

L'Internet des objets

Deux technologies clés : les réseaux de communication et les protocoles

Introduction

Le concept d'Internet des objets (IoT) fait florès depuis quelques années. Il ne se passe pas une journée sans qu'un article ou qu'une annonce commerciale ne vienne vanter tout le parti que l'on peut en attendre. L'idée de base est simple : il s'agit d'étendre à des « choses », c'est-à-dire à des entités matérielles ou logicielles, les fonctionnalités offertes par l'Internet dans le domaine de la communication afin de leur permettre d'échanger entre elles ou avec des humains, toutes sortes d'informations ou de données. On en attend des retombées similaires – mais à une échelle beaucoup plus étendue – à celles qu'a apportées l'Internet dans le domaine de l'information et de la communication.



JEAN-PIERRE HAUET
MEMBRE ÉMÉRITE
DE LA SEE.
RÉDACTEUR EN CHEF
DE LA REE

Les domaines d'applications potentielles du concept d'IoT sont très variés. La figure 1 récapitule les principaux secteurs où la notion d'IoT semble aujourd'hui faire sens. Les attentes sont nombreuses et variées : amélioration et diversification des services, nouvelles distractions, surveillance et sécurité, maintenance à distance, contrôle de procédés ou d'infrastructures... Le discours marketing est riche en superlatifs quant aux apports possibles de l'IoT en termes d'efficacité, interopérabilité, extensibilité, fiabilité, sécurité, etc.

Le but des deux articles de ce Gros Plan n'est pas de discuter la validité de ce discours mais de « donner de la chair » au concept en abordant son contenu technique. En fait, l'IoT n'est pas une technologie mais un ensemble de technologies qui, ayant acquis un degré de maturité suffisant, permettent



Figure 1 : Les principaux domaines d'application du concept d'IoT.

ABSTRACT

In this article, we address one of the key factors of the success of the Internet of Things (IoT): the wireless radio communication networks. We first recall the general structure of IoT as a federation of local area networks capable to communicate with the Internet. We propose a classification of these networks into three functional levels:

- *Edge networks that provide communication between the terminal devices and a backbone router or gateway;*
- *Backbone networks which federate local networks;*
- *Backhaul networks that carry the information to the Internet.*

We review the various solutions available today, including new LWPAN networks (Long distance and low power wireless area networks), for generic applications (home automation, smart cities, agriculture, environment...) or for industrial applications which must comply with specific requirements (time criticality, low latency, availability, etc.). Mobility having to meet specific criteria (hand over, reliability...), is not included in this analysis.

We conclude by expressing the hope that the 5G, currently being specified, allows to achieve a synthesis of all these networks which constitute an eco-system often too complex for most potential users.

de construire l'architecture à la fois globale et locale de l'IoT. L'IoT présente des liens étroits avec bon nombre de concepts qui, eux aussi, font appel à ces technologies nouvelles, en mettant plus ou moins l'accent sur certaines d'entre elles : smart grids, cités connectées, voiture autonome ou connectée, wearables, cloud computing, big data, Industrie 4.0...

Pour rationaliser la discussion, on peut considérer l'IoT comme un concept à trois étages (figure 2) :

- en premier lieu des informations sont collectées, véhiculées, échangées et, au moins pour certaines d'entre elles, acheminées vers des serveurs Internet ;
- parvenues à ce niveau, les informations peuvent être triées, stockées et éventuellement traitées sur des plates-formes logicielles et matérielles relevant du cloud computing. Les grands noms de l'informatique proposent aujourd'hui de telles plates-formes telles que Bluemix (IBM), Google Cloud, SAP HANA ou AZURE (Microsoft).
- enfin, les utilisateurs de ces données, dotés de droits d'accès appropriés, peuvent les récupérer et les exploiter, en utilisant, s'il y a lieu, des techniques propres au traitement des données massives (big data).

Dans ce Gros plan, nous ne nous intéressons qu'à la partie « Collecte et échange des informations » c'est-à-dire au premier étage. Le premier chapitre est consacré aux réseaux de communications, donc à la partie basse du système. Le second à paraître dans un prochain numéro de la REE traitera des protocoles, c'est-à-dire des règles qui permettent à deux équipements connectés à un même réseau non seulement de communiquer mais aussi de se comprendre. Il y aurait bien d'autres sujets à approfondir, notamment les questions de cybersécurité, de miniaturisation et d'intégration des composants, d'alimentation en énergie et "d'energy harvesting". Nous renvoyons le lecteur intéressé au Livre blanc de l'IoT qui résultera des travaux 2016/2017 du Cercle des entreprises de la SEE.

Les problèmes de communication pourraient apparaître triviaux tant l'idée a été ancrée dans l'esprit des gens qu'Internet et son protocole IP étaient une sorte d'espéranto qui permet, une fois que l'on est connecté sur le réseau, d'échanger n'importe quelle donnée avec n'importe qui, où que ce soit dans le monde. Le problème est en fait beaucoup plus compliqué.

L'une des raisons en est que l'IoT ne doit pas être pensé comme un réseau unique universel. Il n'y a aucun intérêt à pouvoir accéder directement à n'importe quel capteur ou instrument de mesure dans le monde, parmi des dizaines de milliards qui se connecteront sur l'IoT, pour pouvoir y lire des données qui nous sont complètement étrangères. L'IoT doit en conséquence être vu comme un réseau de réseaux, dont l'Internet est l'épine dorsale. Nous proposons d'en retenir la définition suivante :

« L'IoT est un réseau de réseaux qui permet, grâce à des dispositifs d'identification électronique d'entités physiques ou virtuelles dites « objets connectés » et via des systèmes de communication appropriés, sans fil notamment, de communiquer directement et sans ambiguïté, y compris au travers de l'Internet, avec ces objets connectés et ainsi de pouvoir récupérer, stocker, transférer et traiter sans discontinuité les données s'y rattachant ».

De façon schématique, l'IoT serait ainsi une fédération de réseaux locaux autour de l'Internet telle qu'illustrée par la figure 3.

Mais la figure 3 ne représente qu'un schéma de communication. La question se pose de savoir où sont stockées et traitées les données. Certaines sont traitées au niveau local dans des équipements dits « intelligents », d'autres sont traitées dans le « cloud » et, considérant qu'il n'y a aucune raison à envoyer toutes les données dans le cloud, certaines données peuvent également être stockées et traitées à des niveaux intermédiaires, par exemple au niveau des routeurs de bordure (*edge routers*) de chaque réseau local : c'est ce qu'on appelle le "fog computing".

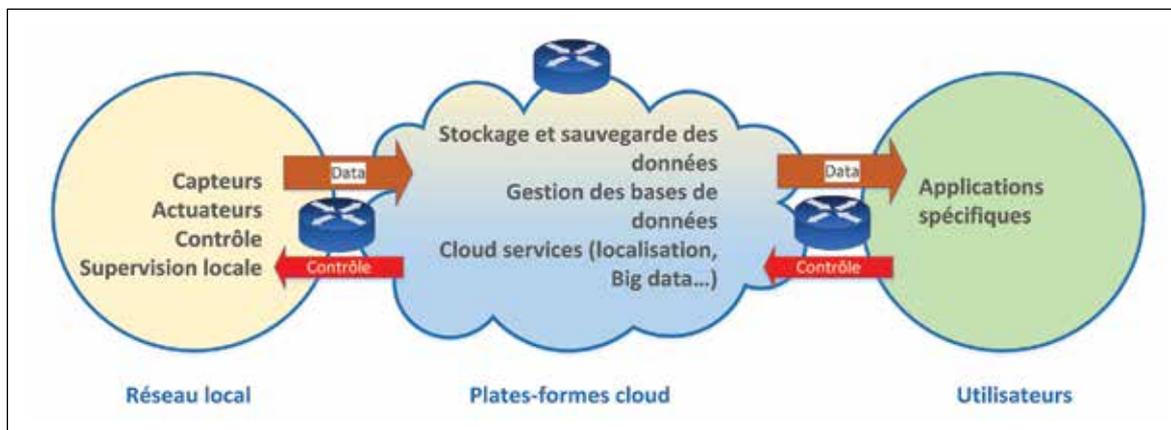


Figure 2 : Architecture générale de l'IoT.

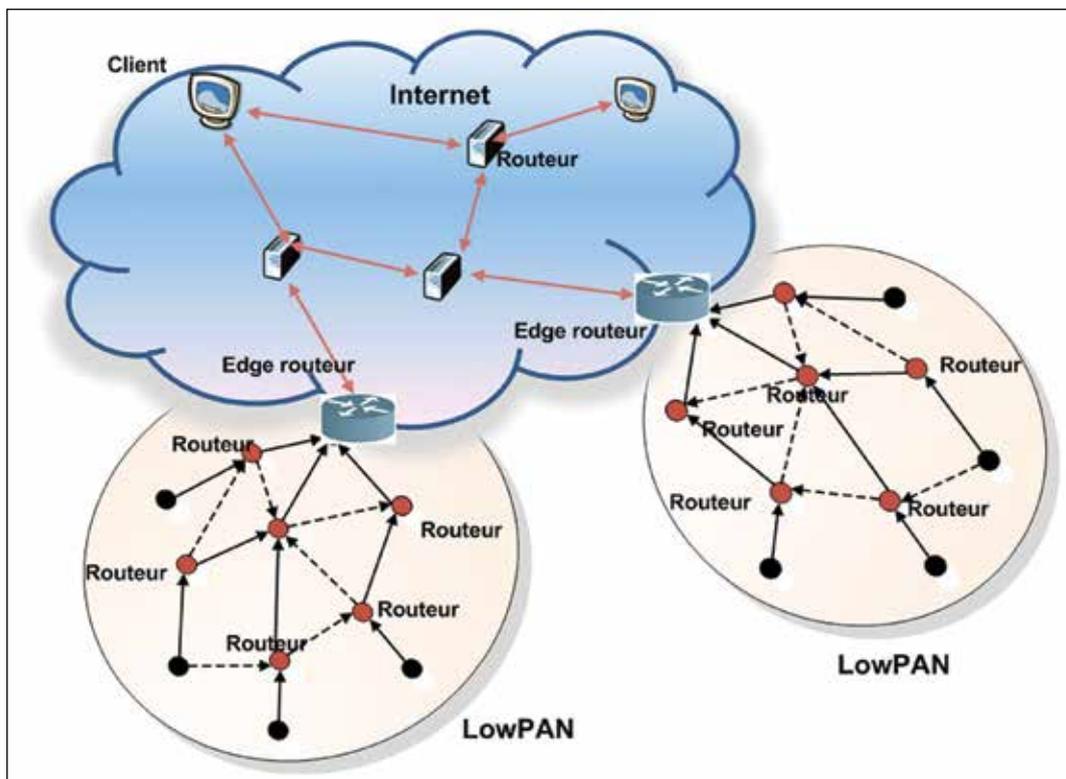


Figure 3 : L'IoT vue comme une fédération de réseaux autour de l'Internet.

Par ailleurs, il faut bien voir que les réseaux locaux apparaissant sur la figure 3 peuvent dans la réalité être de nature très différente selon les domaines applicatifs concernés. Certains sont filaires, d'autres – et c'est de plus en plus le cas – sont des réseaux de radiocommunications. On peut ainsi distinguer, en indiquant W (Wireless) les solutions sans fil, les réseaux :

- PAN et WPAN : Personal Area Networks
- LAN et WLAN : Local Area Networks
- MAN et WMAN : Metropolitan Area networks
- RAN et WRAN : Regional Area Networks
- CAN: Car Area Networks
- BAN : Body Area Networks
- et, plus récemment, LPWAN : Low-Power Wide-Area Network

Ces réseaux n'ont pas les mêmes exigences, en termes de performances (débit, distance, temps de latence), de fiabilité, de disponibilité, de robustesse, etc.

Si l'on considère par exemple les applications industrielles de l'IoT, ce qu'on appelle l'IIoT (Industrial Internet of Things) qui regroupe le secteur de l'industrie proprement dite et celui des infrastructures, on parvient très vite, en partant de la figure 3, à des architectures du type de la figure 4 où des réseaux de différentes natures sont regroupés autour de l'Internet.

On comprend dès lors que, nonobstant l'universalité du protocole IP, une multitude de solutions de réseaux de

communication et de protocoles aient été développées pour tenter de répondre au mieux à des besoins très divers. Il y a là un risque très grand de voir le concept simple d'IoT transformé en tour de Babel par le développement de cette multitude de réseaux hétérogènes incapables d'interopérer entre eux.

Le présent Gros plan vise à donner un panorama didactique de la situation et à dégager les grandes tendances qui se dessinent aujourd'hui. Il se limite à prendre en compte deux grands types d'applications :

- les applications sans contraintes opérationnelles fortes, du type domotique, cités intelligentes, agriculture, environnement, etc. Ces applications correspondent à ce que l'on appelle dans le langage de l'Internet les LLN (Low Power and Lossy Networks) c'est-à-dire les réseaux à faible consommation et avec pertes ;
- les applications industrielles du type IIoT qui peuvent présenter des exigences fortes en matière de temps critique, latence, fiabilité, robustesse, etc. Ces applications relèvent, selon les pays, d'Industrie 4.0 (Allemagne), du plan Industrie du futur (France), de Made in China 2025 ou Japan's Industrial Value initiative.

Nous excluons par conséquent la mobilité (sauf à vitesse réduite) qui pose des problèmes spécifiques de "hand over" et bien entendu des problèmes de fiabilité.

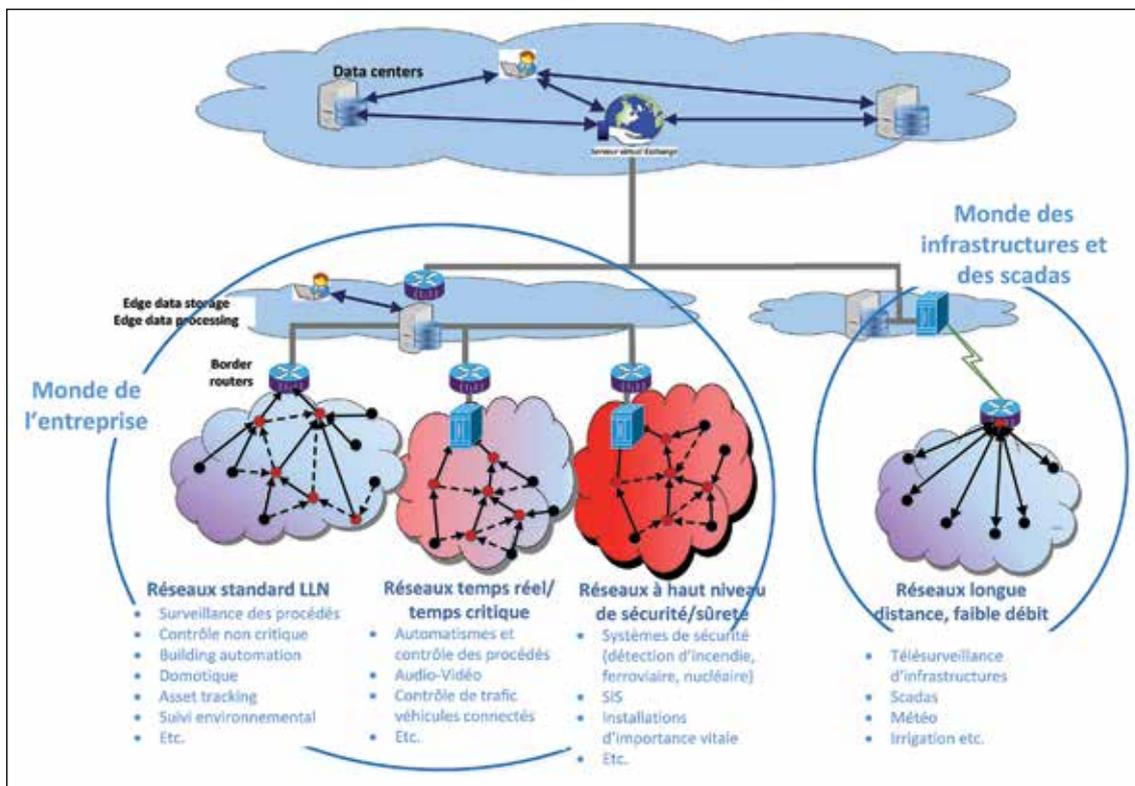


Figure 4 : Schématique des architectures IoT dans l'industrie.

Les réseaux de radiocommunications de l'Internet des objets

Généralités

On comprend de ce qui précède que la question des réseaux de communications soit centrale dans l'Internet des objets. Il existe des dizaines de réseaux, ayant chacun leurs vertus propres. Se pose donc la question de savoir comment sélectionner les principaux d'entre eux et les classer de façon rationnelle.

Le fait de limiter le champ d'étude aux deux domaines précités conduit à écarter des réseaux de communication importants mais dédiés à d'autres fins :

- les CAN (Car Area Networks), indispensables au développement de la voiture autonome et connectée ;
- les BAN (Body Area Network) qui relèvent du domaine de la santé et du bien-être ;
- les solutions essentiellement destinées au multimédia : IEEE 802.11ad ou WiGig, le futur IEEE 802.11ay ; les solutions à très large bande : DS-UWB ou MB-OFDM, ECMA 368 ; le ZigBee RF4CE (pour les télécommandes) ;
- les solutions monodirectionnelles : liaisons infrarouges IrDA (Data et Control) et, à ce stade, le Li-Fi. Toutefois, l'utilisation bidirectionnelle du Li-Fi progresse et son rôle dans l'IoT est à surveiller (au même titre d'ailleurs que dans la voiture connectée) ;

- Les solutions destinées à l'identification et aux transactions à très courtes distances. Ces solutions fonctionnent généralement dans le champ proche : RFID passives, protocoles NFC, RuBee (IEEE 1902.1).

Malgré cette « mise à l'écart », il reste de nombreuses solutions auxquelles il peut être fait appel. La plupart de ces réseaux sont des réseaux sans fil. Si la période 1980-2005 avait été propice au développement des bus de terrain (Profibus, Devicenet, Fieldbus Foundation, WorldFip, etc.), la voie est à présent ouverte aux radiocommunications qui offrent la flexibilité et l'extensibilité indispensables aux réseaux de capteurs. Cela tient à la combinaison de plusieurs facteurs :

- la libération de nouvelles bandes de fréquence :
 - après les bandes 2,4 GHz et 5 GHz, l'Europe s'apprête à ouvrir plus largement la bande libre des 868 MHz, fréquence idéale pour les applications du type IoT¹ ;
 - les regards se portent également vers les très hautes fréquences (de 3,1 à 10,6 GHz) mais aussi vers les ondes millimétriques (au-dessus de 30 GHz) où des ressources importantes de bande passante existent où est définie à présent et à peu près partout dans le monde, une nouvelle bande libre de 57 à 64 ou 66 GHz² ;

¹ Voir la rubrique Actualités dans la REE 2016-3

² Voir la rubrique Actualités dans le présent numéro.

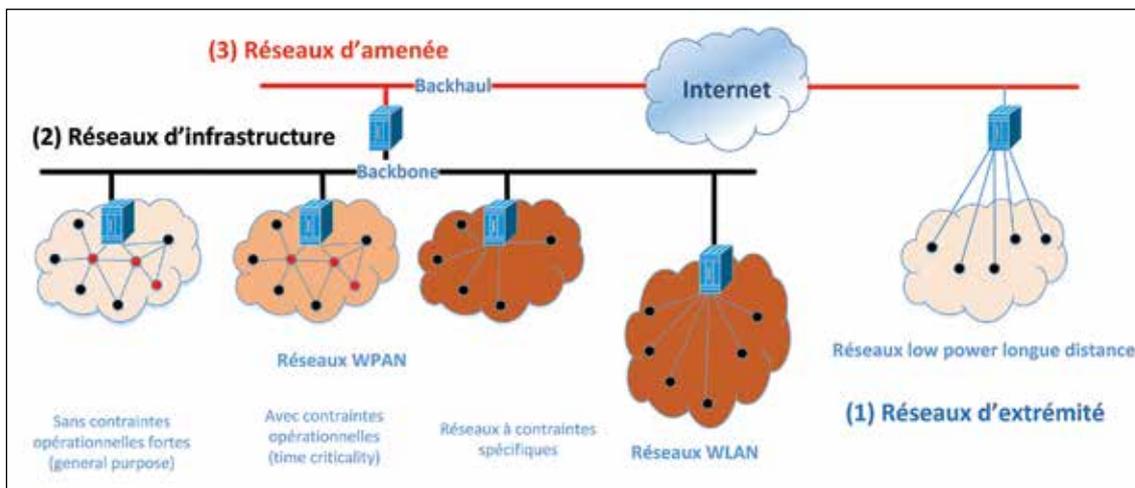


Figure 5 : Typologie des réseaux de l'IoT.

- les progrès de l'électronique qui permettent d'implémenter de façon compétitive, dans de très petits modules, des algorithmes anciens restés pendant des années l'apanage des systèmes professionnels (DSSS, FHSS, OFDM), modules qui atteignent aujourd'hui des limites impressionnantes de sensibilité (-148 dBm ce qui offre des budgets de liaison allant jusqu'à 168 dBm)
- l'émergence de nouvelles technologies : la plus impressionnante est celle du MI-MO (multi-antennes), couramment utilisé dans le Wi-Fi depuis l'IEEE 802.11n, mais sans oublier pour l'avenir, les techniques à ultra-large bande et la radio cognitive (IEEE 802.11af).

Comment classer tous les réseaux auxquels il peut être fait appel ? Une possibilité serait de les classer selon les technologies de base utilisées, c'est-à-dire en fonction de leur couche physique (bandes de fréquences, techniques d'étalement de spectre, schémas de modulation, utilisation de la diversité...) en distinguant le cas échéant les solutions normalisées (ou partiellement normalisées) des solutions propriétaires. Mais cette approche n'est pas parlante du point de vue applicatif et ne motive que les spécialistes.

Nous proposons une typologie des réseaux de l'IoT généralisant la représentation esquissée dans le cas de l'industrie par la figure 4 et introduisant trois niveaux fonctionnels (figure 5).

Les réseaux d'extrémité

Les réseaux de niveau inférieur, desservant directement les objets connectés, pourraient être qualifiés de « réseaux locaux ». Toutefois, ce terme n'est plus réellement adapté du fait de l'émergence des réseaux longues distances du type LoRA et SIGFOX. Nous préférons l'appellation « réseaux d'extrémité » montrant par là qu'ils assurent la desserte d'équipements situés au niveau le plus bas de l'architecture. Ces

réseaux peuvent être filaires (sur CPL par exemple) mais ils sont de plus en plus sans fil.

Dans chaque grappe, ces réseaux amènent l'information vers des concentrateurs de bordure qui peuvent être des routeurs ou des passerelles (gateways) communiquant directement avec l'Internet. Mais ces concentrateurs peuvent également être regroupés sur des réseaux intermédiaires.

Les réseaux d'infrastructure

Les réseaux d'infrastructure sont précisément des réseaux intermédiaires qui permettent de regrouper des grappes d'objets connectés. Ces réseaux sont très souvent filaires mais la technologie permet d'envisager des solutions sans fil.

Les réseaux d'amenée

Les réseaux d'amenée sont les réseaux qui vont permettre de transférer l'information vers l'Internet qui constitue dans l'IoT le cœur de réseau. Ces réseaux d'amenée, ou de « backhaul », peuvent être confondus avec les réseaux d'infrastructure. Ils peuvent également ne pas exister si le routeur de bordure en tête de grappe est en connexion directe avec l'Internet.

Nous détaillons ci-après certaines des spécificités propres à chaque niveau, en mentionnant les réseaux auxquels il peut être fait appel. Il est cependant impossible de donner des détails sur chaque solution et le lecteur devra se reporter à la littérature spécialisée.

Les réseaux d'extrémité

Ces réseaux d'extrémité ont des couvertures géographiques diverses : on trouve dans l'industrie des petits réseaux (du type des *piconets* de Bluetooth par exemple) rassemblant quelques capteurs/actuateurs d'une même

machine, mais on trouve également des réseaux d'atelier voire des réseaux d'usine sur des distances de plusieurs kilomètres. Dans le domaine du building automation, la couverture géographique peut être celle d'une maison. Elle sera plus importante s'il s'agit d'un centre commercial ou d'un quartier. Enfin, l'émergence des réseaux basse consommation à longues distances permet de collecter des données provenant de capteurs localisés à 10 km ou plus, pour les besoins de l'agriculture, de la météo ou de la télésurveillance d'infrastructures distantes.

Nous proposons d'adopter pour ces réseaux une classification dérivée de celle de l'IEEE en distinguant les WPAN (Wireless Personal Area Networks), les WLAN (Wireless Local Area Networks) et les LPWAN (Low Power Wide Area Network).

Les WPAN

L'écosystème des WPAN est très riche. Pour rester simple, nous proposons de distinguer trois catégories : les "General Purpose WPAN" à spectre applicatif large, les "Time Critical WPAN" appelés à répondre à des usages particuliers du monde industriel, les réseaux spécifiques répondant à des exigences spécifiques, par exemple en matière d'extrêmement basse consommation d'énergie.

Les "General Purpose" WPAN

Nous faisons rentrer dans cette catégorie toutes les solutions répondant à des besoins ne soulevant pas d'exigences particulières, par exemple ceux de la domotique et de l'industrie pour des applications non temps critique, dans des périmètres de l'ordre d'une centaine de mètres. Parmi ces applications, on peut citer :

- la surveillance des procédés
- la maintenance préventive
- le contrôle non critique
- la surveillance et la gestion des bâtiments
- la logistique et la localisation
- le suivi environnemental

Parmi les solutions, nous trouvons :

- **Le standard IEEE 802.15.1**, c'est-à-dire, dans la pratique, **Bluetooth**, qui est un standard de communication né dans les années 1990, fonctionnant dans la bande libre des 2,4 GHz et fondée sur l'étalement de spectre par saut de fréquence (FHSS – Frequency Hopping Spread Spectrum). C'est une solution robuste qui permet de réaliser des picoréseaux synchrones constitués d'un maître et de sept esclaves, sur une portée typiquement de 10 m, avec un débit maximum de 2,1 Mbit/s. Cette solution est adaptée à la communication M2M sur courtes distances, elle permet de supporter des

trames IP mais n'a cependant pas été développée pour l'IoT car elle entraîne des consommations d'énergie élevées.

Pour ne pas perdre pied dans ce domaine, les promoteurs de Bluetooth ont développé la version V4, dite Bluetooth Low Energy (BLE ou Bluetooth Smart), issue du projet Wibree initialement promu par Nokia, qui, moyennant certains aménagements techniques (réduction du nombre de sauts de fréquence, limitation de la taille des trames), réduit fortement la consommation d'énergie. Le Bluetooth Smart ne supporte pas à l'état natif les trames IP mais des équipements bimodes (dits Bluetooth Smart Ready) supportent à la fois le Bluetooth Classic et le Bluetooth Smart et peuvent servir de relais avec l'Internet. Les portées sont de l'ordre de la centaine de mètres pour des débits de 270 kbit/s.

La solution BLE est bien adaptée au domaine des "wearables" (lunettes, montres, équipements de sport) mais trouve aussi son application dans la domotique.

- A la différence de l'IEEE 802.5.1, **le standard IEEE 802.15.4** a été d'emblée développé en prenant en compte le souci de limitation des consommations d'énergie. Il est destiné aux équipements qui n'ont d'informations à transmettre qu'épisodiquement ou selon une périodicité lâche et qui peuvent en conséquence rester en sommeil pendant la grande majorité du temps, typiquement 97 %. Le standard IEEE 802.15.4 est une reconnaissance, au niveau des couches basses, de la solution développée par le consortium **ZigBee** pour offrir des communications à faible consommation, avec des débits limités (typiquement 250 kbit/s) sur quelques dizaines de mètres.

Comme le 802.15.1, le 802.15.4 opère essentiellement dans la bande libre des 2,4 GHz mais peut également être installé en Europe dans la petite bande des 868 MHz, pour le comptage notamment. L'étalement de spectre se fait en DSSS (Direct Sequence Spread Spectrum) avec un vecteur d'étalement de 32 chips. Depuis les premières publications, le standard 802.15.4 a beaucoup évolué. Aujourd'hui, la version 2006 constitue la référence de base au-dessus de laquelle ZigBee a bâti divers profils pour répondre aux besoins du comptage de l'énergie, de la santé, de la domotique, des services télécom, etc.

Plus récemment le consortium **Thread** a entrepris la mise au point d'un protocole 802.15.4 destiné à la domotique et intégrant les standards les plus récents du domaine de l'Internet. Il faut souligner que dans la version de base du 802.15.4, les réseaux de communication fonctionnent en "best effort" sur le mode de l'évitement de collisions (CSMA-CA) sans garantie de performances par conséquent.

Par ailleurs, pour différentes raisons, et notamment la longueur limitée des trames, les réseaux 802.15.4 ne peuvent

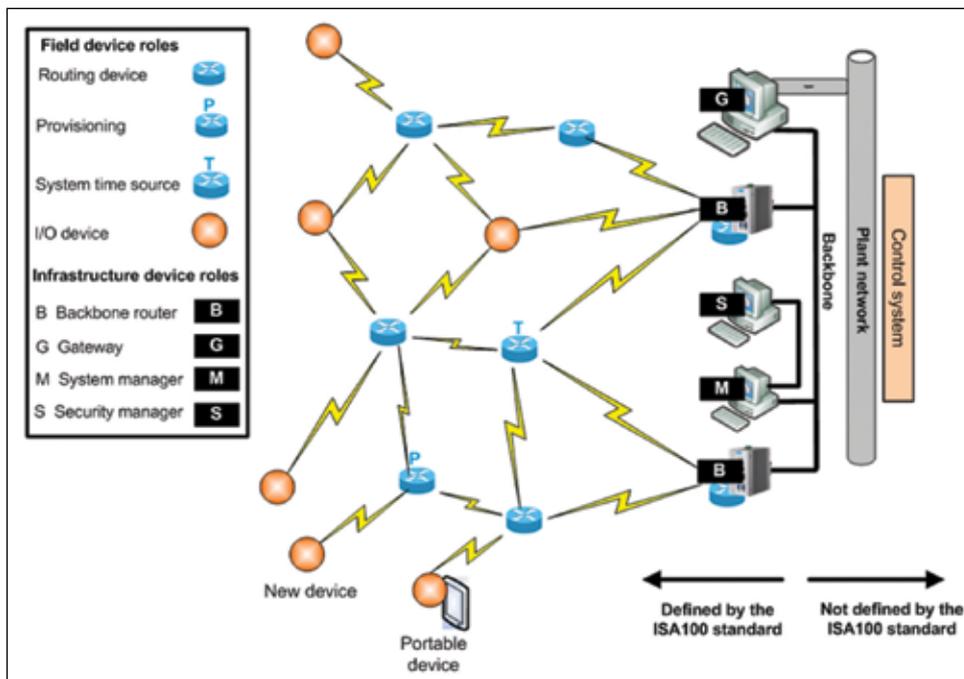


Figure 6 : Architecture générale ISA 100.11a – Source : ISA.

pas accepter directement les trames Internet et une couche d'adaptation 6LowPAN, qui sera décrite dans le chapitre consacré aux protocoles, a été développée par l'IETF (Internet Engineering Task Force) pour interfacier ces réseaux avec l'Internet IPv6.

- Enfin, il faut évoquer, dans cet inventaire rapide, différentes solutions, plus ou moins propriétaires, nées avant que l'IoT n'acquière sa notoriété et qui sont amenées à s'y adapter. Tel est en particulier le cas du standard de fait **KNX** qui présente l'avantage de pouvoir être supporté par une paire torsadée, par CPL ou par liaison radio 868 MHz.

On peut également citer **ANT** et **ANT+** qui sont des réseaux propriétaires, fonctionnant dans la bande des 2,4 GHz et offrant des fonctionnalités proches à la fois de Bluetooth et de ZigBee. C'est une solution reconnue dans le monde des "wearables" mais aussi dans celui de la domotique.

Les WPAN temps critique

Les réseaux 802.15.4 dans leur version de base n'offrent pas des performances suffisantes pour répondre aux exigences de beaucoup de procédés industriels. Ces exigences sont nombreuses et appellent des compromis. On peut les regrouper en 12 critères essentiels listés dans le tableau 1.

A partir de 2005, dans le cadre notamment de l'ISA (International Society of Automation) ont été développés des réseaux maillés, s'appuyant sur le 802.15.4 mais sur lequel a été greffée une organisation déterministe du trafic par un multiplexage temporel (TDMA), accompagné d'un saut de fréquence entre chaque slot de communication afin de renforcer la robustesse du réseau face aux interférences. Ainsi sont nés successivement les standards IEC 62591 (WirelessHART), IEC 62601 (WIA-PA) et IEC 62734 (ISA100.11a). Ce dernier réseau (figure 6) supporte la couche d'adapta-

Critères de sélection d'un réseau industriel	
Disponibilité, fiabilité	Connectivité avec un "backbone"
Coexistence avec d'autres réseaux	Extensibilité (scalability)
Faible temps de latence et déterminisme	Ouverture et interopérabilité
Sécurité (intégrité, authentification, confidentialité)	Débit-distance
Consommation d'énergie – Durée de vie des batteries	Compétitivité
Paramétrage de la qualité de service	Standardisation

Tableau 1 : Douze critères pour évaluer une solution de radiocommunication dans l'industrie.

tion 6LowPAN et constitue un réseau local répondant aux exigences de l'IOT et pouvant s'interfacer directement avec l'Internet IPv6 dont nous parlerons au chapitre 2.

Les principes de l'ISA 100 sont aujourd'hui repris dans un amendement particulier du 820.15.4, le 802.15.4e, qui introduit le déterminisme et le saut de fréquence dans la gestion du réseau local.

Nota 1 : On notera que l'on écarte à ce stade l'utilisation des réseaux sans fil pour les applications à des fonctions sécuritaires. Cependant la question est à l'étude, dans le cadre du groupe de travail ISA-84 notamment.

Les WPAN à extrêmement basse consommation

Dans le domaine industriel, mais aussi dans celui de la domotique, on trouve également des solutions répondant à des besoins très particuliers, notamment l'extrêmement basse consommation d'énergie, à des niveaux compatibles avec "l'energy harvesting" permettant donc de se dispenser des alimentations par batteries (Cf. REE 2015-1 p.127). Mentionnons parmi ces solutions **EnOcean** (ISO/IEC14543-3-1), **Wavenis**, **SARAH** (Arveni) et **DASH7**. L'exigence "d'ultra low power" conduit à des protocoles relativement frugaux, avec des trames courtes, fonctionnant généralement par impulsions. Ces solutions répondent à des besoins typiques de l'IoT (très faible consommation et très bas coût) mais leur intégration dans une architecture Internet va difficilement au-delà de la connexion au travers d'un gateway collectant les informations en provenance des capteurs. A noter que la solution DASH, si elle est utilisée à 250 kbit/s, ne permet une portée que de quelques dizaines de mètres. Par contre, utilisée à très faible débit (9,6 kbit/s), elle autorise des communications allant jusqu'à plusieurs kilomètres. Elle constitue un trait d'union avec les LWPAN dont nous parlons en section 3.

Les WLAN

La deuxième grande catégorie de réseaux d'extrémité que nous retenons est celle des WLAN, les Wireless Local Area Network c'est-à-dire essentiellement le domaine des **Wi-Fi** (IEEE 802.11) qui opèrent dans des plages de portée allant de quelques mètres au kilomètre³.

Les WLAN sont nés avec les premiers Wi-Fi dans les années 1997-2000. A cette époque, on parlait encore peu d'Internet des objets et le Wi-Fi n'a pas été créé dans cette

³ Nous excluons par conséquent de cette catégorie les Wi-Fi à très haut débit mais à faible portée : le 802.11ad (ou WiGig), le 802.11y opérant aux Etats-Unis dans la bande 3 650-3 700 GHz avec une puissance de 20 W et le 802.11af (ou White-Fi) opérant en radio cognitive dans les interstices des bandes TV.

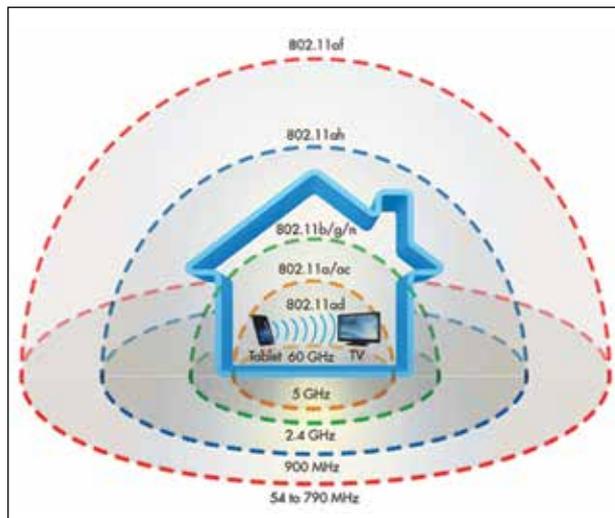


Figure 7 : Positionnement en portée des principales solutions Wi-Fi.

perspective. Cependant, cette technologie possède de précieux avantages dans la mesure où sa structure de trame, différenciée selon les détails de la couche radio, est similaire à celle de l'Ethernet et se prête donc très bien à l'encapsulation de trames IP. Les relais Wi-Fi permettent de créer très simplement des points d'accès au réseau Internet, soit sur support cellulaire, soit par le canal d'un réseau cellulaire 3G ou 4G. Le Wi-Fi peut donc constituer un réseau d'extrémité très simple de mise en œuvre et très performant à la condition que les équipements disposent d'une alimentation en énergie à partir du réseau. En effet, toutes les solutions Wi-Fi développées depuis 1997 : 802.11, 802.11b, 802.11 a et g, 802.11n et plus récemment 802.11ac sont dispendieuses en énergie car les équipements ne sont pas programmés pour être mis en sommeil lorsqu'ils pourraient l'être.

Pour l'IoT, une attention particulière doit être portée au Wi-Fi 802.11ah (labellisé comme "**Wi-Fi Halow**" par la Wi-Fi Alliance), dont la spécification a été publiée au début de l'année 2016 et dont le champ d'application visé est celui des réseaux de capteurs et plus généralement celui de l'Internet des objets. Son ambition est de concurrencer le Bluetooth LE en offrant une meilleure couverture (jusqu'à 1 km) et une connectivité directe avec le monde de l'Internet. Le 802.11ah est destiné à fonctionner dans les bandes sub-GHz (donc à 868 MHz en Europe) en offrant ainsi de meilleures conditions de propagation que les autres Wi-Fi. Les techniques de modulation et de multiplexage sont directement dérivées de celles des 802.11n et ac mais avec une fréquence d'horloge ralentie 10 fois. Le protocole prévoit que les stations regroupées autour de relais (Relay Access Points) pourront être mises en sommeil selon un rythme convenu avec un réveil prédéfini (Target Wake Time). Cependant, ce qui est un point fort peut devenir un point faible car cela implique, pour assurer l'interopérabilité, que tous les

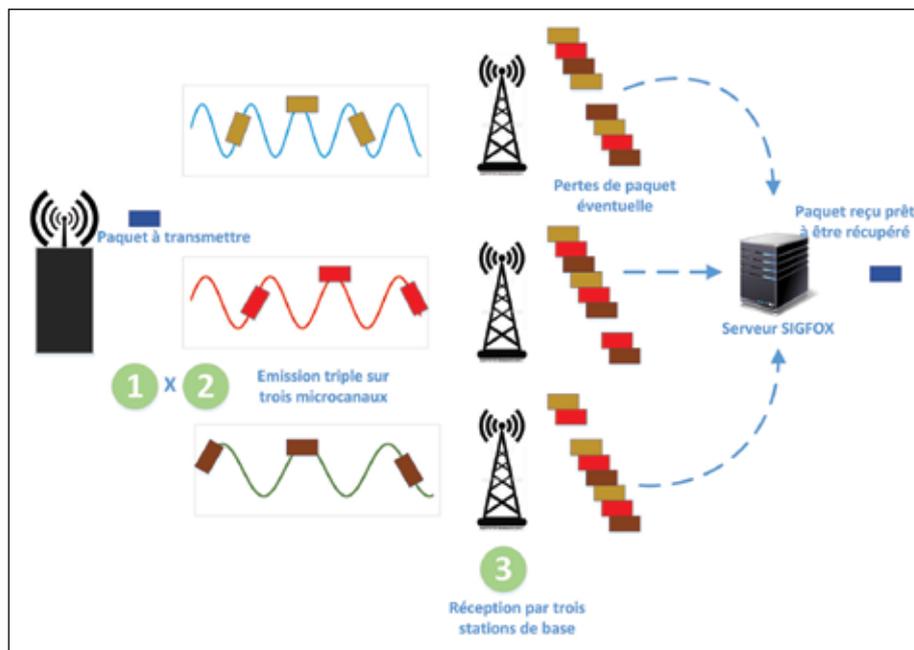


Figure 8 : Architecture du système SIGFOX.

équipements d'un même type (par exemple l'éclairage en domotique) adoptent le même profil, alors que la Wi-Fi Alliance, à la différence de Bluetooth et ZigBee, n'a jamais publié de profils particuliers au-dessus des couches basses du 802.11. Néanmoins, la Wi-Fi Alliance prévoit un développement très large du Wi-Fi Halow dans les secteurs de la domotique, de la santé, de l'agriculture et même de l'industrie.

La figure 7 illustre, en termes de portée, le positionnement sommaire des solutions Wi-Fi évoquées ci-dessus.

Les LWPAN

Le Wi-Fi Halow constitue une transition vers les réseaux LPWAN (Low Power Wide Area Network) apparus à partir de l'année 2015 afin de réaliser à faible coût, sur de grandes distances, des réseaux de capteurs alimentés par batterie. Ce sont donc des réseaux à faible débit tirant parti des développements les plus récents en matière d'électronique afin de permettre de gérer avec une qualité de service acceptable des budgets de liaisons allant jusqu'à -160 dBm. Les réseaux longue distance à très basse consommation d'énergie sont apparus récemment ; ils nécessitent des récepteurs très sensibles pouvant détecter un signal émis par une source à relativement faible puissance même si elle est distante de plusieurs kilomètres.

Plusieurs initiatives très intéressantes ont vu le jour. Deux solutions d'origine française retiennent l'attention, d'autant plus qu'elles sont parvenues à se faire reconnaître au niveau mondial, y compris aux Etats-Unis :

- **LoRa**, solution ouverte fondée sur le protocole LoRaWAN promu par la LoRa Alliance. Ce protocole (tel que publié

en juin 2015) peut être mis en œuvre par n'importe quel opérateur, public ou privé. Tel est notamment le cas de Bouygues Télécom qui l'a inséré dans la plate-forme promue par sa filiale Objenious.

LoRa est un réseau « étoile » bas débit, fonctionnant en France dans la bande des 868 MHz, utilisant des composants d'une très grande sensibilité et permettant de mettre en connexion, de façon bidirectionnelle, des capteurs distants de plusieurs kilomètres avec un relais servant de gateway (situé par exemple sur un point haut Bouygues Telecom) qui transfère ensuite les informations, en mode IP, vers l'Internet. LoRa utilise des canaux de 125 kHz en étalement de spectre. Les débits annoncés vont de 300 bit/s à 50 kbit/s (en Europe).

- **SIGFOX** repose sur un modèle différent. SIGFOX est un opérateur qui, directement ou par l'intermédiaire de partenaires, propose un service de connexion IoT dans le monde entier (en 2016, dans 24 pays). La technologie est également différente : le système SIGFOX utilise une transmission à bande très étroite (Ultra Narrow Band) permettant à un capteur d'envoyer des impulsions très courtes (12 octets de charge utile, au maximum 140 fois par jour) sur des micro-canaux dans la bande des 868 MHz. Les trames sont envoyées trois fois, sur trois fréquences, en direction de toutes les stations de base, sachant que, typiquement, trois d'entre elles pourront les capter, avant d'être récupérées par les serveurs SIGFOX (figure 8). En "downlink" la charge utile est limitée à 8 octets, quatre fois par jour.

Compte tenu des débits limités (équivalents à environ 100 bit/s), les applications préférentielles sont celles du

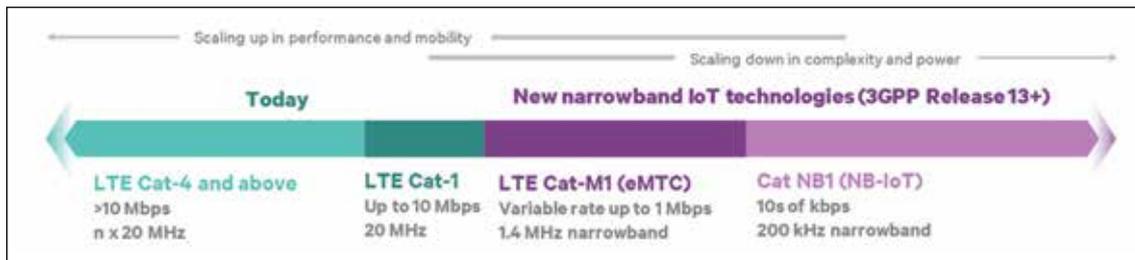


Figure 9 : Positionnement des nouvelles catégories LTE destinées à l'IoT.

comptage, de la maintenance préventive, de l'agriculture, de l'environnement, etc.

D'autres initiatives ont vu le jour, simultanément ou avant LoRa et SIGFOX, avec plus ou moins de succès : **Qovisio** (Opérateur IoT basé à Angers), **Neul**, **Ingenu**, **Weighless N et P**, **nWave**, etc.

Les réseaux cellulaires ne restent pas inactifs. Avec la publication du communiqué 13 du 3GPP (le consortium qui établit et publie les standards de 3^e et 4^e génération), trois solutions fonctionnant dans des fréquences sous licence se trouvent homologuées :

- **EC-GSM-IoT** (EC = Extended Coverage) qui est un complément logiciel du GPRS permettant d'offrir, grâce à la base installée GSM, des services LPWAN dans des fréquences sub-GHz. EC-GSL-IoT utilise des canaux de 200 kHz en half duplex. Le gain de couverture escompté est de 20 dBm pour un débit de 10 kbit/s. Le lancement commercial est prévu pour 2017.
- **eMTC (ou LTE-M)** qui est une extension logicielle de 4G LTE. eMTC requiert un canal de 1,4 MHz (à l'intérieur d'un canal LTE de 20 MHz) et permet des débits de 1 Mbit/s. C'est une solution adaptée au trafic M2M.
- **NB-IoT** qui est intégrée dans LTE mais utilise une interface radio spécifique. Le profil vient en compétition avec LoRa. Il requiert un canal de 200 kHz et permet des débits de quelques dizaines de kbit/s.

La figure 9 positionne les deux solutions LTE par rapport aux catégories classiques du LTE.

Il est encore trop tôt pour dire quel sera l'impact marketing de ces solutions standardisées 3GPP. Leur intérêt à terme paraît clair : elles permettent de construire des architectures « full IP » sans solution de continuité au niveau d'un gateway et préfigurent l'unification des réseaux que pourrait permettre la 5G (voir en conclusion).

Les réseaux d'infrastructure

Dans une architecture IoT, les réseaux d'infrastructure (ou backbone) ne sont pas une obligation. Un réseau d'extrémité peut parfaitement s'interfacer directement avec l'Internet, via un routeur de bordure ou une passerelle.

Cependant dès que l'on affaire à plusieurs réseaux d'extrémité coexistant sur un même site ou au sein d'une même structure, il est nécessaire de fédérer ces sous-réseaux et d'organiser l'échange d'informations entre eux. On peut citer les exemples d'une raffinerie regroupant plusieurs unités de traitement aussi bien que d'un centre commercial abritant de nombreux commerces.

Les données échangées ou regroupées peuvent être des données d'exploitation ; elles peuvent aussi être des données de configuration permettant de partager des règles de sécurité et de gestion des droits d'accès, des règles d'adressage local, des règles de gestion des fréquences. Dans le domaine des radiocommunications, la question du "Common Network Management" appliqué à plusieurs réseaux d'extrémité est délicate et elle est aujourd'hui mal résolue. Si l'on veut éviter la cacophonie, un Common Network Manager communicant par un Common Shared Network avec les différentes passerelles desservant chacun des réseaux sans fil, est nécessaire. Des travaux sont en cours sur ce thème au sein du groupe ISA-100 WG20.

Les réseaux d'infrastructure peuvent être :

- bien entendu des réseaux filaires, notamment du type Ethernet, éventuellement, pour les applications industrielles, Ethernet industriel (du type IEEE 802 TSN – Time Sensitive network) ;
- des solutions Wi-Fi choisies parmi celles à haut débit et notamment les solutions bi-bandes : IEEE 802.11n, IEEE 802.11ac et son successeur en développement : IEEE 802.11ax ;
- Le WIMAX (IEEE 802.16), utilisé dans certains pays mais qui n'a cependant pratiquement pas démarré en France (ne pouvant notamment pas être opéré en bande libre) ;
- Les réseaux cellulaires 3G, HSPA et surtout 4G qui peuvent être utilisés pour connecter les routeurs de tête de réseaux d'extrémité répartis sur de grandes distances.

Les réseaux d'amenée

Les réseaux d'amenée ou de backhaul permettent de renvoyer sur le cloud les informations que l'on souhaite y envoyer afin qu'elles puissent être récupérées par une plate-forme de gestion des données. En soi, cette fonction de backhaul est

moins celle d'un réseau que celle d'un routeur ou d'une passerelle transférant sur le cloud les données collectées soit au niveau du routeur de tête d'un réseau d'extrémité, soit par un serveur de données installé sur le réseau d'infrastructure. La fonction d'amenée peut aussi se confondre avec celle de fédération de sous-réseaux assurée par le réseau d'infrastructure.

Cependant dans certains cas, la fonction d'amenée sera confiée à un réseau dont ce sera la seule vocation. On retrouvera ici :

- les réseaux filaires d'entreprises du type Ethernet ;
- les réseaux cellulaires 3G, HSPA et 3G ;
- les liaisons satellitaires.

Conclusion : La 5G et l'IoT

L'écosystème des réseaux de communication censés répondre à la problématique de l'IoT est complexe. Les solutions se sont empilées de façon hétérogène au fil des années avec pour chacune des avantages et des inconvénients. Dans plusieurs cas, les solutions proposées sont un rafistolage de solutions plus anciennes afin de ne pas perdre pied dans la compétition qui s'amorce autour de l'IoT.

Il serait temps de procéder à une réflexion globale sur l'architecture qu'il faut mettre en place pour permettre à l'IoT de se développer sans que sa mise en œuvre ne devienne un parcours du combattant pour les usagers. Le développement de la 5G, en cours de spécification, est une occasion unique pour réaliser « la grande unification » à laquelle les utilisateurs aspirent.

La 5G ne sera pas seulement un accroissement des débits afin de répondre encore mieux aux besoins du multimédia.

Elle devra être une réponse au problème souvent exaspérant du "deep indoor" qui fait qu'une liaison 4G peut être excellente à l'entrée d'un bâtiment mais s'évanouit lorsqu'on pénètre à l'intérieur. Mais la 5G ne doit pas être que cela : elle doit permettre d'inclure dans le champ de la communication les objets de l'Internet des objets qui, dans le même temps, de par la force du progrès technique, auront acquis des capacités de collecte et de traitement des données très supérieures à ce qu'elles sont aujourd'hui.

Il faut donc que la 5G apporte non seulement des débits très supérieurs à ceux de la 4G mais aussi une couverture plus uniforme des zones desservies, une aptitude à pénétrer à l'intérieur des bâtiments, un temps de latence très court, un service déterministe ou quasi-déterministe, une faible consommation permettant de fonctionner 10 ans sur batteries et bien entendu un coût aussi faible que possible.

Ce sont là des défis considérables et la 5G ne pourra pas répondre d'emblée à tous. De nouvelles technologies, dont la REE se fait régulièrement l'écho, devront être mobilisées : MI-MO massif, ondes millimétriques, picocellules pour la densification, nouvelles formes d'onde pour une meilleure utilisation du spectre... Ceci implique probable-

ment une coopération accrue entre les réseaux cellulaires administrés et les solutions locales, type Wi-Fi, opérant dans des bandes libres qui aujourd'hui leur font concurrence mais qui demain pourront concourir à la réalisation du grand projet de l'Internet des objets. La réelle synergie est là. Il est à parier que dans 30 ans l'exposé qui précède s'apparentera davantage à la visite d'un musée sur la conquête de l'Ouest qu'à un tutoriel sur l'état de l'art de l'époque. ■

Jean-Pierre Hauet est ingénieur au corps des Mines. Il est associé partenaire de KB Intelligence. Au cours de sa carrière, il a dirigé les Laboratoires de Marcoussis du groupe Alcatel-Alsthom, il a dirigé la branche Produits et Techniques de Cegelec et a été Chief Technology Officer du Groupe ALSTOM. Il est membre émérite de la SEE et rédacteur en chef de la REE.