs (et des actionneurs) ;
- ✓ Déploiement et calibration des capteurs (et des actionneurs) ;
- ✓ Dispositifs de communication ;
- ✓ Confiance, sécurité et robustesse (relatives aux réseaux) ;
- ✓ Matériel et logiciel reconfigurables, co-conception et intégration.

Gestion de l'énergie au niveau objet

Ces dernières années, de multiples applications impliquant des réseaux de nœuds sans fil en nombre relativement élevé sont apparues. Chaque nœud réalisait le traitement des données issues des capteurs et la transmission sans fil de l'information. De ce fait, ces nœuds devaient être autonomes en énergie, beaucoup d'avantages du réseau de capteurs sans fil pouvant être perdus en cas d'utilisation d'alimentations externes (câblées). Cette contrainte a contribué à limiter la prolifération des réseaux sans fil.

Ainsi, si l'on se restreint à des alimentations internes, les piles qu'elles soient primaires (jetables) ou secondaires (rechargeables) offrent une densité d'énergie élevée à faible coût. Malheureusement, les progrès en termes de stockage de l'énergie ont été beaucoup plus lents que dans d'autres domaines comme les performances des circuits intégrés. De ce fait, au sein d'un dispositif miniaturisé, la pile représente une part importante de la taille et du poids du dispositif. De plus, il y a d'autres inconvénients associés à l'utilisation de piles :

- ✓ Des problèmes d'environnement en cas de perte de capteurs ;
- ✓ Des problèmes économiques liés au remplacement de piles primaires ;
- ✓ Sans parler de la difficulté de remplacer les piles implantées dans des matériaux ou dans le corps humain (les générateurs à base de piles à combustible pâtissent de ce dernier inconvénient).

Heureusement, on peut éliminer les piles primaires grâce à l'utilisation de la capture d'énergie ambiante pour ainsi obtenir une durée de vie théoriquement infinie. Deux options sont envisageables pour cette capture : la récolte d'énergie (source continue) et la récupération d'énergie (source intermittente). La capture d'énergie est la solution long terme pour les réseaux sans fil du type « déployer et oublier » (« deploy and forget »).

Cependant, la disponibilité de l'énergie est alors limitée par des contraintes physiques. Pour un tel réseau autoalimenté, l'énergie est par conséquent un point critique : on doit donc considérer l'énergie comme un des paramètres les plus importants ou comme un point de départ de la conception globale des dispositifs (capteurs, traitement du signal et communication).

En d'autres termes, les méthodes et les technologies de gestion de l'énergie sont des verrous critiques. C'est donc un domaine d'innovation en forte croissance, quoique manquant encore de réels intégrateurs de systèmes industriels qui ne se focaliseraient plus sur un seul aspect du nœud global.

Les sources de récolte et surtout de récupération d'énergie ne sont caractérisées que par leur densité de puissance. Elles sont un moyen de capturer l'énergie ambiante comme la lumière, les flux thermiques et électromagnétiques ou les mouvements mécaniques (*ex. vibrations*). Cette énergie primaire durement gagnée doit alors être efficacement convertie en puissance électrique utilisable. Ceci implique à la fois la conception de transducteurs qui doivent s'adapter aux conditions toujours spécifiques de leur environnement, et une adaptation d'impédance appropriée entre la sortie du transducteur et la charge, quelle que soit sa nature, afin de maximiser le transfert d'énergie. Si nécessaire, n'importe quel circuit convertisseur basse consommation doit pouvoir se déconnecter si la puissance capturée passe en dessous de ses propres besoins. Evidemment, tous les autres dispositifs doivent aussi suivre les règles de conception et de fonctionnement basse consommation.

Une autre étape dans les solutions d'alimentation serait de gérer plusieurs sources d'énergie avec des technologies compatibles et avec des ratios de puissance substantiels.

L'autre aspect de l'alimentation est l'autonomie. Pour être autonome, le système doit avoir une gestion de l'énergie parfaite afin d'optimiser l'alimentation et les performances. Cet aspect devient crucial pour un système disposant de plusieurs sources d'alimentation et de solutions de stockage de l'énergie. De l'intelligence est alors embarquée dans le système pour gérer toutes les contraintes. Comme l'alimentation, l'autonomie dispose de solutions existantes qui doivent être adaptées ou même redéveloppées pour se conformer aux micro et nano systèmes.

Un autre point est que pour certaines activités le réseau doit être actif alors que son environnement n'offre aucune énergie (l'équipement est à l'arrêt, c'est la nuit, ...). Il faut donc qu'une partie de l'énergie capturée auparavant ait pu être stockée. En pratique, le stockage peut être réalisé soit à travers des batteries secondaires, soit des (super) capacités. La première option souffre néanmoins de certains inconvénients des batteries primaires et nécessite un circuit électronique pour contrôler le profil de charge, ce circuit impactant en outre négativement la dissipation d'énergie.

Finalement, la conception d'un capteur sans fil économe en énergie exige une approche globale (holistique) prenant en compte les différents aspects de la consommation d'énergie. Le défi consiste alors dans le développement d'une architecture de co-simulation qui inclut des modèles énergétiques précis pour l'analyse et l'optimisation de l'utilisation de l'énergie dans le nœud d'un réseau de capteurs.

L'énergie opportuniste (les techniques de récolte d'énergie) devra aussi être abordée et générer ainsi de nouveaux défis concernant les procédures d'optimisation de l'efficacité énergétique. Ce sujet est intrinsèquement lié au chapitre 3 « gestion des capteurs au sein du réseau » mais demandera aussi des investigations spécifiques sur les types de codage notamment, afin de converger vers un ratio de consommation bit/Hz/s/DC amélioré.

Packaging, intégration dans les matériaux, intégration de capteurs (et d'actionneurs)

L'intégration dans les matériaux requiert une percée technologique dans le domaine du packaging de microsystèmes et sa compatibilité avec la matrice hôte. En général, les systèmes microélectroniques doivent être manipulés avec précaution. Ils sont souvent mécaniquement fragiles, sensibles aux décharges électrostatiques et aux agents chimiques environnants. Par conséquent, leur insertion dans un système hôte entraîne de nombreux problèmes.

Le matériau peut être le site de contraintes mécaniques : ces contraintes peuvent être concentrées sur les objets insérés conduisant à un haut niveau de stress (analogue à la concentration de stress autour de trous) à l'interface capteur/support ou, dans le cas opposé, peuvent être redistribuées ailleurs dans le support hôte, impliquant ainsi l'apparition de points faibles. De tels phénomènes peuvent aussi altérer les propriétés intrinsèques des matériaux.

Cet aspect devrait être examiné avec soin, au moins au niveau conception et tests mécaniques. Dans les matériaux plastiques, des problèmes plus pernicious peuvent apparaître une fois le micro-objet incorporé à l'intérieur d'un matériau plastique chaud pendant la fabrication. Il peut se produire une redistribution des stress résiduels pendant la phase de refroidissement qui conduisent à des objets avec des formes finales hors limites de spécification. L'insertion dans une matrice plastique est un réel défi.

Les procédés industriels courants comme l'extrusion ou le moulage impliquent une incursion à haute température (typiquement entre 200 et 400°C) et une pression de l'ordre de 200 bars. Les microsystèmes doivent supporter ces conditions difficiles en présentant un packaging approprié ou au moins un pré-enrobage pour être compatible avec les lignes de production industrielles.

Dans les pires cas, le matériau hôte dans lequel on souhaite intégrer des capteurs peut parfois être un matériau chimiquement agressif : le béton ou le ciment sont des exemples typiques avec des $\text{pH} > 12$. Un contact direct entre le matériau et les puces conduirait à des problèmes de corrosion et de diffusion de moisissures dans le système. Dans ce cas, un packaging sera nécessaire.

La définition et la spécification du packaging approprié est un véritable défi car il faut prendre en compte la compatibilité de l'interface entre le matériau support et le matériau du packaging tout en s'assurant que le packaging n'altère pas les performances du microsystème. Il n'existe pas de règles générales de conception car les types de capteurs et le matériau support peuvent varier d'une application à l'autre. Des défis similaires existent pour l'intégration des actionneurs dans l'environnement.

Déploiement et calibration des capteurs et des actionneurs

La phase de calibration qui suit celle de déploiement est une phase fondamentale pour les réseaux de capteurs, car elle conditionne la mise en œuvre et l'obtention de mesures à la fois correctes et valides. Puisque les capteurs constituent le moyen par lequel les systèmes ambiants « connaissent » leur environnement, et donc élaborent leurs stratégies opérationnelles, les mesures doivent être justes et fiables. De façon identique,

comme les actionneurs constituent les « bras » de ces systèmes ambiants intelligents, il est crucial de bien prévoir et de bien contrôler leurs comportements.

Le but du système de calibration est d'abord d'identifier les imperfections possibles d'une mesure, telles que les biais, les dérives et les niveaux de bruit, et ensuite de les corriger. En effet, ces imperfections qui peuvent engendrer des mesures erronées ou des dispersions perturbantes, doivent être minimisées. Dans un cas idéal, la calibration devrait être effectuée en usine. Cependant, plusieurs types de capteurs demandent une calibration réalisée *in situ*. Par exemple, les capteurs embarqués dans des matériels peuvent altérer les caractéristiques (de réponse) d'un capteur particulier d'une façon spécifique, qui peut ne pas être connue au moment où le capteur est produit. Il peut aussi arriver que le coût de production ciblé pour le capteur rende impossible sa caractérisation précise et sa calibration complète. En conséquence, des méthodologies qui peuvent être appliquées à des capteurs de haut niveau, ne sont en fait pas applicables à toute la gamme des capteurs utilisés, et de nouvelles techniques d'auto-calibration sont à développer.

Le déploiement d'infrastructures de capteurs soulève aussi de nombreux problèmes. Afin de mettre en œuvre un déploiement à un coût raisonnable, le système de capteurs doit être capable de produire lui-même une évaluation de son état effectivement déployé, c'est-à-dire qu'il doit être alors capable d'estimer alors son état réel (où sont les capteurs ? comment peuvent-ils être connectés les uns aux autres ? quelle redondance et quelle résilience doivent-ils établir ?). Un tel besoin implique l'utilisation de technologies de base, telle que l'auto-localisation, l'auto-test et les tests croisés coopératifs.

Dispositifs de communication

Quand un système est intégré dans un nouveau matériau et un nouvel environnement, la communication doit utiliser un mode adapté au transport de l'information à travers ces éléments. Les systèmes de capteurs intégrés peuvent inclure la possibilité de transférer des données d'un point du réseau à un autre. Un système de capteurs intégrés communique à travers des matériaux complexes composés d'une structure conductrice et de différentes couches de matériaux. Beaucoup d'efforts de R&D portent sur le développement de systèmes et de protocoles de transmission basse consommation. Les investigations se focalisent sur la consommation énergétique, la taille, la transmission et la performance afin de répondre aux besoins de l'intégration des capteurs. La fiabilité du lien radio est essentielle pour certaines applications (automobile, médical, sécurité, ...). Une approche au niveau système est alors requise pour la garantir grâce, par exemple, au codage, à la diversité, la coopération et la mise en réseau. Il est aussi évident que le développement de l'antenne aura un grand impact sur la performance de la transmission entre microsystèmes. De plus, les signaux radio peuvent être exploités pour la localisation précise ou approximative de dispositifs communicants, ce qui ouvre la voie à de nombreuses applications ou services géolocalisés.

Le sans-fil dans la gamme 100 MHz à 10 GHz est le plus polyvalent et a été beaucoup étudié dans le passé, bien que dans certains cas très spécifiques, d'autres modes comme le filaire (PLC par exemple) ou l'optique peuvent être utilisés. La conclusion à retenir est que dans une majorité d'applications, la partie communication du nœud du capteur sans

fil est le principal contributeur à la consommation globale, bien au-delà des éventuels sous-systèmes capteur et microcontrôleur.

Néanmoins, la consommation en mode actif a encore un impact sur la gestion de l'énergie et sur le choix et la conception de la source d'énergie, même si c'est de moins en moins la première source de diminution d'énergie, puisque le nœud du capteur passe généralement plus de 99% du temps dans un mode repos pendant lequel il consomme quelques 100 nA, permettant ainsi une durée de vie de plusieurs années.

Les piles à faible coût, de petite taille, jetables et/ou biocompatibles présentent typiquement une capacité de courant crête inférieure aux besoins réels instantanés de la partie radio en transmission ou réception. Par conséquent, l'objectif de réduction de la consommation en mode actif est toujours pertinent.

Le sous-système communication sans fil doit faire face à de fortes contraintes de packaging et d'intégration, comme souligné précédemment. Bien que le circuit radio n'occupe qu'une taille limitée, les lois de la physique pour la conception d'antennes conduisent à des compromis taille-efficacité poussant la sélection de la fréquence radio vers de plus hautes valeurs, toutefois moins appropriées aux objectifs de basse consommation et de faibles courants de fuite du circuit radio en fonctionnement.

Par conséquent, la majorité des capteurs communicants est maintenant dans la gamme des 800 MHz à 2,4 GHz, bénéficiant de bandes sans licences mais encombrées.

La vision de solutions en rupture consiste :

- ✓ soit dans l'optimisation de chaque brique dans une approche « classique » d'une matrice croisée systèmes/compétences, nécessitant une coopération étroite entre chercheurs de domaines très larges, spécialement pour la mise en place des flots de modélisation et de conception ;
- ✓ soit dans l'analyse approfondie des besoins applicatifs spécifiques et l'adaptation d'une solution à ces besoins, en évitant alors les approches génériques, au détriment de l'optimisation des coûts du fait de l'absence de marchés de masse critiques.

Finalement, le caractère défendable et reconfigurable est fortement souhaité pour de tels objets et capteurs intelligents du futur, et des investigations sur les nanotechnologies émergentes sont très attendues, en particulier si on considère l'environnement, les nouvelles activités de recherche relatives aux capteurs biocompatibles et les nouveaux actionneurs avec de nouvelles dimensions physiques (fluidique, thermique, piézoélectrique...).

Confiance, sécurité et robustesse

La traçabilité des exigences en matière de sécurité est un besoin réel dans le contexte de la validation et la certification de systèmes critiques. On doit prouver que les dangers ont été identifiés et que toute autre exigence de sécurité a été correctement mise en place. A l'heure actuelle, le travail d'analyse pour la traçabilité lors de la certification se fait manuellement par des experts qui étudient de vastes ensembles de documents. Ainsi, la certification est parfois plus onéreuse que le développement du système. Malgré des progrès récents dans la technologie matérielle, les services omniprésents et ubiquitaires restent peu nombreux et leurs fonctionnalités sont encore loin de ce qu'on

pourrait attendre. Une des raisons majeures est que l'on ne fait pas confiance à ces systèmes. Pour augmenter la confiance, il faudrait garantir que tout service :

- ✓ se comporte comme prévu, sans aucune erreur (correction fonctionnelle) ;
- ✓ est exempt de conditions qui peuvent causer des blessures ou la mort aux utilisateurs, qui peuvent endommager ou entraîner la perte d'équipements, ou qui posent un risque pour l'environnement (sécurité) ;
- ✓ est protégé contre des adversaires malveillants qui ont l'intention de pénétrer ou de détourner le service (sécurité).

Ce type de systèmes présente de nouveaux défis pour sa validation. Certes, pour l'utilisation pratique de ces services, il est essentiel de pouvoir ajouter d'autres services de manière dynamique pour qu'ils puissent être adaptés aux différentes configurations et aux divers besoins des utilisateurs. L'explosion combinatoire provoquée par la multiplication des services reste un problème difficile. De plus, et puisque les services peuvent interagir, il faudrait procéder à une validation finale après le déploiement (validation en ligne).

Les dispositifs intelligents peuvent potentiellement être accessibles de nombreuses manières par un personnel non-autorisé. Des techniques au niveau matériel, aussi bien qu'au niveau logiciel/réseau, doivent être développées afin d'assurer un degré convenable de sécurité, en fonction des exigences applicatives visées.

Les systèmes autonomes sont complexes. Ils englobent un grand nombre de capteurs contrôlés par logiciel (caméras, sonars, etc.) et d'actionneurs (moteurs, roues, bras, pinces, pompes, etc.). En outre, ils intègrent des fonctionnalités avancées, basées sur des données provenant de ces capteurs et actionneurs afin de fournir des services de haut niveau (corrélation stéréoscopique, modélisation de l'environnement, planification de voyage, évitement d'obstacles, navigation, etc.). Ces fonctionnalités sont mises en place en tant que composants logiciels.

En plus de cette complexité, ces systèmes sont critiques, et les logiciels de ces systèmes autonomes doivent aussi gérer l'incertitude et les contraintes temporelles. Les contraintes temporelles sont critiques parce que le système interagit avec d'autres systèmes dynamiques dans un environnement dynamique. L'incertitude est due au fait que l'environnement et ses interactions ne peuvent pas être entièrement et fidèlement modélisées. En particulier, la sécurité de fonctionnement doit être considérée comme une préoccupation majeure. En effet, la plupart des systèmes autonomes peuvent être un danger potentiel pour les personnes. Les composants de systèmes autonomes doivent disposer de solides capacités pour répondre aux incertitudes de fonctionnement. Néanmoins, l'incertitude est souvent la source d'événements et d'interactions inattendus, et peut mettre le système dans un état imprévisible. D'un point de vue logiciel, un mécanisme doit être prévu pour que ces situations soient sous contrôle et qu'elles ne conduisent pas à des conséquences catastrophiques pour le système et/ou l'environnement.

L'objectif est de développer un environnement pour faciliter la conception de systèmes autonomes à base de composants logiciels. Il doit permettre :

1. la construction de systèmes autonomes complexes à partir de composants logiciels hétérogènes (synchrone, asynchrone, en temps réel) ;

2. de fournir une encapsulation complète de propriétés fonctionnelles et extra-fonctionnelles, et le développement des bases et des méthodes pour que les composants soient réalisables ;
3. la prévision des principales caractéristiques du système comme la performance et la robustesse (temporelle et de sécurité), à partir de la caractérisation des composants systèmes et sans explosion combinatoire.

Reconfiguration matérielle et logicielle, co-conception et intégration

En complément des capacités de traitement embarqué qui leur sont nécessaires, les objets communicants devront également intégrer la possibilité de se reconfigurer dynamiquement et ainsi s'adapter aux réseaux *ad hoc* auxquels ils sont susceptibles d'être associés :

- ✓ L'insertion d'objets dans un réseau spontané doit idéalement se produire de façon transparente, c'est-à-dire sans intervention extérieure. Pour cela, l'objet doit avoir la capacité de scanner son environnement proche et d'y détecter la présence d'objets communicants, de façon à se reconfigurer pour s'adapter aux protocoles nécessaires à la communication dans ce réseau (détails dans le paragraphe concerné). Le besoin de haute flexibilité et de reconfigurabilité requiert le développement d'algorithmes avancés pour contrôler l'objet. Les techniques utilisées sont tout à fait similaires à celles couramment employées dans les systèmes à radio cognitive.
- ✓ D'autre part, certains nœuds du réseau peuvent jouer des rôles différents, en fonction de l'évolution du réseau *ad hoc* dans lequel ils se trouvent. Ils peuvent simplement servir de relais ou jouer le rôle de coordinateur pour un sous-réseau. Dans cette dernière configuration, ils peuvent être amenés à contrôler et synchroniser ce réseau spontané, à récupérer les données issues des nœuds et guider l'information collectée.
- ✓ L'objet devra embarquer une puissance de calcul suffisante pour piloter ses ressources, de façon notamment à assurer une bonne gestion de son énergie.

L'exécution de ces algorithmes est réalisée par un processeur embarqué, impliquant des contraintes liées à l'approche logicielle : la surface de silicium nécessaire et la consommation énergétique. Cette dernière est particulièrement importante dans le cas d'objets autonomes. Le budget énergétique d'un circuit intégré programmable est entre 10 fois (DSP) et 100 fois (microprocesseur) supérieur à celui d'un circuit intégré dédié (ASIC). Cela implique qu'une part significative du traitement doit être implémentée au niveau de la couche matérielle (ASIC, fonctions dédiées, compromis mesure-service). L'optimisation de l'architecture de traitement ne devra pas simplement se baser sur des processeurs « faible consommation » mais devra aussi prendre en considération la possibilité d'une reconfiguration au cours du fonctionnement.

Cette notion de reconfigurabilité s'applique à tout type de composants et concerne aussi bien les circuits analogiques que les circuits numériques. En effet, réduire la consommation énergétique tout en gardant un maximum de flexibilité, nécessite le développement de composants analogiques reconfigurables. Par exemple, la conception de nouvelles fonctions analogiques telles que celles liées à la récupération d'énergie devrait être abordée lors des toutes premières phases de conception de l'architecture matérielle. Ces architectures matérielles doivent également s'appuyer sur les

technologies émergentes comme l'intégration 3D pouvant associer une partie radiofréquence, voire même les capteurs (ou actionneurs) et le système de gestion de l'énergie.

Un défi essentiel pour la conception de futurs nœuds consistera à implémenter la reconfigurabilité et la flexibilité tout en gardant un budget énergétique acceptable. Cela passera par l'intégration optimisée du matériel, en grande partie basée sur des circuits analogiques reconfigurables.

DEFIS LIES A L'INTERCONNEXION MASSIVE, SECURISEE ET FLEXIBLE D'OBJETS

Cette partie est divisée en quatre sous-thématiques associées à la communication et à la mise en réseau, en prenant en compte les exigences techniques identifiées au niveau des objets et des couches de protocoles, ainsi que les aspects liés à la sécurité et la protection de la vie privée :

- ✓ Les protocoles de communications & le routage de l'information dans un environnement réseau hétérogène ;
- ✓ La Qualité de Service (QoS), recouvrant la convergence des standards, le dimensionnement, le passage à l'échelle, les modèles et le contrôle ;
- ✓ Les substrats d'intermédiation ;
- ✓ La géo-localisation et la protection de la vie privée (en lien avec le défi de la gestion des services).

Dans le contexte de l'Internet des Objets, diverses technologies hétérogènes seront disponibles, depuis les objets connectés jusqu'au réseau. Ainsi, il sera important d'investiguer les synergies entre ces technologies hétérogènes afin de mieux adresser différentes fonctionnalités dans le réseau, que ce soient des fonctions classiques telles que le routage, la mobilité et la sécurité ou de nouvelles fonctions telles que la connectivité intelligente des objets, l'usage de la radio cognitive, ou de nouvelles techniques. Les approches dites « cross-layer » seront d'un fort intérêt, de même que d'autres qui devront aussi faire l'objet de recherches.

L'Internet des Objets n'est pas simplement une évolution de l'Internet actuel pour connecter des nouveaux « nœuds », c'est-à-dire des objets, mais c'est aussi la nécessité d'introduire de nouveaux paradigmes de communication spécialement conçus pour ces objets. Dans tous les cas, les problématiques liées à la connectivité, à la transmission efficace des données, à l'accès simplifié aux services etc. seront essentielles. Les contraintes ne seront pas seulement associées aux ressources limitées dont disposent ces objets communicants, mais aussi à l'hétérogénéité des équipements, au passage à l'échelle en termes de nombre d'objets connectés, et à la sécurité. L'architecture globale de l'Internet des Objets reste une question ouverte : les objets doivent-ils être intégrés dans une approche de convergence « tout IP » et implémenter des piles de protocoles IP légères (*ex.* 6Lowpan, voir aussi IPSO: IP for Smart Object Alliance), ou bien doivent ils être connectés à des sous-réseaux locaux basés sur des techniques de communications différentes, et interconnectés avec des passerelles spécifiques telles que les passerelles sémantiques aux réseaux IP d'accès ou cœur ? Il est aujourd'hui difficile de répondre à cette question, et les deux approches doivent faire l'objet de recherches afin d'essayer de résoudre les problématiques propres à chacune.

Protocoles de communication et routage de l'information dans un environnement réseau hétérogène

L'hétérogénéité des objets touche divers aspects : leurs natures et fonctionnalités, leurs caractéristiques (fixes ou mobiles), les types de ressources, les médias et modes de

communications (synchrones, asynchrones, multi-sauts, diffusion) et les types d'applications.

Au-delà de l'étude des synergies possibles entre technologies hétérogènes, il est important de classer les objets connectés hétérogènes : (i) selon leurs fonctionnalités, leurs propriétés, leurs niveaux de mobilité et leurs ressources ; (ii) selon leurs capacités en termes de calcul, mémoire ou énergie, selon leur aptitude à supporter les échanges synchrones ou asynchrones, diffusion ou *ad hoc* ; (iii) leurs applicabilités au regard des types de services à supporter.

Concernant les fonctionnalités des objets hétérogènes connectés, il faut identifier et classer les nouvelles fonctions qui seront sources de nouveaux trafics dans le réseau. Pour les objets existant aujourd'hui, on peut par exemple identifier les nouvelles fonctions suivantes : l'identification pour le suivi des objets, le monitoring de l'environnement avec des capteurs et actionneurs, etc. Il sera ainsi très intéressant d'analyser les nouveaux modèles de trafic associés et plus particulièrement leurs exigences techniques vis-à-vis du réseau.

Sur la base des caractéristiques des objets communicants, le modèle de communication à mettre en place pour les interconnecter devra nécessairement être capable de s'adapter aux ressources limitées et à l'hétérogénéité de ces objets. Il devra aussi être capable de supporter une très forte densité de ces objets dans le réseau et ainsi permettre le passage à l'échelle. La mise en réseau de ces objets impliquant l'identification, l'adressage et le nommage de ces objets, renverra nécessairement à l'époque où l'adressage IP a été mis en place pour permettre l'interconnexion modulaire/évolutive (« scalable ») d'un très grand nombre de réseaux hétérogènes. Toutefois, la technologie IP est relativement « gourmande » en termes d'utilisation de ressources alors que celles-ci sont a priori rares dans la plupart des objets communicants envisagés. Ainsi, concevoir un plan d'identification et d'adressage « scalable » et prenant en compte les contraintes en termes de ressources et d'énergie, est l'un des verrous les plus importants à lever pour permettre une interconnexion efficace des objets communicants. L'adaptation du plan d'adressage IP (comme proposé par le groupe de travail 6LOWPAN de l'IETF), la conception de nouveaux adressages, ainsi que l'interfaçage IP de ces derniers pour permettre l'interconnexion à des réseaux IP, devront tous faire l'objet de travaux de recherche.

Une fois résolus l'identification et l'adressage des objets communicants, des mécanismes adaptés devront être conçus pour permettre le démarrage (« bootstrapping »), l'auto-configuration et la découverte des objets voisins (« neighbor discovery ») nécessaires à l'établissement de la connectivité entre objets et le maintien du réseau d'objets. Là encore, ces mécanismes devront être capables de s'adapter aux contraintes de ressources et d'énergie.

Ensuite, lorsque les objets communicants disposent d'adresses, ils doivent être capables de transmettre et relayer le trafic d'un objet vers un autre en direction de la bonne destination, et ce de manière fiable et « scalable ». Ici, les recherches devront porter sur les modèles de transmission/« relayage » du trafic entre objets tels que la diffusion (« broadcasting »), le routage IP, le routage ad-hoc, le routage tolérant aux délais et interruptions, etc. Là encore, la prise en compte des contraintes en termes de ressources et d'énergie est nécessaire, de même que pour la gestion de la mobilité des objets

communicants. Sur ce point, la localisation et le suivi des objets peuvent être exploités pour un « relaying » efficace des données. Deux approches principales devraient être considérées : la première, similaire à l'approche IP, permettra la transmission du trafic de bout en bout (« end to end »), et la seconde s'appuiera sur l'utilisation de passerelles, telles que par exemple des passerelles sémantiques, qui interconnecteront des sous-réseaux d'objets au reste du réseau et interpréteront et traduiront les communications d'un sous-réseau à un autre.

En fait la conception du réseau de communication nécessitera de traiter en parallèle la conception du modèle de communication pour la connectivité entre objets, de même que le modèle de communication pour la connectivité d'un objet, ou d'un réseau d'objets, vers un autre réseau tel que l'Internet. Dans le premier cas, les travaux de recherche pourraient conduire à l'élaboration d'un nouveau modèle de communication exploitant de nouveaux paradigmes tels que les communications autonomiques, ou conduire à l'adaptation de modèles de communication existants tels que le modèle Internet. Dans le second cas, comme mentionné précédemment, les recherches vont poursuivre les travaux en cours (tels qu'à l'IETF ou IPSO) concernant l'adaptation du modèle IP actuel dans l'optique d'étendre la connectivité à ces nouveaux nœuds, c.à.d. objets, ou de concevoir des passerelles protocolaires spécifiques pour interconnecter ces objets à un réseau cible, c.à.d. l'Internet, et permettre de concevoir et d'accéder à de nouveaux services construits sur ces objets et accédés à travers un réseau convergeant « tout IP ». Ce dernier scénario attire tout particulièrement les acteurs des télécommunications mobiles.

Pour conclure, le modèle de communication qui sera conçu, aussi bien entre les objets que des objets vers le réseau global tel que l'Internet, devra intégrer les nécessaires mécanismes de sécurité, là encore adaptés à des ressources et niveaux d'énergie limités, pour assurer la confidentialité de l'information et le respect de la vie privée.

Qualité de Service (QoS), convergence des standards, prestations, dimensionnement, modularité, modèles et contrôle

De nos jours, nous expérimentons une nouvelle évolution d'Internet. Des milliards d'équipements connectés à Internet fourniront de l'intelligence numérique et de la connectivité pour presque tous les produits et les appareils commerciaux et industriels, étendant l'emprise d'Internet sur la plupart des aspects de notre vie. C'est le concept de la dissémination d'Internet. Internet évolue progressivement vers une infrastructure globale de communication offrant de nouveaux services temps réel en complément des applications traditionnelles de recherche de documents.

Avec Internet devenant de plus en plus présent dans nos activités quotidiennes, les interruptions de service du réseau ou même les dégradations significatives de la qualité de service deviennent plus critiques. Pour éviter l'engorgement du réseau et les dégradations de service qui en résulteraient, les fournisseurs de services internet doivent correctement dimensionner le cœur du réseau et les interconnexions donnant à l'abonné l'accès à Internet. Dans le contexte actuel de concurrence, ils ne peuvent pas se permettre d'installer des capacités excédentaires et de ce fait ont besoin de méthodes de planification efficaces. Le but de ces méthodes est d'assurer un réseau solide qui pourra croître pour faire face aux futurs besoins.

L'évolution des réseaux actuels vers des solutions « tout-IP », vers l'Internet des Objets, prend différentes formes, alors que les grands groupes de télécommunications traditionnels (telcos) migrent vers les réseaux de nouvelle génération à partir des recommandations de l'ITU et de l'ETSI, tandis que les fournisseurs de services Internet (ISP) développent leurs réseaux IP orientés vers des réseaux multi-services, s'appuyant davantage sur les spécifications IETF. Les principales caractéristiques des réseaux de nouvelle génération sont une séparation des fonctions (contenu, service, transport) et l'utilisation d'un réseau par paquet pour fournir des services multiples, avec l'ouverture et la convergence sur la couche IP.

Afin d'avoir un réseau ouvert capable de transporter des flots multiples et différents services, et qui devrait aussi permettre de connecter toutes sortes d'équipements dans le monde, y compris toutes les séries de capteurs, tout en conservant l'interactivité, il est nécessaire de s'assurer qu'un ensemble minimum de conditions relatives à la Qualité de Service (QoS) sont remplies. Par exemple, le débit, le retard maximum, le « jitter » et la perte en ligne doivent être correctement conçus ou garantis pour un grand nombre de sessions multimédia d'un bout à l'autre.

Des mécanismes pour assurer le QoS permettraient aux ISP de fournir de nouveaux services et aux Fournisseurs de Réseaux de construire des voies de QoS. Cependant, le QoS peut conduire à des problèmes complexes dans les réseaux IP, bien que les réseaux telcos historiques aient été conçus pour fournir un niveau garanti de QoS, au contraire de l'Internet actuel qui ne fournit qu'une connectivité « au mieux » (« Best Effort »).

Perte de paquets, délai de latence et « jitter » sont les principaux paramètres de QoS, décrivant ainsi la performance du réseau et donc les caractéristiques de qualité du trafic IP. Trois stratégies et approches fondamentales existent pour maîtriser le QoS sur Internet, solutions très différentes dans leurs principes, mécanismes, architectures, déploiement et difficulté :

- ✓ la première approche suppose que les réseaux sous-jacents sont capables de fournir la QoS demandée : rien n'est à faire dans l'architecture internet pour ce qui relève de la QoS. C'est la solution technique la plus simple basée sur l'hypothèse que, quel que soit le trafic envoyé, l'infrastructure du réseau et son équipement fourniront toujours une QoS suffisante. Ceci signifie que le réseau doit être mis à jour et amélioré, autant et dès que nécessaire, de façon telle que le réseau fournisse toujours la QoS nécessaire pour tout le monde. Cette supposition repose sur l'expérience que jusqu'à ce jour la technologie matérielle du réseau continue à s'améliorer en ligne avec la demande. C'est une solution statistique et long terme, implantée par le gestionnaire du trafic avec l'espoir d'être capable de garantir que presque tous les liens seront en sous-charge la plupart du temps. Ainsi, en réalisant un monitoring sur des périodes suffisamment courtes, les liens qui approchent de la saturation devront être détectés et mis à jour. Evidemment, les recherches en monitoring, en gestion du trafic, en optimisation de la topologie et en déploiement à temps des mises à jour, sont nécessaires.
- ✓ La deuxième approche reconnaît que les réseaux actuels ne peuvent pas fournir de la QoS dans tous les cas, mais elle suppose que des améliorations de l'Internet actuel peuvent être ajoutées pour fournir une QoS acceptable. Cette approche part de l'Internet « Best Effort » actuel et développe différents mécanismes d'optimisation.

Comme quelques réseaux existants ne peuvent garantir une QoS, des améliorations sont nécessaires et ainsi de nouvelles conceptions et solutions doivent permettre d'améliorer l'Internet actuel « Best Effort » en introduisant des solutions d'optimisation. Cette approche satisfera les besoins en QoS de l'utilisateur dans certains cas, mais le résultat de ces mécanismes d'optimisation dépendra toujours des capacités maximales de QoS des réseaux sous-jacents. Ici encore par conséquent, on fait appel à une solution statistique, moins coûteuse mais aussi sujette à des problèmes de conflit. Afin de minimiser ces problèmes, les fournisseurs de réseaux peuvent réaliser un monitoring afin de définir de manière adéquate leur capacité d'utilisation acceptable avant toute mise à jour. Par conséquent, dans notre vision, la recherche sur les mécanismes nouveaux ou optimisés, protocole et architecture (*i.e.* respectivement ECN..., DCCP..., proxys...) et une comparaison (partielle) des modèles est nécessaire.

- ✓ La dernière approche propose de construire une nouvelle architecture de réseaux qui doit être capable de fournir aux utilisateurs de réseau n'importe quelle QoS demandée. Les utilisateurs recevront la QoS qu'ils demandent. La conception d'une telle solution n'est pas une tâche facile puisqu'elle demanderait d'utiliser l'IP et, en même temps, d'être aussi générique et ouverte que l'Internet actuel. De plus, il est nécessaire d'être capable de suivre et gérer toutes les demandes et ressources Internet. En clair, concevoir, développer et déployer une telle solution conduit à une grande complexité, d'une part pour définir une solution, et d'autre part pour montrer que le coût de son déploiement est raisonnable. En particulier, il est nécessaire de signaler le passage de l'information entre éléments afin de réserver les ressources, de réaliser le contrôle de l'admission et le routage des paquets vers certaines voies, de gérer les priorités de trafic et d'utiliser les protocoles de transport adéquats, ce signal permettant les transferts d'information entre utilisateurs et différents Systèmes Autonomes (AS) ou entre AS sans fournir de fonctionnalité pour gérer les priorités d'utilisation des ressources du réseau.

Le degré de difficulté s'accroît pour chacune de ces approches, la plus difficile étant la dernière qui doit être aussi générique et ouverte que l'Internet actuel, alors qu'en même temps, il faut être capable de garantir une réponse à toutes les requêtes et gérer toutes les ressources. Dans notre vision, une proposition pour de nouvelles solutions peut être faite dans les domaines de l'architecture QoS, de la qualité d'expérience et des préférences utilisateur, du plan de contrôle, des protocoles QoS, des signaux et de la synchronisation inter domaines, des abstractions et mappings multi-technologies, de l'optimisation des réservations hôte à hôte (« host-to-host »), de modularité en modèles complets d'architecture et de déploiement de classes de services.

Substrat d'intermédiation

Une condition préalable pour le déploiement de services provenant de différents objets communicants basés sur des technologies hétérogènes et interconnectés de façon hétérogène est un « substrat d'intermédiation » qui permettra l'auto-découverte, la connectivité, l'échange d'informations entre les objets – réseaux – et – utilisateurs, ainsi que la traçabilité des transactions qui seront nécessaires dans un environnement sécurisé.

Il faudra résoudre un certain nombre de questions techniques, parmi lesquelles :

- ✓ La capacité d'auto-découverte d'objets selon différents niveaux sémantiques (services aux utilisateurs, protocoles, etc.) ;
- ✓ L'interopérabilité entre les protocoles hétérogènes basés sur diverses technologies suivant les environnements (bâtiments, infrastructures, réseaux de télécommunications, etc.) ;
- ✓ Les solutions techniques pour gérer de bout en bout la chaîne de confiance (à travers les différents opérateurs ayant une responsabilité administrative pour gérer les objets), ce qui garantirait à l'utilisateur la fiabilité des services, la protection des données sensibles privées, les mécanismes d'authentification simples et sûrs et la traçabilité des opérations ;
- ✓ La combinaison d'applications avec différents niveaux critiques (par exemple la sécurité et les applications de divertissement fonctionnant sur un même objet), tout en tenant compte des capacités limitées de traitement.

Les études au niveau des architectures doivent également être effectuées, en particulier les questions relatives aux interactions entre architectures centralisées et distribuées. Les applications requerront des objets en mobilité tout en garantissant une connectivité au travers d'infrastructures réseau d'opérateurs et/ou, le cas échéant, par le biais de réseaux *ad hoc* spontanés entre les objets.

Géo-localisation et protection de la vie privée

La géo-localisation consiste à repérer la position géographique d'un objet équipé d'un système GPS (« Global Positioning System ») tel qu'un téléphone portable, un ordinateur ou encore un véhicule. Ces objets étant la plupart du temps associés à des individus identifiés, la géo-localisation peut conduire à une divulgation d'informations personnelles vers des entités non autorisées et, par voie de conséquence, à une intrusion dans la vie privée. Dans un contexte de multiplication de systèmes ubiquitaires, la « géo-privacy » (souvent appelée « locational privacy ») vise à concilier géo-localisation et respect de la vie privée pour des applications liées à l'utilisation de données spatio-temporelles d'un individu. Même si elle n'en est encore qu'à un stade primitif, la géo-privacy cherche à empêcher une entité non-désirée de connaître la localisation géographique passée, présente et future d'un individu. Les méthodes permettant de préserver la géo-privacy peuvent être classées selon trois dimensions principales :

- ✓ Moment et lieu de la protection : il s'avère nécessaire de préserver la confidentialité d'un utilisateur, qu'il soit en ligne (physiquement connecté) ou hors ligne (lors d'un accès futur aux données enregistrées) ;
- ✓ But de la protection : selon le contexte, il est important de garantir la confidentialité d'une personne ou d'un groupe de personnes impliquées dans une application géo-localisée ;
- ✓ Technique de protection : la préservation des données spatio-temporelles d'un individu peut se faire par différentes techniques telles que la perturbation de la géo-localisation, l'utilisation d'algorithmes de cryptographie ou de protocoles de calcul

distribué sécuritaires multiparties, ou enfin l'accès contrôlé à l'information (ex. accès aux données géo-localisées *via* un serveur surveillant les requêtes).

La géo-privacy peut être assurée en utilisant des attaques d'inférence, des mesures d'utilité et de protection des données personnelles, des méthodes d'assainissement (« sanitisation » en anglais) ou un contrôle d'accès.

Une attaque d'inférence utilise des données géo-localisées, complétées éventuellement d'informations auxiliaires, permettant de produire une connaissance supplémentaire. Une attaque d'inférence peut, à partir de traces de mobilité et de contact mesurées par un téléphone, permettre l'identification de points d'intérêts caractérisant un individu tels que sa maison, son lieu et ses horaires de travail, son itinéraire.... Puisque les attaques d'inférence peuvent être utilisées contre les données recueillies (contexte hors-ligne) ou contre une application géo-localisée permettant d'obtenir des informations privées en ligne, elles peuvent également permettre d'évaluer le niveau de protection offert par un ensemble de données ou un système à ses utilisateurs.

Une autre façon de quantifier le niveau de protection de la vie privée consiste à utiliser des métriques plus générales telles que la mesure d'entropie conditionnelle dans un ensemble de données ou le calcul des statistiques globales. Malgré plusieurs solutions proposées dans la littérature, le problème de définition de la mesure du niveau de confidentialité reste encore ouvert. Ceci soulève une interrogation fondamentale : que signifie avoir une « bonne » protection de la vie privée dans un contexte de géo-localisation ? Une personne cachée dans une foule rassemblée dans un espace restreint est-elle mieux « protégée » qu'une personne seule au milieu d'un vaste désert ? Peut-être est-il nécessaire de définir la vie privée selon la différenciation qu'il est possible de faire entre le comportement d'un individu et celui de ses congénères ?

Il faut noter que les méthodes de protection de la vie privée peuvent avoir un impact sur l'utilité (et donc sur la facilité d'utilisation) des données géo-localisées et des systèmes. En effet, si trop d'informations sont supprimées par assainissement, si les algorithmes de cryptographie utilisés sont trop coûteux ou si le contrôle d'accès impacte les performances et l'accessibilité, l'utilité globale du système est alors remise en cause. Cela conduit souvent à un compromis entre le niveau de protection de la vie privée et l'utilité du système. Par conséquent, il est important de pouvoir évaluer l'utilité du système global et, désormais, de mesurer l'impact des méthodes de protection de la vie privée sur l'utilité. Un processus d'assainissement ajoute de l'incertitude aux données et élimine certaines informations sensibles de manière à protéger les données géo-localisées d'un individu. L'utilisation d'un pseudonyme généré aléatoirement remplaçant l'identifiant d'un individu n'est souvent pas suffisante en tant que telle pour assurer un haut niveau de confidentialité. Les méthodes les plus avancées d'assainissement comprennent, en particulier, le sous-échantillonnage, la perturbation, l'agrégation, la couverture spatiale ou le « mix-zone » rendant plus difficile la traçabilité des actions d'un individu.

En utilisant des algorithmes de cryptographie, les systèmes ubiquitaires peuvent effectuer de manière sécurisée des calculs sur les données géo-localisées qu'ils collectent et dont seul le résultat final est connu. Les procédures de contrôle d'accès peuvent être utilisées pour analyser la manière dont une entité externe accède aux données géo-localisées d'individus au sein d'un système. En auditant les requêtes, le

système peut alors décider s'il doit ou non divulguer davantage d'informations, au risque de causer une violation de la confidentialité.

DEFIS LIES A LA GESTION DES SERVICES

La présente partie est divisée en sous-parties traitant de l'approche « service » :

- ✓ La fusion locale de données ;
- ✓ La gestion distribuée du traitement de l'information et l'hétérogénéité ;
- ✓ L'intelligence ambiante ;
- ✓ Les environnements et outils pour la création, la composition et l'orchestration de services ;
- ✓ Les interfaces utilisateurs.

Fusion locale de données

La fusion de données est une technique de traitement de l'information qui vise l'association, la combinaison, l'agrégation, l'intégration et la fusion de données multiples provenant de capteurs le plus souvent hétérogènes. Il s'agit d'extraire des connaissances à partir de toutes les informations délivrées par ces capteurs considérés comme des ensembles et non pris individuellement.

Le problème de l'agrégation et de l'utilisation simultanée des données et de l'information de sources multiples peut être trouvé dans beaucoup de champs d'application souvent liés au besoin d'observer un environnement par exemple avec des sondes plus ou moins fiables, plus ou moins précises et plus ou moins efficaces. La fusion de données est un concept plus général qui recouvre de vastes secteurs de traitement des données : elle inclut la fusion des sources d'information, provenant de capteurs de systèmes de navigation, de diverses bases de données (données de carte, documentaires, modèles numériques de terrain, règles d'expertise) et l'analyse des données comme la fouille des données.

Les problèmes induits par la fusion de données dépendent du domaine d'application : par exemple, comment placer les capteurs dans l'environnement considéré de sorte que l'information résultant de la fusion de données soit optimale ? Quels capteurs choisir et pour quelle fonction ? Comment assurer une bonne couverture de l'environnement observé et des interactions dans cet environnement ? La linéarisation de la couverture d'un environnement par un réseau de capteurs est une question cruciale. Cette question demeure fortement liée à la communication, à la détection, aux capacités de calcul et d'énergie des capteurs déployés.

Traitement distribué de l'information et management hétérogène

❖ Traitement distribué de l'information

Augmenter le nombre de capteurs permet d'obtenir un maillage plus fin de l'environnement observé. Cette augmentation est associée à un accroissement significatif de la quantité de données à traiter. Le traitement de ces données peut être considéré soit au niveau d'un nœud central ou dans un mode distribué au niveau de différents capteurs. Une autre approche consiste à regrouper les capteurs dans plusieurs groupes, chacun dirigé par le capteur disposant des ressources de calcul les plus significatives. Une telle approche permet une meilleure gestion des ressources

énergétiques dans le réseau. Une architecture arborescente peut alors être adoptée de manière dynamique.

Deux niveaux de fusion de données peuvent être envisagés : la fusion de la décision ou des mesures. Dans le premier cas, les capteurs échangent avec leurs capteurs voisins ou avec un nœud central une décision locale, tandis que dans le second cas, ils partagent leurs mesures. En termes de coût de communication, le transfert de mesures brutes est généralement plus coûteux qu'une décision. Dans le cas des réseaux suffisamment denses, une approche hybride peut être considérée, offrant un meilleur compromis entre le coût des communications et la qualité de l'estimation ou de la décision.

Lorsque la décision est prise à un nœud central, les erreurs locales sont généralement facilement détectées et supprimées. Toutefois, l'existence d'un nœud central crée un goulot d'étranglement au niveau du réseau. Selon l'application, il peut être nécessaire d'utiliser un traitement hautement décentralisé. Une telle approche est plus adaptée en termes de dimensionnement et de mise à l'échelle et plus tolérante à l'ajout ou à la suppression d'un nœud ou à des changements dynamiques dans le réseau.

De plus, le développement d'un processus de fusion de données dans un réseau de capteurs doit tenir compte de l'asynchronisme entre les capteurs, la perte possible de paquets en particulier dans le cas de la communication sans fil et les perturbations locales. Les algorithmes de fusion de données doivent être insensibles aux pertes de paquets, ou du moins être en mesure de s'adapter efficacement lorsque la perte de données est partielle ou totale.

❖ « Plug & play », auto-déploiement et management hétérogène

De minuscules dispositifs de détection sont de plus en plus présents dans les applications qui exigent une qualité de service accrue avec la capacité d'adaptation et des propriétés de reconfigurabilité. Cependant, le grand nombre et l'hétérogénéité des dispositifs de détection rendent difficile la gestion avec des outils classiques. En outre, la nature « temps réel » des systèmes de détection impose des actions de gestion critique en termes de temps de ces systèmes fortement dynamiques. L'auto-gestion est donc une propriété essentielle pour les systèmes de détection en réseau. Plusieurs défis points-clés doivent être posés :

- ✓ Le déploiement de capteurs : ce problème a été rencontré par exemple par la communauté Télécom. Cependant, il semble qu'aucun travail n'existe encore aujourd'hui sur le déploiement optimal d'un capteur/actionneur. Au niveau du réseau les indicateurs doivent être définis. La plupart du temps, les capteurs sont placés là où ils peuvent être placés en raison de contraintes externes, et non là où ils devraient être fixés selon les exigences de l'application. Des modèles de type « Building Information Models » seraient utiles pour prendre de telles décisions.
- ✓ Configuration et déploiement automatique du logiciel : ce sont des éléments importants pour les systèmes de détection flexibles car l'utilisateur final n'est ni un expert ni un spécialiste de l'outil logiciel. Tout ce qu'on peut demander à l'utilisateur à ce niveau est une interaction *via* un navigateur Web. Idéalement, on pourrait s'attendre à ce que le système s'auto-configure sans intervention humaine, en réponse aux changements dynamiques de son environnement. La mise à jour du microprogramme de l'appareil, la fourniture de nouveaux services

et la mise à jour des applications sont nécessaires pour les systèmes extensibles. Un logiciel de gestion autonome, sans intervention humaine, serait une étape vers une véritable prise d'autonomie des systèmes de détection. À cette fin, un mécanisme d'événement est nécessaire afin d'informer les acteurs qui sont impliqués dans la prise de décisions sur le déploiement de nouveaux logiciels ou la mise à jour des versions existantes. Le consortium a notamment souligné ce besoin au niveau « Hardware » et « Software » dans le paragraphe « matériel reconfigurable et logiciel, co-design et l'intégration ».

- ✓ Le suivi des performances et l'entretien de ces réseaux de capteurs/actionneurs sont essentiels. Comme les capteurs peuvent être placés à des endroits qui sont difficilement accessibles, la télésurveillance et l'entretien revêtent une importance particulière. Par exemple, quand un ensemble de capteurs ou d'actionneurs est soupçonné d'être défectueux, plusieurs scénarios peuvent être envisagés. Le premier est le cas idéal où la pièce défectueuse est répliquée. Cependant, ce n'est pas toujours possible et une dégradation tolérable pourrait être une réponse. Une dégradation tolérable consiste à ne pas assurer le service complet, mais un service dégradé (par exemple un nombre de données d'entrée réduit, un ralentissement du traitement). Dans certains cas, ceci pourrait être suffisant pour s'assurer que le système offre un mode de fonctionnement alternatif acceptable.

L'objectif global est de fournir un système de détection/d'écoute « plug & play » (PnP). L'utilisateur devrait pouvoir, à partir d'un capteur disponible sur le marché, le brancher sur le système et le dispositif serait alors auto-découvert, auto-configuré, automatiquement mis à jour avec la dernière composante logicielle, et suivi pendant l'ensemble de son cycle de vie. Le domaine de l'informatique autonome travaille sur des questions similaires. Toutefois, les concepts existants doivent être repensés et adaptés aux ressources limitées des appareils en réseau dotés de système de détection, considérant de surcroît les contraintes sévères sous-jacentes, notamment du point de vue temps-réel, et avec par exemple des questions liées à la sécurité ou au système de commande.

Intelligence ambiante et coopérative

❖ Intelligence ambiante et coopérative :

Les réseaux actuels sont composés d'un grand nombre d'éléments (NEs) tels que des routeurs, des pare-feux, et des passerelles chacun d'eux exécutant un ensemble de fonctions élémentaires liées au routage, à la gestion de la sécurité, à la réservation de ressources, à la gestion de la qualité de service, etc. Les fonctions plus sophistiquées comme la configuration des NEs, l'optimisation des tables de routage, ou la gestion des incidents sont principalement gérées d'une manière centralisée, demandant le plus souvent l'intervention humaine.

Cependant, les réseaux doivent faire face aux changements rapides de situations et à des configurations de plus en plus complexes qu'il devient de plus en plus difficile de gérer de façon centralisée et de manière adéquate en raison principalement des contraintes de délai (la collecte et le traitement d'informations prennent du temps) et des enjeux de complexité (centralisation/globalisation des réseaux).

L'idée de l'intelligence ambiante et coopérative est de piloter l'Internet des objets en utilisant des outils provenant du domaine de l'intelligence artificielle. Une plateforme basée sur des agents intelligents distribués permet d'effectuer de manière décentralisée un nombre de fonctions de gestion, en gérant localement des situations simples d'une manière plus réactive.

Chaque agent distribué associé à chaque NE est capable de percevoir et d'observer des événements et des changements dans son environnement. Les agents communiquent avec leurs voisins afin d'améliorer leur connaissance à partir de celle du voisinage, pour ainsi consolider et coordonner les décisions à l'intérieur d'un espace du réseau.

Les caractéristiques des agents sont les suivantes :

- ✓ Décentralisation : aucun agent n'a la vision globale du système et les décisions sont prises d'une manière totalement distribuée ;
- ✓ Réactivité : un agent fait partie de son environnement et ses décisions sont basées sur ce qu'il perçoit de son environnement et sur son état courant. Il prend la vue locale de son environnement (appelée également « vue située ») ;
- ✓ Pro-activité : ce terme regroupe la capacité à définir ses buts et à les réaliser ;
- ✓ Sociabilité : c'est la capacité de distribuer l'intelligence entre les différents agents et de coopérer avec les autres agents du système.

En distribuant les agents dans le réseau, les problèmes sont traités localement, de manière plus rapide et de façon plus simple que dans une approche centralisée, soumise à la latence. Par exemple, un agent peut changer immédiatement la configuration de son NE pour réagir à un problème de charge locale.

Au-delà des problèmes locaux, les agents coopèrent avec leurs voisins pour traiter des problèmes de voisinage : un problème de connectivité peut être détecté par divers agents qui peuvent coopérer pour caractériser le problème de manière plus précise et fournir un rapport synthétique au centre de contrôle du réseau.

Chaque agent maintient sa propre vue du réseau sur les bases de l'information obtenue (i) directement de l'observation locale de son NE et (ii) du reste du réseau en échangeant des informations avec ses voisins. Cette vue centrée sur l'agent et orientée sur l'environnement proche de l'agent est appelée la vue située.

Le principe de la vue située repose sur le fait que les événements survenant dans l'environnement de l'agent sont de plus grande importance pour l'agent que les événements survenant dans une partie éloignée du réseau. Le fait que l'événement local soit connu plus tôt et soit plus documenté et de manière plus pertinente dans la vue située facilite une réaction rapide et appropriée de l'agent.

Les agents vérifient régulièrement les modifications importantes survenant dans la vue située et donc dans l'environnement réseau tel qu'il est vu par chaque agent, peuvent décider d'adapter automatiquement certains paramètres de leur propre NE et demander aux agents voisins de faire de même avec leurs propres NEs. Si un agent détecte localement un problème de sécurité potentiel, il peut renforcer cette information en vérifiant des informations similaires dans son voisinage et ainsi décider d'ajuster une politique de sécurité et/ou de déclencher une alarme de sécurité.

L'utilisation de la vue située implique une coopération implicite entre les agents qui s'influencent les uns les autres au travers de la connaissance qu'ils partagent. La coopération implicite est le mode élémentaire de la coopération. Ce mode est simple, particulièrement robuste et bien adapté aux environnements se modifiant dynamiquement, car il n'implique pas l'établissement d'un dialogue explicite et une synchronisation stricte entre les agents.

Ce qu'un agent est capable de faire est défini dans un ensemble de comportements. Chacun de ces comportements peut être considéré comme une fonction spécialisée avec des capacités expertes, capable de traiter des aspects spécifiques du travail à accomplir par l'agent. Les comportements ont accès à la vue située qui fonctionne en chaque agent comme un tableau blanc partagé par tous les comportements agent.

L'activation, le paramétrage dynamique et l'ordonnancement des comportements au sein de l'agent sont réalisés par un module de planification dynamique. Celui-ci décide du comportement à activer, du moment où il doit l'être et avec quels paramètres. Ce module détecte les changements dans la vue située et l'apparition d'événements internes ou externes. A partir de là, il peut orchestrer la réaction de l'agent aux changements de l'environnement réseau.

Les éléments décrits ci dessus proviennent de la société GINKGO NETWORKS et de la plateforme proposée par cette société. La plateforme fournit des moyens simples et décentralisés pour traiter la complexité croissante des réseaux modernes et de leurs besoins qui sont de plus en plus difficiles à traiter avec les systèmes centralisés classiques.

- ❖ Environnement et outils pour la création, l'agencement et la mise en œuvre de services, et l'interaction avec l'utilisateur :

L'intelligence ambiante est appelée à impacter tous les aspects de la vie quotidienne ; elle constitue un vecteur puissant de développement et d'innovation. Il est nécessaire de fournir des services et des équipements adaptés à toute circonstance, à tout moment et en tout lieu, pour satisfaire les besoins individuels et répondre à des enjeux sociétaux, dans des domaines d'activité très diversifiés.

Il ne s'agit plus seulement d'augmenter les gains de productivité des individus et des organisations mais également de développer des dispositifs technologiques qui améliorent la qualité de vie à l'échelle des individus, des communautés et de la société, et qui, subséquentement, contribue à la sauvegarde de la planète. Il ne s'agit plus de produire des ordinateurs prêts à l'emploi (aux niveaux logiciel et matériel) mais de permettre aux citoyens et aux compagnies de devenir les architectes de leurs propres services. Ces services seront idéalement (re)configurables de manière illimitée, en accord avec les règles de sécurité, la législation et les valeurs du plus grand nombre.

Les enjeux adressés :

- ✓ La mobilité (incluant la persistance et la continuité dans la communication), le déplacement d'objets communicants (avec une connexion intermittente), la sensibilisation et l'apprentissage de l'informatique ubiquitaire, la téléprésence d'individus ou la présence partielle (segments corporels) ;

- ✓ L'identification et la gestion de l'identité d'objets divers sachant qu'au-delà d'un certain nombre d'éléments, l'identité d'un objet perd de son efficacité ;
- ✓ Les propriétés-clés des objets communicants : sécurité, transparence des fonctions, non-intrusivité, reprise de contrôle ;
- ✓ Les interfaces multimodales et les interactions hétérogènes dans l'assemblage et la composition de différents ensembles dans les architectures des systèmes, les négociations ;
- ✓ L'intégration, la coopération (planifiée ou opportuniste) et la capacité d'apprentissage à différents niveaux de granularité ; la gestion de la complexité en résultant ;
- ✓ Les dimensions transversales d'utilisation prenant en compte une approche pluridisciplinaire.

Les enjeux non-techniques couvrent un large spectre de points critiques relatifs à :

- ✓ La « convivialité », l'interaction intuitive (au-delà des critères habituels d'utilisabilité) ;
- ✓ Les phénomènes psychologiques de rejet de dispositifs dédiés à l'assistance des seniors ;
- ✓ Les aspects légaux : sécurité des robots, propriété intellectuelle, droits d'accès à une entité numérique, droits à « l'oubli » (parmi l'ensemble des éléments enregistrés par les dispositifs numériques), dispositions légales relatives aux objets physiques ;
- ✓ La dimension éthique : respect de la vie privée, dignité numérique ;
- ✓ La dimension politique : droits d'expression des citoyens dans des espaces semi-privés.

Un environnement de déploiement de services comporte trois dimensions :

- ✓ Evaluation des services, en termes technique et d'usage (*cf.* « matériel et logiciels reconfigurables, co-design et intégration ») ;
- ✓ Création de services : les systèmes « machine-to-machine » (M2M – communication entre machines) seront incontournables. Ces systèmes hautement interactifs créent des liens entre terminaux mobiles (PDA, smart phones, capteurs,...) et utilisateurs de manière à réaliser des tâches collaboratives dans un contexte d'informatique « pervasive » et ubiquitaire. Du fait de leurs caractéristiques intrinsèques, ils doivent reposer sur des architectures logicielles fortement dynamiques et auto-reconfigurables. Par exemple, dans le domaine de l'automatisation des espaces domestiques, l'introduction de processeurs communicants dans la maison génère un ensemble important d'informations et de ressources de calcul. En termes d'énergie, l'information et les ressources techniques constituent des données potentiellement utilisables pour l'optimisation de la consommation en regard des exigences écologiques. En termes de confort, de sécurité et d'assistance à la personne (seniors, malades,...) les besoins sociétaux sont d'ores et déjà considérables et connaîtront une croissance continue au cours des années à venir. Cependant, les technologies actuellement disponibles ne permettent pas de concevoir des services domestiques qui satisfassent aux

attentes des utilisateurs. Un des problèmes réside dans le fait que la configuration de chaque espace domestique est différente, que les dispositifs fournissent différents services, et que la multiplicité des dispositifs peut être à l'origine de conflits et d'incompatibilités difficilement détectables a priori.

Le premier enjeu est de parvenir à concevoir des services de haut niveau formés de services composites et de vérifier que l'équipement de l'espace domestique fournisse des services en accord avec les attentes exprimées.

Le second enjeu réside dans la gestion du comportement dynamique inhérent à ce type d'application : les services sont créés, interconnectés, et supprimés durant leur exécution. Le caractère de dynamique répond aux contraintes d'adaptabilité des applications distribuées et à la mobilité de ses utilisateurs. Dans le cas d'architectures statiques, des modèles ont été proposés mais ces approches ne sont pas utilisables et il est donc nécessaire de se baser sur des formalismes de modélisation puissants, par exemple les grammaires de graphes qui traitent l'évolution dynamique des architectures logicielles par des transformations de graphes.

- ✓ Accès aux services, interfaces, interfaces Homme-Machine (IHM) : les services fournis doivent non seulement être accessibles à l'utilisateur mais ces derniers doivent également être capables de les surveiller et de les contrôler. Il est donc nécessaire de rester attentif aux questions d'usage et d'ergonomie, par le biais notamment de la conception d'IHM adaptées qui permettent à l'utilisateur de « rester dans la boucle de contrôle », de façon à ce que les systèmes soient plus facilement acceptés. La recherche de solutions innovantes dans le domaine des IHM doit se traduire par des solutions qui permettent aux utilisateurs d'avoir accès à l'état courant du système technique, notamment à la logique qui sous-tend une action système, de façon à ce que ce dernier ne constitue pas une « boîte noire ». L'utilisateur doit ainsi garder le contrôle et être en mesure à tout moment de passer outre aux décisions du système (exception faite des contraintes de sécurité). Dans le domaine de la maîtrise de la consommation d'énergie, l'objectif poursuivi est que l'utilisateur puisse être conscient de son empreinte énergétique, de manière à, dans la mesure du possible, modifier son comportement grâce à un retour en temps réel de l'impact de ses actions.

Il existe plusieurs types d'IHM qui peuvent être distingués selon le contenu de l'information véhiculée et le dispositif d'affichage et de contrôle. Elles doivent être adaptées à l'usage qu'en font les utilisateurs. On considérera différents types d'IHM : traditionnelles, tangibles, multimodales, centralisées ou distribuées, mobiles, semi-mobiles ou statiques.

Enfin, les facteurs déterminants pour la mise en œuvre des services peuvent être exprimés en termes de qualité du service (telle que discutée dans la partie « modèles et contrôle, dimensionnement, extensibilité, convergence et standards de Qualité de service » QoS) ainsi qu'en relation à l'existence du « substrat d'intermédiation » pour la conception de services appropriés.

ANNEXE 1 : SCENARIOS INDUSTRIELS

Scenario smart Building – Schneider contribution

LES RENDEZ-VOUS
CARNOT 2010
Lyon - 5 et 6 mai 2010



Inter Carnot Objet Communicant

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

5 Mai 2010

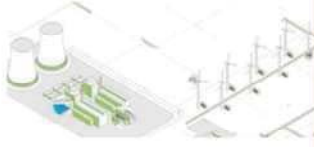
LES RENDEZ-VOUS
CARNOT 2010
Lyon - 5 et 6 mai 2010

Unique positioning



Global specialist in Energy Management

Energy production & transmission



Making energy:

- Safe
- Reliable
- Efficient
- Productive
- Green

Covering
72%
World Energy
consumption

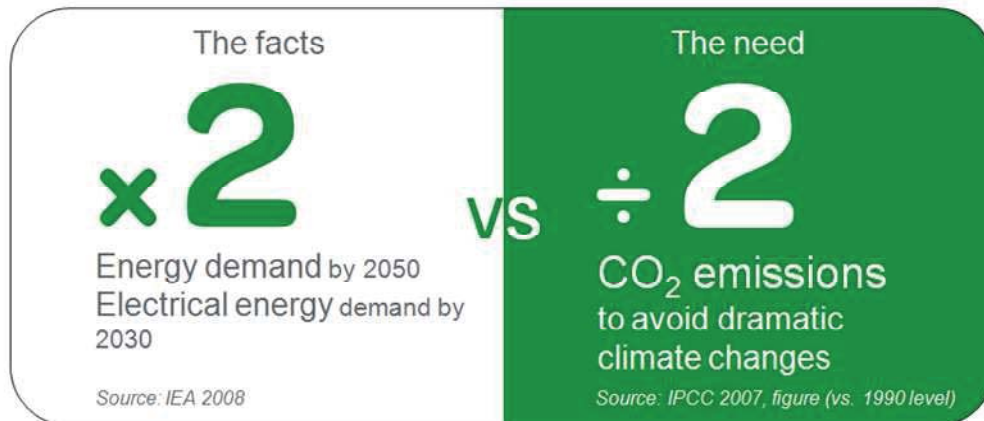
up to
30%
energy saving



Energy usage



The energy dilemma is here to stay



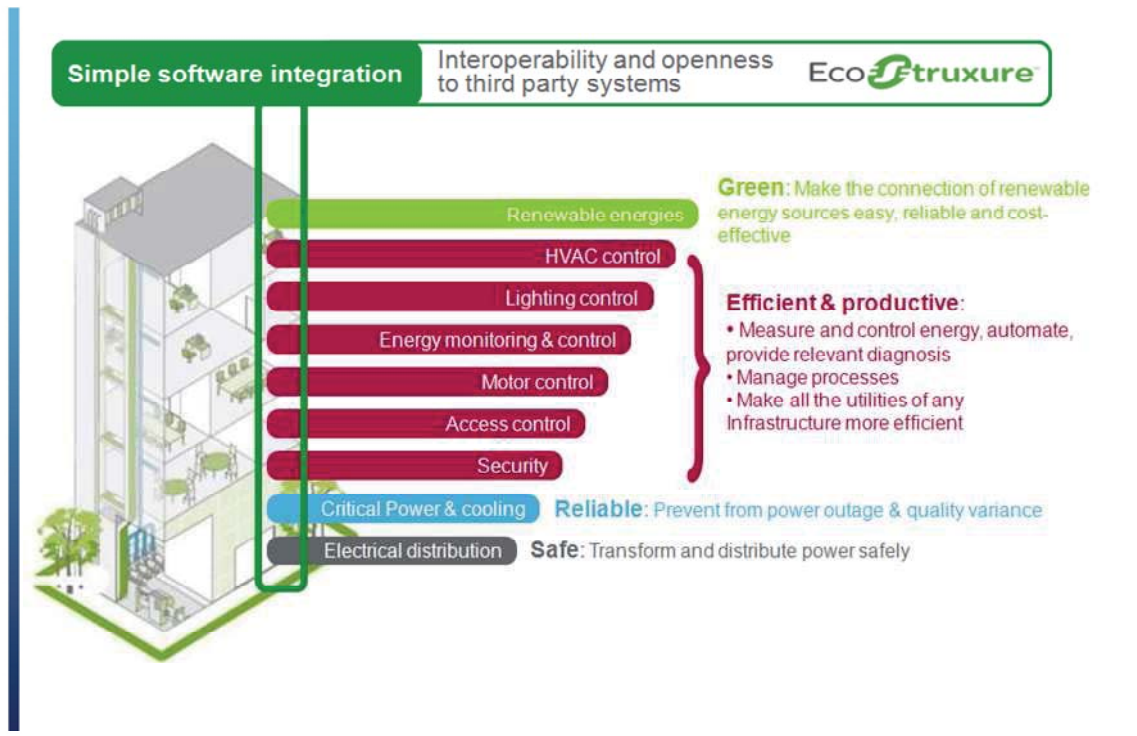
Energy management is the key
to address the dilemma



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





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)

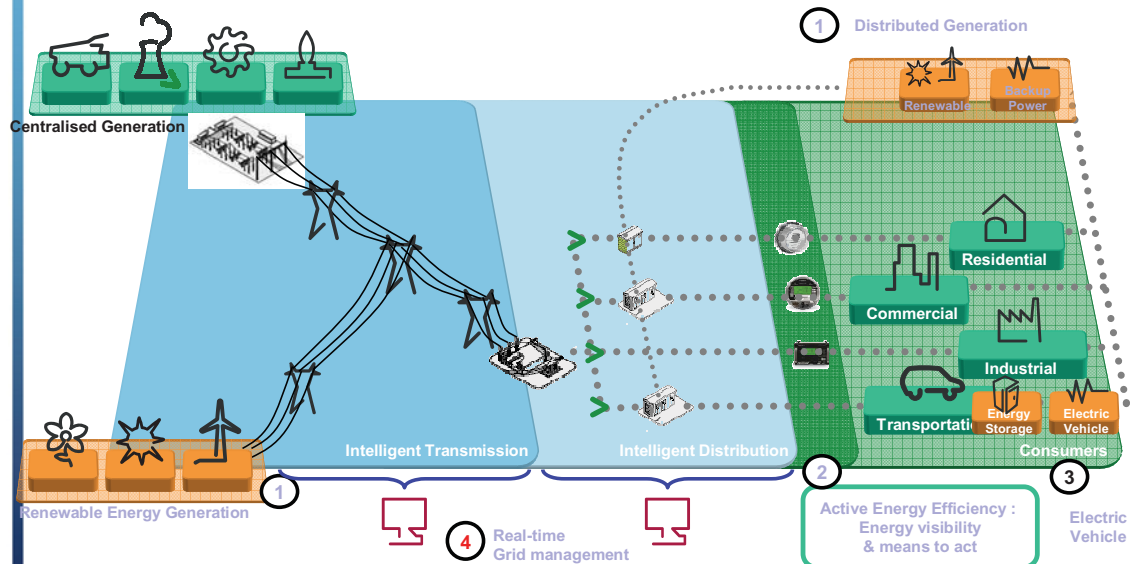
■ Main Characteristics of the Autonomous Wireless Multisensors



- **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



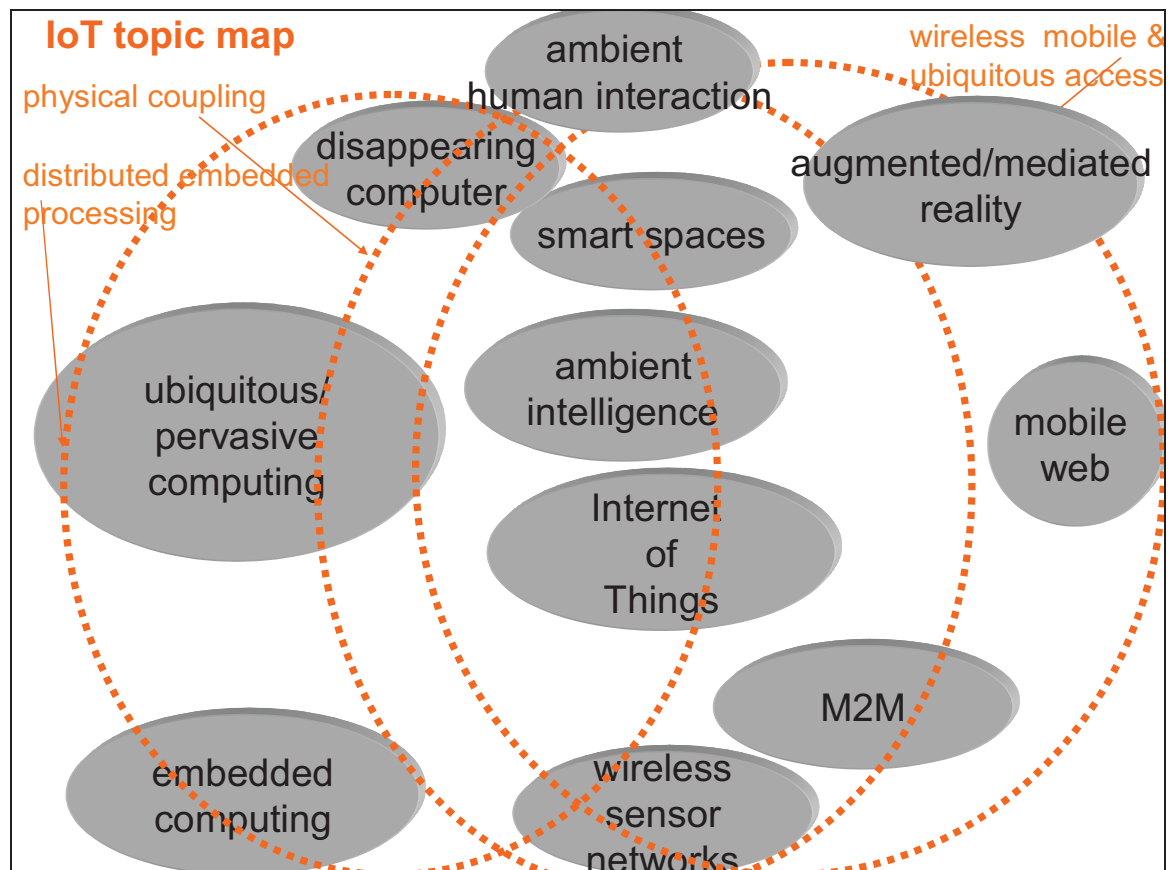
Make the most of
your energy™

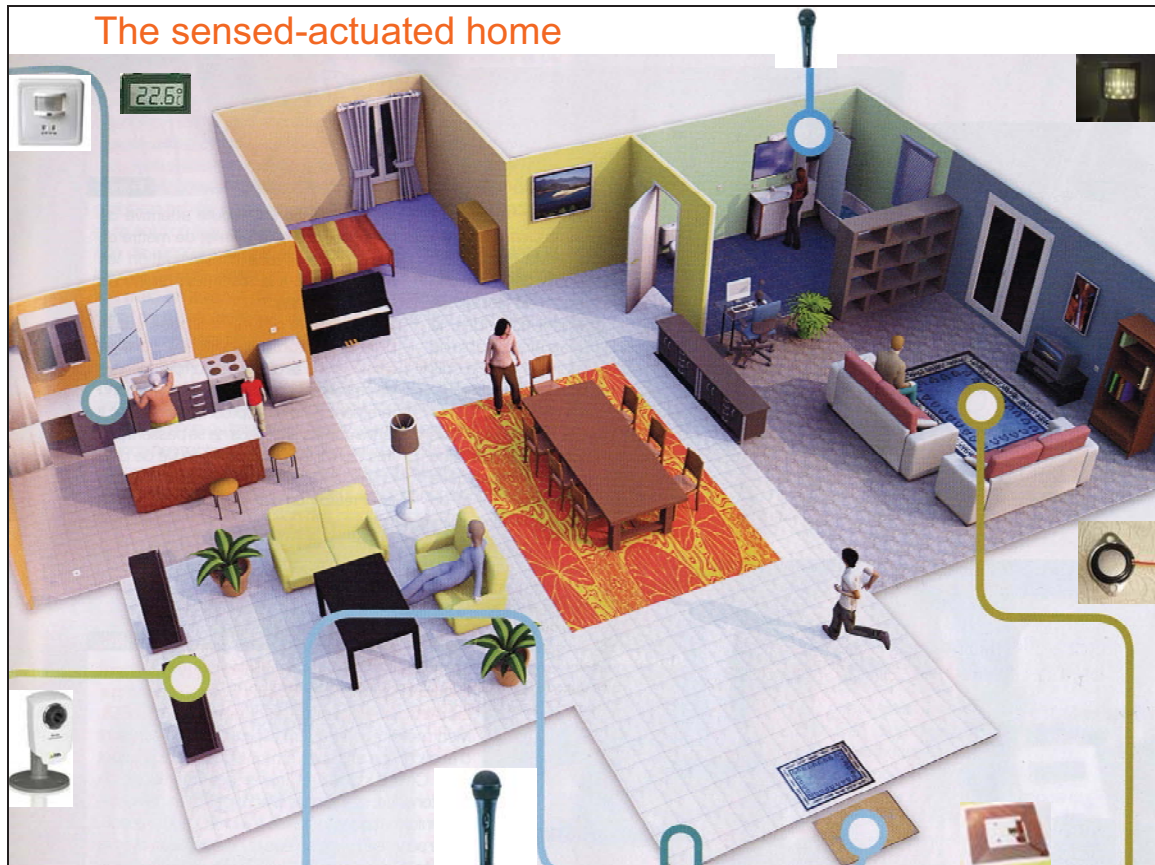


M2M & Internet of Things, from smart spaces to smart cities

*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

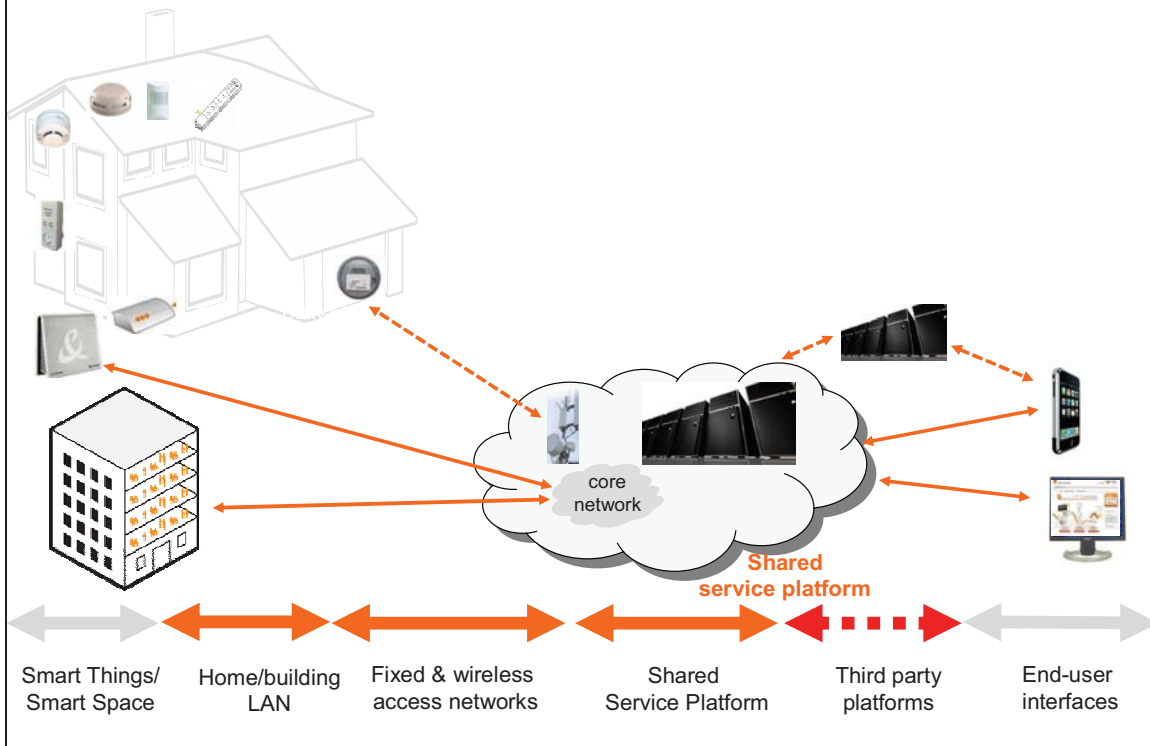




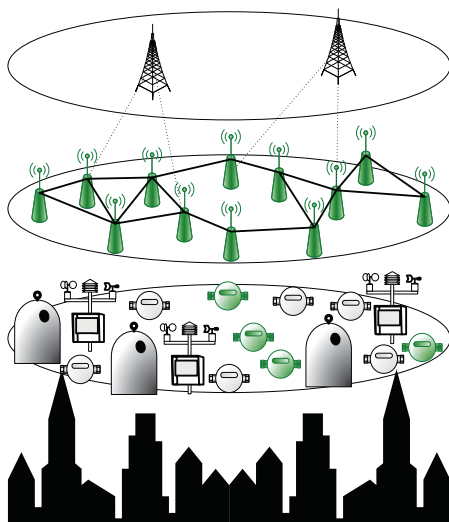
Common IoT/smart space services for the sensed-actuated home

- 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



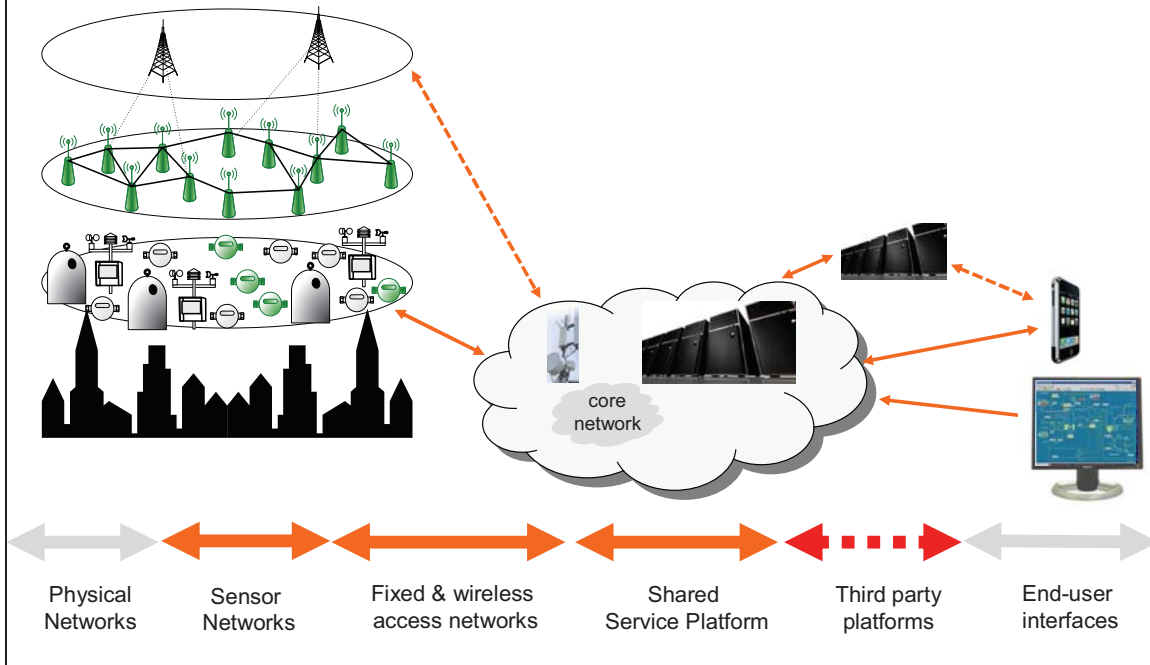
Physical networks

- 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 –

LES RENDEZ-VOUS
CARNOT 2010
Lyon - 5 et 6 mai 2010

Alcatel-Lucent 

Communicating objects and mobile services

From Internet of things to web of objects

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

LES RENDEZ-VOUS
CARNOT 2010
Lyon - 5 et 6 mai 2010

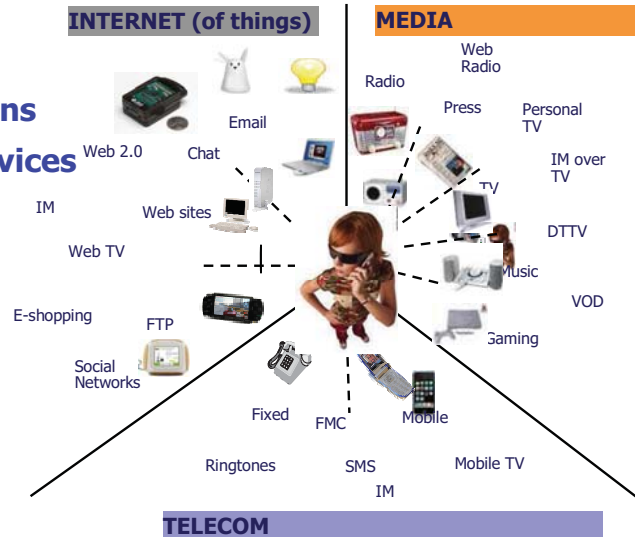
Communicating objects and mobile services
Societal demand

Alcatel-Lucent

The word cloud features the following terms and phrases:

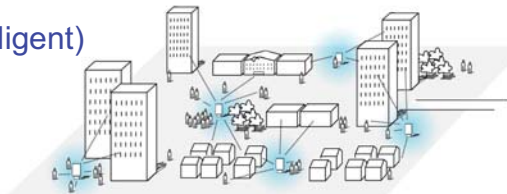
- transport
- multimodal
- sanitaire
- sécurité
- tracking
- techno
- NFC
- paiement
- service
- Trust: Reliability, privacy, traceability?
- geolocalisation
- partage
- services
- risque
- secteur
- ville
- mobile
- logistique
- données
- environnement
- interface
- tourisme
- robotique
- santé
- surveillance
- web/smartphone
- commerce
- augmentée
- culture
- boisson
- conteneurs
- géolocalisation
- mobiles
- machine-objets
- homme
- logiciel
- machine
- robots-objets
- distribu
- dédiée
- assistance
- authentification
- alimentaire
- Asset
- billetique
- cartouches
- capteurs
- architecture
- industrielle
- identification
- distance
- domicile
- developpement
- IdO
- logiciel
- machine
- robotique
- surveillance
- web/smartphone

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

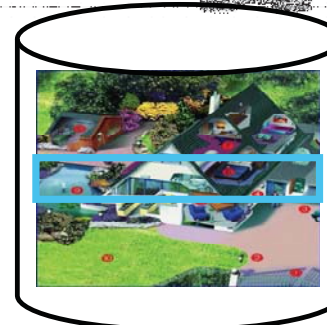
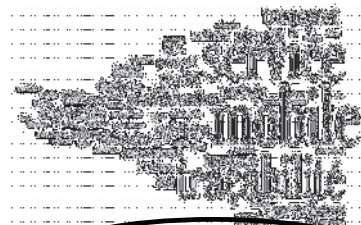
- Leveraging data and services brought by the objects
- « Mash up » with communication and web services



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.

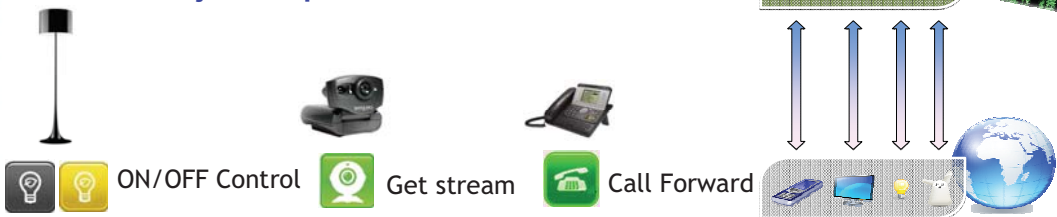


Time to free (web) services from the browser as we know it - and free Internet of Thing applications from their current silos !

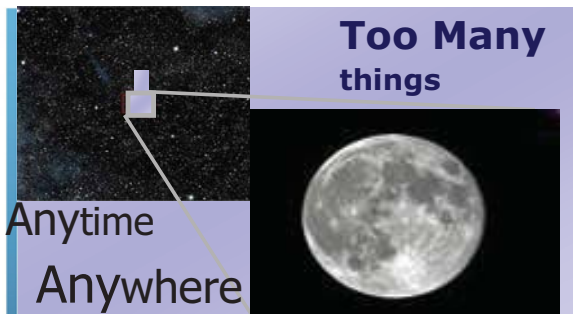
Invent new applications leveraging real-world object exposed using web technologies (smart environments)

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

**Service representation of the Real world
objects exposed on the Web**



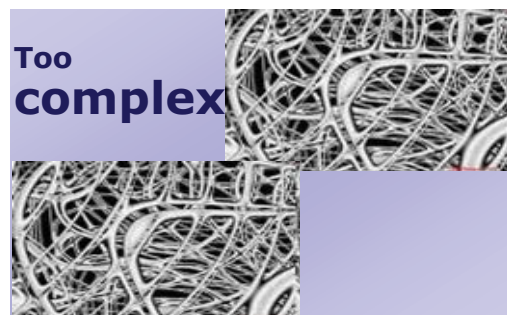
Intermediation: Interoperability, composition, end-to-end trust management



**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 (galleys, 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 : CLASSIFICATION DES COMPETENCES

Instituts Carnot											
Challenges	CEA LETI	CEA LIST	LAAS	LSI	STAR	Télécom et Société Numérique	ESTIA	FEMTO-ST	IEMN	MIB	UTT
Design and Integration of Objects											
Massive Secure and flexible Networking of Objects											
Service Management											

Informations données par chaque laboratoire

ANNEXE 3 : CONTRIBUTEURS ET POINTS DE CONTACT

ESTIA	Renaud BRIAND Guillaume TERRASSON	(point de contact)
FEMTO-ST	Gregory HAYE	(point de contact)
IEMN	Charles ANSSENS Stéphane BEAUSSART Alexandre BOE François Xavier COUDOUX Patrick KENNIS Christophe LETHIEN Christophe LOYEZ Paul Alain ROLLAND Nathalie ROLLAND	(point de contact)
Institut Carnot CEA 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	(point de contact)
Institut Carnot CEA LIST	Jean-Noel PATILLON Karine GOSSE Christophe JANNETEAU	(point de contact)
Institut Carnot LAAS	Marise BAFLEUR Michel DIAZ Jean-Marie DILHAC Daniela DRAGOMIRESCU Marc-Olivier KILLIJIAN	(point de contact)
Institut Carnot LSI	Jean CAELEN Alain KIBANGOU Salvador MIR	(point de contact)
Institut Carnot STAR	Christophe MULLER Philippe PANNIER	(point de contact)
Institut Carnot Télécom et Société Numérique	Hakima CHAOUCHI Serge GOURRIER Daniel KOFMAN Christian PERSON David SADEK Alain SIBILLE Djamal ZEGHLACHE	(point de contact)
MIB	Thierry TARIS Xavier DELORD Christophe MAGRO	(point de contact)
UTT	Dominique GAITI Pascal SALEMBIER	(point de contact)