Internet des objets 2018

RAPPORT PRINCIPAL

Préambule

A la fin de l'année 2015, la SEE publiait un Livre blanc sur la cybersécurité des réseaux électriques intelligents (REI), fruit d'un travail collaboratif mené au sein de son Cercle des entreprises. Ce Livre blanc a bénéficié d'une forte audience dans les milieux concernés et les attaques survenues en 2015 et 2016 sur les réseaux électriques de l'Ouest ukrainien ont montré la justesse de ses analyses.

Les REI, ou smart grids, sont une instanciation particulière du concept d'Internet des objets ou IoT (Internet of Things). La SEE a en conséquence décidé d'élargir son champ d'investigation en constituant, toujours dans le cadre du Cercle des entreprises, une task-force dédiée à l'IoT. Ce groupe de travail a procédé à de nombreuses auditions, collecté une importante documentation et recueilli l'avis de divers experts. La présente étude « **IoT 2018** » est le résultat de ces travaux

Son objectif est de faire un tour d'horizon complet de l'IoT, d'en préciser la définition, d'en évaluer les enjeux et de passer en revue les technologies-clés qui sous-tendent son développement. Cette étude n'a pas la prétention d'épuiser le sujet qui est très vaste et très évolutif, mais elle lui consacre l'approfondissement qu'il mérite. Les enjeux de l'IoT sont passés en revue, mais avec circonspection et les prévisions souvent trop optimistes sont discutées. Cependant il ressort clairement que l'IoT est l'une des technologies de base qui permettra, en France comme dans la plupart des pays industrialisés de gagner quelques points de croissance, évalués à horizon 2021/2025 aux environs de 3 à 3,5 % de PIB. Tous les domaines de l'activité économique et de la vie courante sont concernés et l'IoT n'est pas seulement un facteur de productivité et de création de valeur, il remet en cause les modèles d'affaires traditionnels et **ceux qui ne prennent pas à temps le train de l'IoT seront évincés du marché**.

Parmi les techniques qui sous-tendent l'IoT, deux grands domaines se détachent :

- **les communications** afin d'assurer la connectivité, au travers de l'Internet, avec les objets connectés. Depuis une quinzaine d'années, on a vu se développer les réseaux locaux (Bluetooth, ZigBee, Wi-Fi…) qui s'adaptent aujourd'hui à l'IoT en réduisant leur consommation d'énergie. Mais l'événement marquant des deux dernières années est l'émergence rapide des réseaux longues distances et faible consommation d'énergie (les LPWAN) dont deux « têtes de série », LoRaWAN et Sigfox, sont d'origine française. Les réseaux cellulaires arrivent à leur tour sur le marché avec des profils s'appuyant la 4e génération de réseaux mobiles (eMTC et NB-IoT) dans l'attente de la 5G qui pourrait apporter des progrès décisifs.
- **le traitement et le stockage des données**, qui se fait de plus en plus en infonuagique (*cloud computing*) mais doit respecter un principe de subsidiarité. La donnée devient la principale richesse de l'entreprise qui passe ainsi du *Data Management* au *Management by Data*©.

Comme pour les REI, **la cybersécurité** est une préoccupation fondamentale. En 2016, l'attaque a progressé plus vite que la défense et de nouvelles menaces ont vu le jour. L'étude **IoT 2018** analyse les spécificités de l'IoT et propose des voies pour construire une riposte adaptée et permettre de porter une confiance justifiée dans les futurs objets connectés.

Nous pensons que cette étude sera utile aux décideurs pour mieux comprendre l'IoT et aux responsables techniques pour le mettre en œuvre. Pour rendre sa lecture plus aisée, beaucoup de développements techniques ont été renvoyés en annexes. Par ailleurs, la SEE se propose d'approfondir les problèmes liés à la mobilité, qu'il s'agisse de véhicules connectés ou de drones, dans un futur travail qui démarrera à la fin 2017. ■

François Gerin
Président de la SEE

Jean-Pierre Hauet
Rédacteur en chef de la REE

Table des matières

Résumé

L'Internet des objets ou Internet of Things (IoT) correspond à l'extension au domaine des « choses » – c'est-à-dire aux entités matérielles et logicielles, que l'on appelle communément les « objets » – des fonctionnalités offertes par l'Internet et le Web en matière de communication entre personnes. Dans cette approche, l'humain apparaît comme un cas particulier d'objet qui associe des capacités matérielles et logicielles spécifiques. On en vient alors à parler d'Internet of Everything selon la conception introduite par Cisco en 2011.

L'IoT n'est pas un produit, ni un réseau, ni un système : c'est un système de systèmes et, sur le plan des communications, un réseau de réseaux, dans lequel l'Internet va jouer un rôle fédérateur, une sorte de glu qui va permettre à des réseaux de natures très diverses de se concaténer et de constituer un maillage permettant aux objets localisés dans les réseaux les plus proches du terrain, que nous appelons dans cette étude « réseaux d'extrémité », de communiquer entre eux grâce à l'universalité de l'Internet et de ses protocoles.

Les enjeux de l'IoT

Combien d'objets seront un jour connectés et à quelle échéance ? Les prévisions divergent : en 2011 Cisco avait annoncé 50 milliards d'objets connectés en 2020. Ce chiffre, qui aurait correspondu à un facteur 10 par rapport aux connexions conventionnelles sur l'Internet, ne sera pas atteint et l'on parle aujourd'hui de 20 milliards d'objets à cette échéance. Mais la tendance est forte, les chiffres régulièrement publiés par le Gartner Group font état d'une croissance de 33 % par an et le potentiel de connexion d'objets est manifestement considérable.

Mais la connectivité n'est pas une fin en soi : elle ne prend son sens que si elle s'accompagne de la transmission d'informations dont les destinataires peuvent tirer parti. L'IoT est donc un concept qui s'appuie en définitive sur deux grands courants :

- d'une part le développement des moyens de communication, à courte, moyenne ou longue distance, au travers de l'Internet et de tout l'écosystème des réseaux de communications qui peuvent se fédérer autour de lui ;
- d'autre part les méthodes nouvelles de traitement des données : tri, validation, traitement et stockage, toutes opérations qui peuvent se faire soit de façon locale, soit de façon « infonuagique » par des moyens hébergés dans le « cloud ». Ces données peuvent être « massives », eu égard au potentiel qu'offrent les solutions nouvelles de connectivité permettant de collecter des informations en provenance de myriades de capteurs. Le traitement des données dans l'IoT fait alors appel à des solutions qui relèvent du domaine des données massives (*Big Data*).

La présente étude, après avoir développé dans le chapitre 1, la problématique générale de l'IoT brièvement rappelée ci-dessus, aborde au chapitre 2 la question de son enjeu économique et de ses applications-clés. L'enjeu de l'IoT est considérable : il s'agit d'une technologie habilitante (*enabling technology*) qui sert de fondement à la modernisation des économies et qui va impacter l'évolution de la vie professionnelle et de la vie courante de chacun.

On retrouve l'IoT dans tous les grands programmes nationaux de modernisation des économies, qu'il s'agisse d'Industrie 4.0 en Allemagne, du Plan Industrie du futur en France, du Made in China en Chine ou de la Japan's Industrial Value Initiative au Japon.

L'enjeu économique de l'IoT peut s'apprécier sous deux aspects complémentaires :

- d'une part, il y a le marché des produits, systèmes, applications, solutions… sous forme matérielle ou logicielle : les estimations varient mais elles se situent pour l'ensemble du monde aux environs de 500 à 600 Mrd USD à des horizons variant de 2020 à 2025[1]. En France, une étude d'AT Kearney a évalué ce marché à 15 Mrd EUR en 2020 ;

[1] A noter que le Gartner group situe ce marché à 2 900 Mrd USD en 2020.

- d'autre part, il y a la création de valeur induite par l'IoT sous forme de modernisation de l'économie, d'amélioration de la productivité, de réduction des coûts d'approvisionnement, etc. L'évaluation de cet impact est très difficile car l'IoT se combine à d'autres facteurs de modernisation. Il semble cependant que l'on puisse multiplier par 4 ou 5 l'évaluation du marché pour estimer de façon globale l'impact de l'IoT sur l'économie. Au niveau mondial, cela conduirait à une création de valeur de l'ordre de 2 000 à 2 500 Mrd USD en 2025 soit 2,6 à 3,3 % du PIB mondial actuel. Pour la France, la création de valeur attendue serait, toujours selon l'étude d'AT Kearney, de 74 Mrd EUR en 2020 soit 3,3 % du PIB actuel (2015). Les estimations sont donc convergentes et confèrent un enjeu majeur au développement de l'IoT.

L'analyse des secteurs concernés présentée au § 2.3 montre qu'aucun secteur de l'activité économique n'échappe au défi des objets connectés. L'enjeu s'exprime souvent directement en termes de :

- productivité dans l'industrie avec l'Internet industriel des objets (IIoT) et dans l'agriculture ;
- qualité de services rendus, dans les domaines de la météo, de l'environnement, des transports et des infrastructures ;
- sécurité et confort dans les domaines de la santé, de la domotique (ou *home automation*) ;
- nouveaux services et nouveaux loisirs (sports, objets portés communicants, etc.).

Il est essentiel de prendre conscience que l'IoT n'est pas un simple perfectionnement technologique : c'est un mouvement disruptif qui conduit, comme l'Internet dans certains domaines (ventes par correspondance, tourisme, taxis, locations…) à une remise en cause des modèles d'affaires traditionnels en introduisant des circuits courts et en ouvrant la possibilité de collecter des masses d'information, de les croiser entre elles, d'analyser les signaux faibles et de prendre des décisions fondées sur une analyse objective des données. De la traditionnelle gestion des données, le *Data Management*, on passe ainsi au "*Management by Data*[2]" qui fait de la donnée la richesse centrale de l'entreprise. L'IoT est une chance à saisir pour redynamiser le secteur industriel de la France, soit en offrant de nouvelles solutions, soit en les intégrant dans le processus productif afin d'en améliorer l'efficacité.

Le secteur de la mobilité, qu'il s'agisse des véhicules électriques ou des drones, sera à coup sûr l'un des domaines où l'Internet des objets jouera un rôle central, couplé à d'autres technologies-clés telles que la géolocalisation précise (avec Galileo), le stockage par batteries, les moteurs électriques et l'électronique de puissance de haute performance. S'agissant d'un immense marché, orienté grand public mais avec des exigences techniques fortes, il est possible qu'il serve de marchepied aux autres segments du marché potentiel de l'IoT. La voiture connectée fait l'objet de développements considérables et d'une compétition déjà féroce dans le monde, qui va voir s'affronter les constructeurs automobiles traditionnels aux grands acteurs du domaine de l'information et de la communication, avec cependant des espaces de respiration possibles pour les PME et ETI innovantes. Les questions relatives à la mobilité ne sont pas traitées en détail dans cette étude car elles appellent, sur le plan de la disponibilité, de la fiabilité, de la sécurité et de la dynamique des processus, des investigations très approfondies que la SEE se propose de mener dans une phase à venir des travaux du Cercle des entreprises en y intégrant notamment les résultats attendus du développement de la 5e génération de communications mobiles.

Les architectures de l'IoT

Au chapitre 3, nous montrons comment les briques essentielles de l'IoT peuvent s'organiser pour constituer des architectures cohérentes répondant aux besoins à satisfaire. Par définition, le monde de l'Internet y est présent mais pas seulement : l'IoT est l'art de combiner le global et le local et de traiter et stocker les données au niveau approprié : l'IoT interfère avec l'infonuagique (*cloud computing*) mais débouche également sur des architectures de subsidiarité que

[2] ©KB Intelligence.

l'on appelle informatique en brouillard (*fog computing*) ou informatique à la marge (*edge computing*). L'analyse des exigences à satisfaire, notamment dans le domaine industriel en termes de temps réel, temps critique, disponibilité et fiabilité, conduit également à identifier des architectures maillées auxquelles correspondent des solutions de radiocommunications spécifiques.

La connectivité et les réseaux de communication

Au chapitre 4 et dans les annexes 2 à 5, nous abordons la question des réseaux de communication. Ces réseaux de communication, qui sont à la base de l'IoT, sont de plus en plus des réseaux sans fil de radiocommunications. L'offre en est extrêmement diversifiée et la quasi-totalité des solutions, même celles développées il y a 20 ans et plus, se réclament à présent de l'IoT. Cependant ces réseaux doivent satisfaire, s'il s'agit de réseaux d'extrémité, à des critères de robustesse face aux interférences avec les autres réseaux environnants, et d'économie d'énergie afin de permettre une longue durée de vie des batteries lorsque les objets ne sont pas connectés à une alimentation permanente en électricité.

Nous proposons une classification de ces réseaux en trois niveaux fonctionnels hiérarchiques :

- **les réseaux d'extrémité** qui desservent les objets proprement dits et qui peuvent être :
  - soit des réseaux locaux courte ou moyenne distance, tels que les Bluetooth Low Energy (BLE), ZigBee et autres réseaux IEEE 802.15.4 (ISA100.11a, Thread…), les Wi-Fi et notamment l'un des derniers nés de la série, le Wi-Fi 802.11ah publié en mai 2017 ;
  - soit des réseaux longue distance et à faible consommation d'énergie : concept récent, fruit des développements technologiques menés par des sociétés ou consortiums tels que Sigfox, LoRa, Ingenu, Weightless…
  - soit enfin des réseaux cellulaires sur de nouveaux profils de radiocommunications mobiles s'appuyant sur les systèmes de deuxième ou quatrième génération (2G et 4G), en attendant la 5G.
- **les réseaux d'infrastructure (*backbone*)** qui fédèrent les réseaux d'extrémité et qui peuvent être filaires et de type conventionnel, ou bien des réseaux sans fil, du type Wi-Fi 8021.11n notamment ;
- **les réseaux d'amenée (*backhaul*)** qui permettent le transfert de ces informations vers l'Internet et qui peuvent être filaires ou sans-fil (Wi-Fi, réseaux cellulaires ou satellitaires).

Bien entendu, dans la pratique, un même réseau peut combiner plusieurs fonctionnalités.

Il n'existe pas aujourd'hui de solution universelle : le chapitre 4 permet d'apprécier les avantages et inconvénients des solutions en présence au regard des exigences à satisfaire.

L'un des débats du moment est de savoir comment se positionneront les solutions faible énergie-longue distance opérant en bande libre (généralement à 868 MHz en Europe) au regard des nouvelles catégories de services de communications cellulaires standardisées par le 3GPP (*3rd Generation Partnership Project*) : EC-GSM sur la 2G, NB-IoT et eMTC sur la 4G. Certains pensent que l'une ou l'autre des approches l'emportera, d'autres estiment que les deux cohabiteront selon les marchés, d'autres enfin considèrent – et les conclusions de la présente étude vont plutôt dans ce sens – que les solutions 5G finiront par l'emporter, avec sans doute une agrégation de plus en plus forte entre réseaux cellulaires et réseaux opérant dans les bandes libres[3].

L'analyse de ces diverses solutions conduit à souligner l'importance d'élargir, en France et plus généralement en Europe, les fréquences utilisables par l'IoT et en particulier la petite bande libre des 868 MHz qui offre des qualités de propagation propices à l'IoT mais est bien trop étroite au regard des besoins à satisfaire et qui impose notamment un coefficient d'utilisation (*duty cycle*) de 1 % au plus, alors que la bande des 900 MHz est largement ouverte aux Etats-Unis.

[3] Notamment par extension de la technologie LTE-WLAN Aggregation définie par le 3GPP.

Les protocoles de l'IoT

Au chapitre 5 et dans l'annexe 6 est traitée la question des protocoles. En effet les informations, pour pouvoir circuler sur l'Internet, doivent être conditionnées sous forme de trames IP ce qui soulève de nombreuses questions. Au niveau de la couche « réseau », c'est-à-dire de la trame IP, le chapitre discute du passage de l'IPv4 vers l'IPv6, mutation qui s'accélère et semble indispensable à ne nombreux égards, notamment pour résoudre les problèmes d'adressage sur lesquels bute l'IPv4.

Mais les trames IP, IPv6 en particulier, ne peuvent pas circuler sur la plupart des réseaux d'extrémité qui ont été conçus pour faire transiter des trames courtes (typiquement de 127 octets dans le cas des réseaux 802.15.4), entre des abonnés repérés par des adresses également courtes. La couche logicielle 6LowPAN permet d'assurer la connectivité entre l'IPv6 et les réseaux 802.15.4. Elle peut être complétée par la couche additionnelle 802.15.4 TISCH permettant de faire fonctionner le réseau local, lorsque cela est nécessaire, en mode déterministe. Ces travaux d'adaptation ne sont pas encore achevés. Des travaux sont en cours pour développer des interfaces similaires à 6LowPAN entre Internet et les réseaux Bluetooth Low Energy et LoRaWAN (alors que cet interfaçage existe à l'état natif sur les réseaux Wi-Fi). La question se pose de savoir jusqu'à quel point un tel interfaçage est nécessaire. En d'autres termes, peut-on se contenter de connecter les réseaux d'extrémité à l'Internet par l'intermédiaire d'une passerelle, ce qui est le cas actuellement des réseaux Bluetooth Low Energy, Sigfox et LoRaWAN, ou bien faut-il permettre un adressage direct de chaque objet moyennant une couche adaptation du type 6LowPAN ? La question est aujourd'hui débattue et ce pourrait être l'un des avantages des solutions cellulaires que d'apporter à l'état natif une solution.

Les trames IP doivent également s'interfacer avec les niveaux supérieurs des piles protocolaires afin d'offrir aux applications les services requis. Si l'usage d'UDP, de préférence à TCP[4], est la règle quasi-générale dans l'IoT afin d'assurer aux communications la dynamique voulue, l'éventail des solutions reste ouvert au niveau de la couche application et, aux côtés de CoAP, variante légère de HTTP pour les équipements à ressources limitées, se développe l'usage du protocole Pub/Sub MQTT qui est particulièrement bien adapté aux applications de type SCADA pour le contrôle d'infrastructures ou d'installations distantes.

Les plates-formes de traitement et de stockage des données

Au chapitre 6 et dans l'annexe 7, sont présentées les plates-formes d'hébergement et de traitement des données offertes soit par les grands offreurs du type Google, Amazon, Microsoft, IBM soit par des sociétés ciblant leur offre sur des marchés particuliers et notamment sur le marché industriel (Siemens, General Electric, Actility…).

La cybersécurité de l'IoT

Au chapitre 7 et dans l'annexe 8, est traité le problème essentiel de la cybersécurité. L'IoT, de par son ouverture, son déploiement géographique, son évolutivité, offre une très grande surface d'attaque qu'il est très difficile de contrôler. L'IoT en tant que système informatique est sujet aux attaques classiques mais les années 2016/2017 ont vu éclore, à grande échelle, de nouvelles menaces telles que le déni distribué de service (DDoS), le déni de sommeil (DoS), la prise de contrôle d'équipements à distance, les rançongiciels, le déni de service sur le Wi-Fi, etc. Il n'est pas exagéré de dire que l'année 2016 a vu l'attaque progresser plus vite que la défense. Il est donc nécessaire d'organiser la riposte et le chapitre 7 donne des pistes pour y parvenir.

---

[4] UDP est un protocole qui consiste simplement à envoyer un datagramme vers un destinataire donné. TCP est un protocole plus complexe qui nécessite en particulier l'établissement d'une connexion avec le correspondant recherché.

Il faut bien entendu appliquer à l'IoT, lorsque cela est possible, les règles de base de la protection des systèmes informatiques et en particulier des systèmes de contrôle industriel selon la norme IEC 62443. Mais le découpage en zones, assorti d'une protection aux frontières, est difficile dans le cas de l'IoT et la surveillance physique des équipements, souvent isolés dans la nature, peut poser problème. L'étude IoT 2018 préconise de poursuivre dans la voie de la spécification et de la certification d'objets « *Secure by Design* » permettant à l'utilisateur d'accorder une confiance justifiée dans les équipements qu'il aura acquis. Cependant, ces équipements, même dotés de toutes les protections souhaitables, sont amenés à être intégrés dans un système dont il faut pouvoir contrôler le fonctionnement. La question d'une autorité centrale, pouvant contrôler les droits d'accès et les privilèges de tout objet souhaitant se raccorder à un système donné ,se trouve ainsi posée. A défaut d'une telle autorité – qui pourrait exister dans le cas de la 5G – l'étude IoT 2018 recommande de poursuivre le développement de systèmes de détection d'intrusion, permettant, grâce à des techniques d'intelligence artificielle et d'apprentissage, de détecter toute anomalie dans les trafics d'information. Les possibilités offertes par les systèmes décentralisés du type blockchain sont également à investiguer.

La nécessité de disposer de standards reconnus

L'analyse des marchés de l'IoT montre que dans la plupart des secteurs concernés par la présente étude – applications stationnaires, nomades ou faiblement mobiles – les technologies sont disponibles mais qu'elles ne sont pas pour autant stabilisées : beaucoup de voies de progrès restent ouvertes et l'interopérabilité entre ces solutions, malgré le facteur commun que constitue Internet, demeure insuffisante, notamment dès qu'il s'agit de construire un système cohérent associant divers types de réseaux d'extrémité. L'annexe 1 aborde la question de la standardisation et montre que, si plusieurs centaines de normes intéressant l'IoT sont aujourd'hui disponibles, en provenance de grands organismes de standardisation tels que l'IEEE, l'ISO, l'IEC et l'IETF, il existe très peu de normes véritablement transversales qui permettent de donner à l'IoT son universalité et d'assurer l'interopérabilité des objets connectés et, pour un type d'objet donné, leur interchangeabilité. L'identification unique des objets qui est une question essentielle pour l'organisation de la cybersécurité n'est pas un problème réglé aujourd'hui : l'adressage IP, la numérotation mobile, l'identification RFID et NFC, l'identification ISO sont autant de briques qu'il faudrait consolider dans un ensemble cohérent.

Chapitre 1 Aperçu sur l'Internet des objets

1.1. Un concept d'actualité mais difficile à définir

Le concept d'Internet des objets ou *Internet of Things* (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 tirer. 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.

La notion d'objets connectés est ancienne. Selon l'International Electrotechnical Commission (IEC), les distributeurs de billets, apparus en 1974, seraient les premiers objets connectés [1]. D'autres considèrent que la notion d'IoT est née à l'université Carnegie Mellon aux Etats-Unis, au début des années 1980, lorsque des étudiants eurent l'idée de doter la machine à Coca Cola de leur département de capteurs permettant de connaître à distance le nombre de bouteilles restant dans la machine et de prévenir ainsi une rupture de stock traumatisante. Assez vite, en parallèle au développement de l'Internet, des idées du même type se sont répandues, souvent axées sur la surveillance des réfrigérateurs et la gestion de leur contenu. Kevin Ashton, cofondateur de l'Auto-ID Center au MIT, revendique d'avoir été le premier à utiliser les termes "Internet of Things" pour décrire un réseau de capteurs communicants, dans une présentation faite à Procter et Gamble en 1999 [2]. D'autres considèrent que c'est l'annonce en 2007 par Steve Jobs du lancement de l'iPhone qui marque véritablement le démarrage du concept, toutes les réalisations antérieures étant restées anecdotiques.

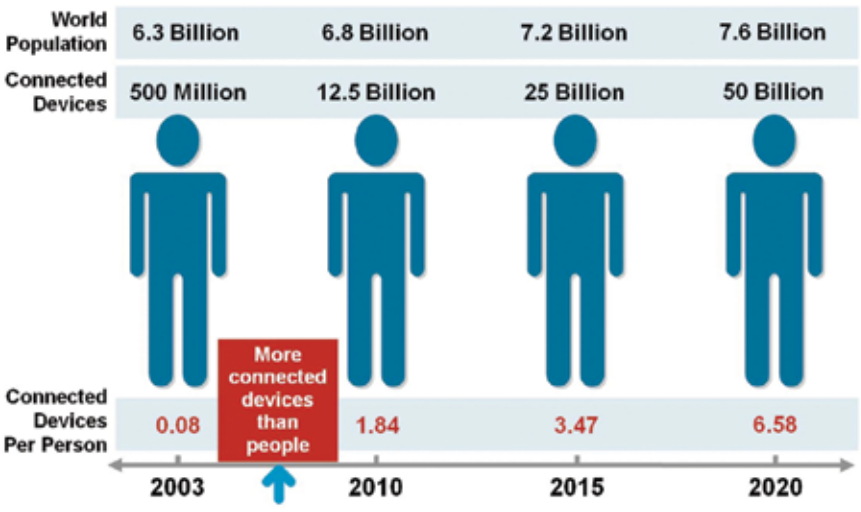


Figure 1-1 : Le développement de l'Internet des objets vu par Cisco en 2011.

Il est vrai que c'est depuis 2009-2010 que les publications se sont multipliées et les prévisions les plus enthousiastes ont été formulées. Parmi celles-ci, le Livre blanc publié par Cisco en 2011 [4] a eu un retentissement particulier ; il prévoyait en effet que le nombre d'objets connectés à l'*Internet of Everything* passerait de 500 millions en 2003 à 50 milliards en 2020 (figure 1-1). Cette prévision s'appuyait sur la constatation faite à l'époque d'un doublement du trafic Internet tous

les 5,32 ans. Cisco considérait également que 200 objets par personne pouvaient être connectés ce qui conduisait à un potentiel d'objets connectables de 1 500 milliards. Imaginer que 50 milliards soit 3,3 % soient effectivement connectés en 2020 apparaissaient comme une prévision raisonnable.

Il n'est pas sûr que cet échéancier de croissance soit respecté. Les dernières estimations du Gartner Group font en effet état de 8,4 milliards d'objets connectés en 2016 et en prévoient 20 milliards en 2020 [5]. Le chiffre de 50 milliards a eu cependant un effet d'entrainement considérable car il a été repris dans des dizaines d'études présentant l'Internet des objets comme un espace de développement pratiquement sans limite qu'il était urgent de s'approprier, tant pour soutenir le développement économique que pour améliorer les conditions de vie, le confort et le bien-être des populations.

Bien évidemment, s'est trouvée posée la question de savoir ce que l'on entendait par Internet des objets. De nombreuses organisations ont proposé des définitions. Un comité technique conjoint de l'ISO et de l'IEC (ISO/IEC JTC1 SWG5) [6] en a listé deux douzaines et même beaucoup plus si l'on intègre les appellations dérivées ou adjacentes de *Cyber Physical Systems (CPS), Machine to Machine communications* (M2M), *Internet of Everything* (IoE), *Industrial Internet of Things* (IIoT) et plus récemment Industrie 4.0, Usine du futur, etc.

Pour IoT 2018 nous proposons, au choix du lecteur deux définitions : l'une est celle proposée par l'UIT (Union Internationale des Télécommunications) [7], l'autre est propre aux auteurs de cette étude et est dérivée de celle élaborée par la chaire Orange « Innovation et régulation des systèmes numériques » de l'Ecole polytechnique [8].

Définition de l'UIT

« *L'IoT est l'infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution* ».

Définition IoT 2018

« *Un réseau de réseaux qui permet, via des dispositifs d'identification électronique d'entités physiques ou virtuelles, dites « objets connectés », et 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* ».

La diversité des définitions proposées pour l'IoT, et leur longueur très variable, montrent bien qu'il s'agit d'une notion complexe, évolutive et susceptible de recevoir différentes formes d'instanciation. Ces instanciations sont souvent « décorées » du vocable de « smart » : *smart citizen, smart home, smart building, smart grid, smart factory, smart city, smart territory…* Si le domaine d'application se trouve ainsi précisé, le flou demeure sur le contour et le contenu du système que l'on entend désigner.

L'Internet des objets apparait *in fine* comme un concept fonctionnel très général qui associe trois composantes fondamentales : les objets, les réseaux de communication, les données.

1.2. Les objets connectés

L'IoT se donne comme objectif de réaliser la connexion entre objets de toute nature, qu'ils soient matériels ou immatériels. Cisco a proposé l'appellation « Internet of Everything (IoE) » afin de souligner l'universalité du concept. Les objets matériels, ce sont les « choses » de la vie : tous les objets de la vie courante mais aussi les équipements du monde industriel ou professionnel. Les objets immatériels, ce sont les constructions de l'esprit et tout particulièrement les logiciels. A cette dichotomie, il faut ajouter les humains qui associent capacités matérielles et logicielles. En fait, tous les objets du monde de l'IoT dispose d'une capacité logicielle, d'une forme d'intelligence, plus ou

moins développée, qui leur permet de percevoir et saisir des informations, de les transmettre et éventuellement les traiter et, en retour, de comprendre des instructions et d'agir en conséquence.

La distinction pertinente est donc plutôt à faire entre « personnes » et « machines ». Les communications « personne à personne » sont celles rendues possibles par l'Internet, tel que nous le connaissons depuis 40 ans et plus. Les communications « machine à machine » sont celles du MtoM (ou M2M), qui sont parfois assimilées à l'IoT mais qui en constituent en fait un sous-ensemble. Ce sous-ensemble est extrêmement important du point de vue de la valeur ajoutée qui lui est associée. Ce sont en effet les communications M2M qui sont, pour une large part, à l'origine des progrès de productivité que l'on peut espérer grâce au développement « d'usines du futur » dotées de machines « intelligentes », plus efficaces, plus adaptatives, plus robustes, permettant de diminuer les coûts de production et de simplifier les chaînes d'approvisionnement.

On notera cependant que le M2M serait insuffisant s'il n'était pas associé à une communication entre les machines et les personnes car c'est *in fine* la conjonction de l'intelligence créatrice de l'Homme avec celle programmée de la machine qui permet de faire face aux situations les plus variées et de prendre, le plus rapidement possible, les bonnes décisions.

Les objets de l'IoT ont une personnalité propre : ils sont capables de saisir et de recevoir de l'information et de les échanger avec les autres objets de l'IoT. Mais il faut pour cela qu'ils puissent être identifiés de façon certaine. Le problème n'est pas trivial compte tenu du nombre considérable d'identifiants à gérer potentiellement. De sa solution dépend la possibilité pour les correspondants de s'identifier mutuellement de façon certaine, sans risque d'être abusés par des cyberattaques. L'identification est indispensable sur le plan local, elle l'est aussi sur un plan beaucoup plus large si l'on veut gérer la mobilité et offrir des fonctions d'itinérance (*roaming*). Enfin, pour les opérateurs de réseau, elle est nécessaire pour procéder, s'il y a lieu, à la facturation des services de communication.

Aujourd'hui, plusieurs systèmes d'identification coexistent :

- ceux du monde des télécoms et des réseaux cellulaires en particulier : numéros de téléphones mobiles, identifiants de carte SIM ;
- ceux du monde de l'Internet : adresses IP (v4 et v6), adresses MAC, adresses EUI 64 ;
- ceux du monde des RFID (étiquettes radiofréquences) et du NFC (*Near Field Communication*) : plusieurs systèmes d'identifiants coexistent aujourd'hui, notamment ceux promus par l'organisation EPCglobal.

Par ailleurs beaucoup de réseaux locaux utilisent des systèmes d'adressage locaux qui n'ont de signification que dans le périmètre couvert par ces réseaux. Comme on le verra plus loin dans l'étude, un mécanisme de correspondance (le standard 6LowPAN) a été défini entre les adresses IPv6 et les adresses locales des réseaux WLAN répondant au standard IEEE 802.15.4. Par contre, aucun mécanisme de ce type n'existe à ce jour pour les réseaux d'extrémité longues distances (LWPAN) du type LoRaWAN, ce qui pose problème à la fois du point de vue cybersécurité et organisation de l'itinérance (*roaming*)[1].

Récemment (août 2016), l'ISO et l'IEC ont publié une norme, l'ISO/IEC 29161 : 2016, visant à établir un schéma d'identification unique pour les objets de l'IoT [9]. Cette identification est censée être une construction universelle s'appliquant aussi bien aux objets physiques que virtuels ainsi qu'aux personnes. Une telle norme est indispensable, il reste à savoir si elle sera dans la pratique adoptée.

Une autre particularité des objets de l'IoT est d'être souvent éloignés d'une alimentation en énergie électrique permanente. Dans certains cas, les ampoules connectées par exemple, l'alimentation électrique ne pose pas de problème en régime normal. Il faut cependant penser aux situations dans lesquelles le réseau électrique devient défaillant et aux cas des objets isolés, tels

[5] Il est à signaler qu'en juillet 2017, la société Objenious, filiale de Bouygues Telecom, a annoncé s'être associée à la société Acklio afin d'intégrer les protocoles de l'Internet au réseau LoRaWAN d'Objenious.

que les capteurs de l'humidité des sols agricoles. Ces objets doivent être à même de remplir leurs fonctions et de communiquer leurs informations en s'appuyant sur des ressources locales en énergie qui pourront être des batteries ou des systèmes de piégeage de l'énergie ambiante (energy harvesting). Il faut alors limiter les consommations au strict minimum, aussi bien pour la prise d'informations que pour leur transmission, souvent par radio. Cette exigence a des incidences non seulement sur la conception des objets mais aussi sur le choix des protocoles de communication qui devront être aussi sobres que possible en énergie.

1.3. Les réseaux de communication

Les réseaux de communication entre objets constituent la deuxième composante essentielle de l'IoT. Si l'on admet comme objectif plausible le chiffre de 50 milliards d'objets connectés, on peut considérer que 10 % de ces objets seront des personnes et 90 % des machines avec, pour ces dernières, des perspectives de développement bien plus considérables que pour les humains. L'Internet a résolu le problème de la connectivité entre humains mais la connectivité entre objets pose des problèmes qui sont, au moins, de deux ordres de grandeur plus complexes. L'appellation « Internet des objets » laisse à penser que c'est l'Internet qui s'imposera et que l'IoT sera un gigantesque réseau regroupant autour de l'Internet des milliards d'objets. Certaines illustrations, telles que celle de la figure 1-2, incitent à croire qu'il en ira ainsi. En fait, tel n'est pas du tout le cas aujourd'hui. La plupart des objets n'ont pas besoin de disposer d'une connexion directe à l'Internet et il serait absolument inutile de déverser dans le nuage (le cloud) des milliards de milliards de données qui n'ont qu'un intérêt local ou éphémère.

Figure 1-2 : Une image d'Epinal. Les objets de l'IoT @Pixabay.

Comme le marque clairement la définition retenue pour la présente étude, l'Internet des objets doit être vu comme un **réseau de réseaux** dont l'élément fédérateur est l'Internet. Les réseaux « élémentaires » sont de plus en plus des réseaux locaux sans fil construits autour de divers systèmes de communication tels que Bluetooth, ZigBee, les Wi-Fi ou les LPWAN et qui communiquent avec l'Internet au travers d'un routeur de bordure qui peut assurer également la conversion de protocole pour pouvoir acheminer les données vers les serveurs connectés à Internet.

Cette structure fédérative peut être illustrée par la figure 1-3 où sont représentés des réseaux locaux et un réseau longue distance fédérés par l'Internet.

Il existe aujourd'hui une pléthore de réseaux locaux répondant à des spécifications diverses, certains standardisés, au moins pour les couches basses, d'autres propriétaires. Un aperçu en est donné dans le chapitre 4 consacré aux réseaux de communication avec des présentations plus détaillées dans les annexes 2 à 5. L'arrivée sur le marché des solutions LWPAN (longues distances et faible consommation) tels que Sigfox et LoRaWAN est venue enrichir encore davantage la palette des choix possibles. En fin d'année 2017, commenceront également à émerger les solutions cellulaires spécifiées en 2016 par le 3GPP : EC-GSM, eMTC et NB-IoT.

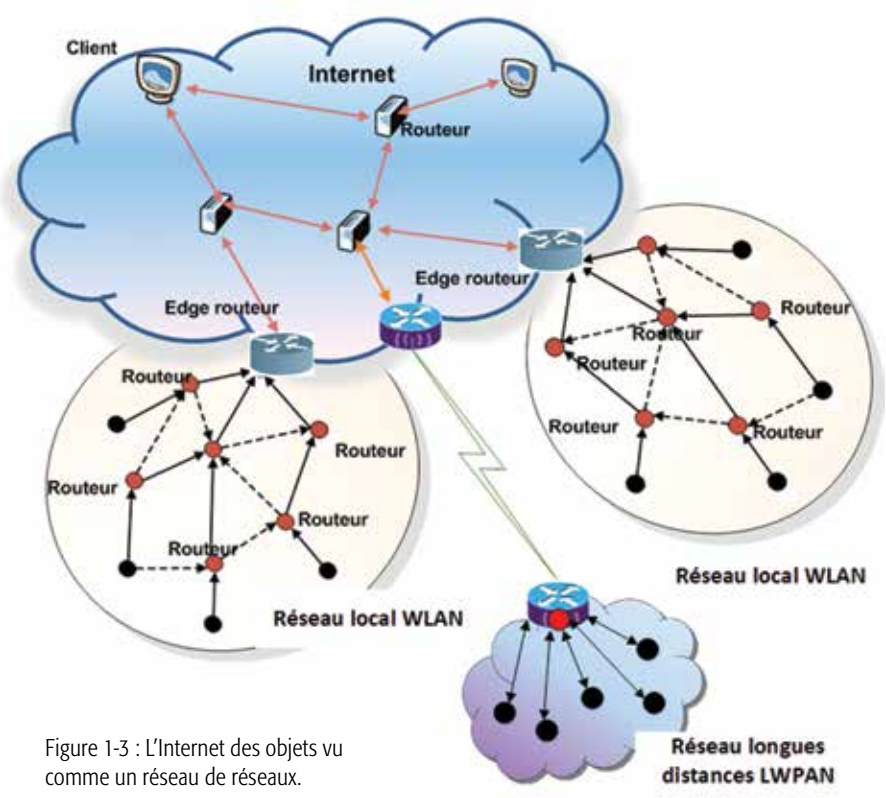


Figure 1-3 : L'Internet des objets vu comme un réseau de réseaux.

Toutes ces solutions ont leurs avantages et leurs inconvénients. Les consortiums qui généralement sont à l'origine ou soutiennent ces solutions font valoir leur adaptation aux exigences de l'IoT : être IoT ready ou IoT compliant est devenu un élément de langage incontournable du discours marketing. Mais ces solutions posent des problèmes d'interopérabilité, de positionnement respectif – notamment dans les bandes de fréquences radio, qui constituent une ressource rare – et d'intégration entre elles et avec l'Internet, pour constituer un ensemble cohérent et ouvert. Il est vraisemblable que la situation actuelle évoluera sous l'effet du marché, de l'évolution technologique et de l'émergence de nouveaux standards. Des solutions disparaîtront et la palette des choix se resserrera.

Cependant il est difficile de dire au stade actuel quel sera l'aboutissement de ce processus de rationalisation. Il est probable que l'adoption d'un identifiant unique, identifiant physique et/ou adresse IP, s'imposera car c'est une condition essentielle pour mettre en place des mesures de sécurité visant à prévenir les intrusions d'objets non autorisés dans les réseaux. Beaucoup pensent que l'adressage IPv6 finira par s'imposer mais d'aucuns estiment qu'il restera trop lourd pour répondre correctement aux besoins propres à l'IoT de communication rapide sur la base de messages courts. Il est possible que l'arrivée des solutions cellulaires, 4G aujourd'hui, 5G à l'horizon 2020, modifie fondamentalement la donne en offrant des possibilités de connexion omniprésentes, basées sur des standards universellement reconnus, apportant de façon native la compatibilité avec l'IPv6 et des solutions résilientes aux cyberattaques. Toutefois, d'aucuns estiment que ces solutions resteront coûteuses et dispendieuses en énergie et donc laisseront une large part du marché à d'autres solutions mieux adaptées aux besoins locaux.

1.4. Les données

Troisième volet du triptyque de l'IoT, les données sont en fait au cœur du concept d'Internet des objets. Plus de données, plus facilement : l'accroissement considérable du volume de données accessibles est le premier élément nouveau apporté par l'IoT en matière de *data*. Le développement de capteurs communicants, miniaturisés et bon marché, permet d'instrumenter de

façon beaucoup plus fine tous les procédés – au sens conceptuel du terme : qu'il s'agisse d'une installation industrielle ou agricole, d'un bâtiment, de l'environnement d'un malade, d'un véhicule, etc. – et de collecter ainsi, au travers de réseaux performants à très haut débit, des masses considérables de données.

Mais **collecter les données n'est pas un but en soi**. Les données n'ont d'intérêt que si elles sont utilisées pour accroître l'efficacité des procédés contrôlés. Traditionnellement, l'utilisateur était en prise directe avec le procédé et réagissait en fonction des données qu'il recevait. Un individu retire sa main s'il vient malencontreusement la placer sur une plaque chauffante ou remonte la température de réglage de son thermostat s'il constate, en rentrant chez lui, que la température de confort n'est pas atteinte. Au fil des années, l'algorithmie s'est enrichie et l'opérateur a pu disposer de méthodes d'analyse, de simulation et d'optimisation de plus en plus sophistiquées avant de prendre ses décisions sous forme d'envoi de consignes appropriées. L'IoT n'ôte rien à ces possibilités de contrôle direct des processus. Mais il ouvre de nouveaux horizons grâce aux capacités de traitement et de stockage hébergées dans le nuage qu'offre l'infonuagique (ou *cloud computing*).

En effet, après avoir été collectées par les réseaux d'extrémité appropriés, les données deviennent disponibles au niveau d'un routeur de bordure capable de les envoyer dans le monde de l'Internet. Réceptionnées par des serveurs appropriés, elles vont être triées et validées avant d'être stockées dans de gigantesques centres de données (*data centers*) capables d'héberger des exaoctets de données (1 Eo = 10^{18} octets soit l'équivalent de 10 milliards de dictionnaires Larousse en cinq volumes). Ces données sont alors mises à la disposition des utilisateurs ayant souscrit aux services du centre de données afin de leur permettre de les traiter et de les utiliser à leur convenance. L'utilisateur pourra soit faire appel à des services de traitement proposés de façon standardisée par la plate-forme Internet – c'est ce qu'on appelle les *analytics*, soit les rapatrier vers ses propres serveurs pour y effectuer les traitements de son choix.

Ce passage par le nuage offre plusieurs avantages. Il permet en effet de :

- disposer de capacités de traitement et de stockage considérables qu'un utilisateur aurait des difficultés à acquérir et à maintenir de façon isolée ;
- sécuriser les données et y donner accès à partir de postes clients situés n'importe où dans le monde ;
- accéder à des méthodes d'exploitation statistique relevant du traitement des données massives (*Big Data*) afin de tirer parti, en particulier, des signaux faibles enfouis dans un volume considérable de données ;
- croiser les flux de données entre eux et prendre en compte l'ensemble des paramètres pouvant influer sur la décision. Dans le domaine agricole, on pourra par exemple croiser entre elles des informations sur l'état des sols, la maturité des cultures, la météo, les cours sur les marchés, etc.Dans le domaine de la santé à domicile, on croisera les informations venant du patient avec l'expertise des médecins et les données disponibles dans des bases de données, etc.

La figure 1-4 explicite dans un cas tout à fait basique de processus. L'occupant d'un logement correctement instrumenté peut décider de continuer à piloter en direct, comme il l'a toujours fait, le chauffage, l'éclairage ou la sécurité de sa maison. Mais il peut aussi recourir à des services hébergés dans le nuage et, à distance ou en local, grâce à son smartphone ou à sa tablette, visionner l'intérieur de son logement, s'assurer du bon fonctionnement de ses appareils, programmer le chauffage en fonction du confort désiré ou en fonction du budget qu'il s'est fixé, programmer l'ouverture des stores, gérer des scénarios d'animation pour donner l'illusion de la présence, etc.

Ce schéma est transposable, moyennant adaptation, aux autres domaines d'application de l'IoT. Bien évidemment se trouve posée la question, déjà évoquée à propos de la connectivité et des réseaux, de l'opportunité d'envoyer sur l'Internet des données massives qui n'ont qu'un intérêt limité. Pour éviter un gaspillage de ressources au niveau du nuage et aussi pour offrir

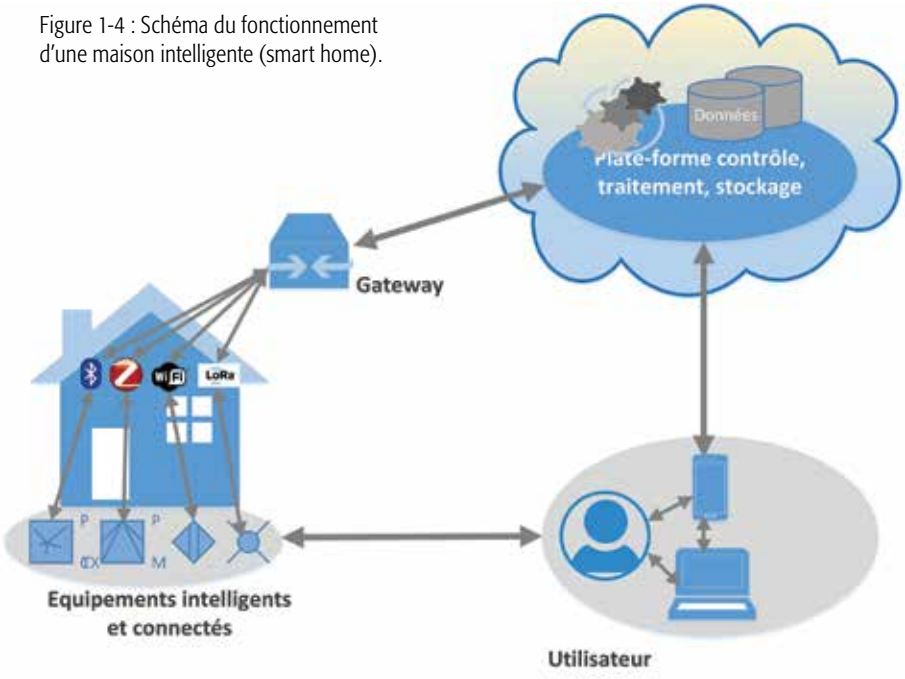


Figure 1-4 : Schéma du fonctionnement d'une maison intelligente (smart home).

une meilleure réactivité dans le traitement de ces données, est apparu le concept d'informatique de brouillard (*fog computing*) développé par Cisco et repris aujourd'hui par Microsoft sous le vocable d'informatique à la marge (*edge computing*). Cette approche consiste à appliquer le principe de subsidiarité dans le traitement et le stockage des données et à réaliser ces opérations de façon distribuée, là où des ressources (passerelles intelligentes ou nœuds terminaux) sont disponibles, au plus près des sources de données et/ou de leurs utilisateurs. Ce principe de calcul décentralisé, aussi dénommé *mesh computing, peer-to-peer computing, self-healing computing, autonomic computing, grid computing* est repris par tous les grands offreurs d'infrastructures dans le domaine de l'IoT. Amazon et Dell s'orientent vers cette approche dans laquelle des ressources dispersées, voire mobiles telles que les voitures, sont mobilisées pour participer au traitement des données, y compris selon des algorithmes évolués d'apprentissage et d'intelligence artificielle. L'*edge computing* est certainement l'une des voies les plus prometteuses dans le traitement des données afin de tempérer le développement des centres de données qui posent des problèmes croissants en termes de consommation d'énergie ; en outre leur dynamique – dépendant de celle des réseaux qui sont fortement sollicités par des applications très lourdes en flux de données images et vidéos – risque d'être insuffisante pour faire face aux besoins des applications telles que la mobilité, qui exigent des temps de latence de quelques millisecondes.

Les données, qui donnent à l'IoT sa valeur première, doivent être protégées. Les données sont comme une monnaie qui circule, des individus vont chercher à se les approprier pour en tirer parti de façon frauduleuse. Mais les données sont plus fragiles que l'argent : elles peuvent être divulguées alors qu'elles devraient rester confidentielles, elles peuvent être utilisées à des fins non autorisées, elles peuvent être corrompues ou tout simplement détruites. Les motivations de ces actes délictueux sont extraordinairement diverses : ce peut être la volonté de nuire, de discréditer, de se venger, de montrer simplement sa capacité à agir, d'intimider, d'étouffer un organe de presse, de tirer un profit – par revente ou utilisation de ces données ou versement d'une rançon –, de masquer d'autres actions, etc. Ces actes peuvent être commis par des Etats ou des bandes organisées agissant à leur solde, des hackeurs professionnels (*white hats* ou *black hats*), des amateurs ou des hackers occasionnels (*grey hats* ou *script kiddies*). Bien entendu les attaques sur les données vont souvent de pair avec la compromission des équipements qui les hébergent ou qui les traitent. Dans ce cas, le préjudice causé peut ne pas se limiter à celui occasionné aux données. Dans le cas des systèmes contrôlant des installations industrielles ou de grandes infrastructures (électricité, eau, transports), dans le domaine de la santé et dans bien d'autres domaines, la donnée n'a pas d'intérêt en elle-même (qui se préoccupe du niveau d'un fluide dans un réservoir ?) mais elle prend sa valeur au travers du procédé dans lequel elle s'insère. La corruption de données peut alors entrainer des situations catastrophiques, non pas dans le domaine de l'IT (*Information Technology*) mais dans celui des OT (*Operational*

Technology) qu'elles servent à piloter. Les responsables des procédés sous la menace de cyberattaques doivent prendre en conséquence des mesures pour protéger les données mais aussi pour mettre en sécurité le procédé dans le cas où une attaque viendrait à en compromettre le fonctionnement.

Au cours des toutes dernières années, **les attaques ont progressé plus vite que la défense**, en prenant des formes nouvelles, telles que le déni distribué de service ou le déni de sommeil, empêchant les objets de se mettre au repos et les conduisant à épuiser prématurément leurs batteries. Le chapitre 8 de l'étude dresse un panorama de l'état actuel de la question mais celle-ci est éminemment évolutive et il est clair que l'IoT ne pourra se développer que si, en parallèle à son développement, on parvient à mettre en place des mesures de protection permettant d'accorder une confiance justifiée aux objets et aux données qu'ils génèrent ou manipulent.

1.5. Les technologies de l'IoT

L'IoT n'est pas une technologie mais un concept qui s'appuie sur un ensemble de technologies qui se sont développées au cours des dernières décennies et qui, à différents niveaux, concourent à rendre possible l'IoT. Il est vain de chercher à lister toutes ces technologies car l'IoT irrigue l'ensemble de l'économie et par conséquent toutes les technologies que l'homme a développées peuvent trouver dans le concept d'IoT une justification nouvelle. A la base de toutes ces technologies, on trouve bien entendu les technologies matérielles et logicielles, toujours en progrès, qui permettent de doter, à des coûts et avec un encombrement de plus en plus réduits, les objets des capacités de traitement, de mémoire et de communication nécessaires à l'IoT. De façon plus spécifique, les points suivants doivent être soulignés :

- **les capteurs :** la technologie des capteurs continue à faire des progrès considérables en termes de précision, de fiabilité, d'encombrement, de capacité de traitement et de communication. Ces progrès associent l'utilisation de phénomènes physiques très diversifiés aux possibilités offertes par la microélectronique. Les microsystèmes électromécaniques sont des systèmes miniaturisés présentant des dimensions micrométriques, comprenant un ou plusieurs éléments mécaniques, utilisant l'électricité comme source d'énergie, en vue de réaliser une fonction de capteur ou d'actionneur. Ces dispositifs relevant des technologies MEMS, jouent un rôle fondamental et on les retrouve à présent dans un très grand nombre de secteurs : automobile, aéronautique, médecine, biologie, électronique grand public…

  Les technologies « nano » permettront de miniaturiser encore davantage les capteurs et, ce faisant, de réduire leur besoins en énergie qu'ils pourront, de plus en plus, satisfaire à partir de l'environnement en utilisant toutes les technologies de piégeage de l'énergie ambiante par *energy harvesting* (utilisation de l'énergie des vibrations, de l'effet piézo-électrique, de la thermoélectricité, de l'effet photoélectrique, etc.).

  Nous rattachons au domaine des capteurs celui des compteurs communicants (*smart meters*) qui, dans les statistiques de brevets, ressortent comme l'un des thèmes privilégiés de l'innovation relative à l'IoT.
- **les communications :** les techniques de communication sont au cœur de l'IoT puisque ce sont elles qui permettent de construire les réseaux nécessaires à son fonctionnement : réseaux d'extrémité sur lesquels viennent se connecter les objets, réseaux d'infrastructure permettant de fédérer ces réseaux d'extrémité, réseaux d'amenée permettant de convoyer les données vers le monde de l'Internet.

  Parmi ces technologies, les radiocommunications jouent un rôle primordial. Le chapitre 4 et les annexes 2 à 5 décrivent les principales technologies sans fil aujourd'hui disponibles mais les technologies filaires ne doivent pas être négligées. Les technologies de courant porteur en ligne, qui sont en particulier à la base du système Linky de compteurs communicants ont fait des progrès considérables et sont devenues d'application courante.

Pour l'avenir, les technologies Li-Fi associées à l'éclairage par LED semblent ouvrir des domaines d'application intéressants. Mais la plus grande attention doit surtout être portée à la 5e génération de radiocommunications pour les mobiles qui, grâce à la mise en œuvre de technologies réellement « disruptives » (MIMO massif, ondes millimétriques, etc.) pourrait devenir la technologie de base en matière de communications dans le domaine de l'IoT.

Il ne faudrait pas pour autant négliger les technologies satellitaires, encore onéreuses aujourd'hui, mais qui peuvent assez rapidement, grâce aux galaxies de satellites en cours de constitution, offrir des possibilités immenses pour l'interconnexion des objets, sur terre, dans l'air ou dans l'espace.

- **le traitement des données :** les technologies nouvelles de traitement des données sont un autre moteur de l'IoT. Nous rappellerons simplement les technologies de base qui permettent de miniaturiser les capacités de traitement et les mémoires et celles, technologies optiques notamment, qui permettent de construire les grands centres de données hébergés dans le nuage et de proposer les services d'infonuagique sous leurs différentes formes. Plus spécifiques à l'IoT, sont les technologies de traitement des données massives autour des fameux cinq V : *Volume, Velocity, Veracity, Variability* et *Variety*. Ces techniques du *Big Data*, d'inspiration statistique, débouchent sur des méthodes de recherche de tendances lourdes à partir de signaux faibles, d'analyse de risques, de détection de fragilités et de maintenance préventive.

Nous appelons également l'attention sur les technologies de *Digital Twins*, ou jumeaux numériques, qui permettent d'associer à un objet réel sa réplique numérique qui regroupe et modélise l'ensemble de ses caractéristiques, permettant d'effectuer sur lui toute sorte de tests, de simulations et de comparaisons. Ce concept est évidemment associé aux techniques de conception assistée mais il connaît aujourd'hui un prolongement essentiel avec les technologies d'impression 3D qui permettent de passer du jumeau numérique à son instanciation physique (figure 1-5).

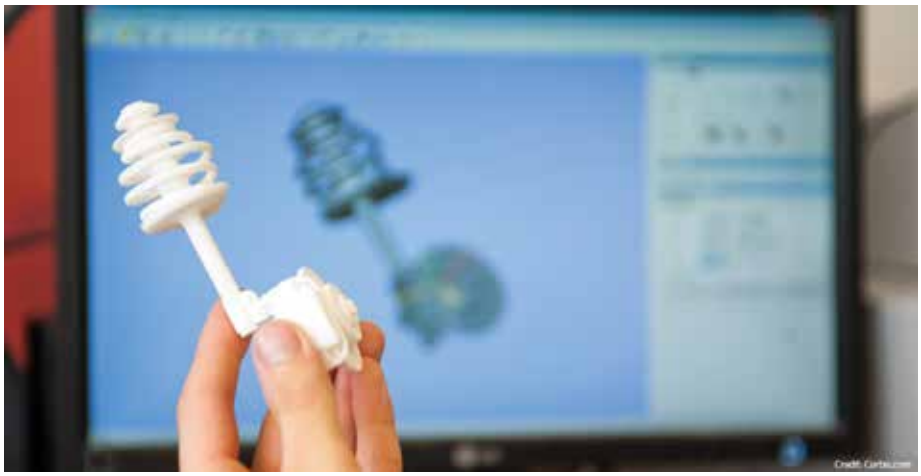


Figure 1-5 : Illustration du concept de jumeaux numériques – @Corbis.com.

Le BIM (*Building Information Modeling* ou modélisation des données du bâtiment) – fichier numérique qui comprend toute l'information technique nécessaire à la construction, à l'entretien, aux réparations éventuelles, aux modifications ou agrandissements et à la déconstruction d'un bâtiment, est un exemple d'approche *Digital Twin* appliquée à un système. Si les hologrammes utilisés lors de la campagne présidentielle française de 2017 avaient été de véritables hologrammes, ils auraient représenté un pas significatif de création d'un jumeau numérique pour un objet évidemment infiniment plus complexe qui est celui de l'être humain.

1.6. Les standards de l'IoT

L'un des fondements de l'IoT repose sur l'aptitude des objets à communiquer entre eux, quelle que soit leur nature, leur origine et leur localisation. Interopérabilité et ouverture sont deux mots clés de l'Internet des objets. Certains pensent que le recours au protocole IP est suffisant pour atteindre cet objectif. La question est en fait infiniment plus complexe et pose d'énormes problèmes de standardisation. Dans l'annexe 1, nous passons en revue les principales organisations qui se préoccupent de l'IoT, elles sont nombreuses et certaines (ETSI, IEEE, ISO/IEC, IETF)

ont émis de très nombreux standards interférant de près ou de loin avec l'IoT. Selon l'IEC, il y en aurait aujourd'hui plus de 400. Et pourtant le problème de la standardisation de l'IoT est loin d'être réglé. Il n'existe pas d'appréhension globale du concept de l'IoT conduisant à des déclinaisons sectorielles cohérentes avec une vision d'ensemble. Il existe de nombreuses approches spécifiques traitant d'une partie du problème dans un cadre donné mais la réconciliation du puzzle reste à faire.

L'ISO y travaille mais nous sommes aujourd'hui encore loin du compte. Il faudrait pour cela travailler concurremment sur plusieurs chantiers :

- **l'identification unique des objets :** nous avons évoqué précédemment cette question essentielle qui est un prérequis incontournable pour l'organisation de l'interopérabilité et de la cybersécurité. L'adressage IP, la numérotation mobile, l'identification RFID et NFC, l'identification ISO sont autant de briques qu'il faudrait consolider dans un ensemble cohérent ;
- **les couches basses de communication :** c'est le domaine où les initiatives sont le plus légion (voir le chapitre 4), sans qu'il soit possible aujourd'hui de savoir quelles solutions finiront par s'imposer. Au niveau le plus bas, celui de la couche physique, la standardisation des fréquences indispensables à l'IoT est loin d'être achevée, exception faite de la bande libre des 2,4 GHz mais qui est aujourd'hui trop fortement sollicitée. L'élargissement au niveau européen de la petite bande des 868 MHz, entreprise en France par l'ARCEP, est une initiative qu'il faut faire aboutir ;
- **la couche IP et les protocoles de niveau supérieur :** la question des protocoles Internet, traitée au chapitre 5, est tout aussi importante que celle des niveaux inférieurs. Les protocoles Internet sont nombreux et se concurrencent. Sans doute faut-il attendre que le marché joue son rôle et, de la même façon qu'il a su reconnaître l'universalité du protocole HTTP pour les communications entre personnes sur le Web, qu'il détermine les protocoles les plus adaptés au transfert des données de l'IoT, CoAP et MQTT étant aujourd'hui deux candidats bien placés.

Cependant, il faudra aller plus loin et définir des profils adaptés à chacune des classes d'équipements afin, par exemple, de pouvoir assurer l'interopérabilité fonctionnelle des objets, sans devenir tributaire d'un fournisseur particulier.

- **la gestion des données :** l'administration des données issues de l'IoT pose aujourd'hui de grands défis. Il faut en effet intégrer les données de nature différente, structurées ou non structurées, issues de sources disparates, afin qu'elles soient analysées et utilisées de concert avec des données déjà existantes. A défaut, les objets connectés ne resteront que des gadgets livrant à l'utilisateur des données éphémères dont il fera un usage pour le moins limité [10]. L'une des caractéristiques des données de l'IoT est de se présenter souvent sous forme de séries temporelles mais il n'est pas sûr que ceci confère à la donnée IoT un caractère très distinctif des données traditionnellement manipulées. Il est clair par contre que la valeur de l'IoT réside pour une large part dans l'exploitation de données issues de différentes origines. Pour en extraire cette valeur, il faut les agréger entre elles et avec les données préexistantes, et y ajouter une dimension d'analyse voire d'apprentissage. Cette fusion des données en ensembles cohérents sera facilitée si des standards suffisamment précis sont élaborés et acceptés.
- **la gestion des systèmes :** les systèmes pouvant se réclamer de l'IoT sont des systèmes complexes qui impliquent le déploiement de fonctionnalités allant bien au-delà de la gestion des communications : identification et accueil des nouveaux équipements, procédures d'accueil ou de configuration de ces nouveaux objets (*provisioning*), management des réseaux, gestion de la sécurité. Le projet de norme IEC/ISO 30141 [11] liste, sur la base d'une architecture de référence, les exigences à remplir ; mais ce texte sera plus un aide-mémoire des fonctionnalités à satisfaire qu'un guide sur la façon d'y pourvoir.

• **la cybersécurité :** comme nous l'avons souligné précédemment, la cybersécurité représente un défi majeur pour le développement de l'IoT. Nous y consacrons le chapitre 8. Des normes existent ou sont en cours de finalisation afin de fixer les exigences à satisfaire par les systèmes d'information, y compris les systèmes de contrôle de procédé (séries ISO/IEC 27000 et IEC 62443 notamment). Mais ces normes ne sont pas spécifiquement conçues pour répondre aux préoccupations de l'IoT. Une extension et une adaptation seraient nécessaires. Par ailleurs il faudrait définir de façon normative, ce qu'on appelle objet "*Secure by Design*". A une époque où les citoyens sont particulièrement sensibilisés aux questions de sécurité, il serait hautement souhaitable que des mécanismes de certification, reposant sur des référentiels normatifs, puissent leur apporter l'assurance que les objets qu'ils acquièrent ou manipulent, répondent aux exigences essentielles en matière de cybersécurité. De telles exigences ont été définies au niveau national pour certaines catégories d'équipements (compteurs communicants, contrôleurs d'automatisme), il serait souhaitable que cette approche soit étendue à des gammes beaucoup plus larges d'équipements, afin de mieux garantir leur sécurité de fonctionnement et d'éviter qu'ils ne soient pris en otage dans des armées de zombies (*botnets*) comme ce fut le cas dans les attaques en DDoS du deuxième semestre 2016.

1.7. Les enjeux de l'Internet des objets

L'Internet des objets concerne pratiquement tous les domaines de l'activité humaine qu'il s'agisse de la vie privée ou de la vie professionnelle, des activités individuelles ou des activités collectives.

L'enjeu en est donc considérable et nous exposons au chapitre 2 les formes que la généralisation du concept d'IoT pourrait revêtir dans un certain nombre de secteurs. Le chiffrage de cet enjeu n'est pas facile. En effet, les avantages apportés par l'IoT s'expriment souvent en termes d'amélioration du confort ou de simplification de la vie quotidienne. Comment chiffrer par exemple le surplus économique dégagé par une montre, un thermomètre connecté, un système de contrôle à distance du chauffage… Dans ce dernier cas, par exemple, une évaluation ne retenant que les économies d'énergie sera minorante et n'intègrera pas les aspects confort qui sont pourtant essentiels.

Il faut considérer également que le remplacement d'un objet par un objet connecté va s'inscrire généralement dans une trajectoire d'amélioration continue du produit avec une meilleure qualité de service pour l'usager et l'assurance du maintien de l'emploi pour les fabricants. Cette évolution darwinienne est manifeste dans le domaine de l'automobile dont les modèles n'ont cessé de s'améliorer depuis plus de 100 ans et continueront de le faire avec l'arrivée progressive des véhicules électriques, connectés et autonomes.

Dans le domaine de l'entreprise, il est cependant possible d'évaluer, au moins de façon grossière, l'enjeu économique que revêt l'IoT. Cisco s'y est risqué en publiant en 2013 un Livre blanc, traduit en français, sur « L'Internet of Everything, un potentiel de 14,4 trillions de dollars » [12]. Dans ce document, Cisco estime en effet à 14 400 Mrd USD, l'enjeu économique de l'IoT sur la période 2013-2022 pour les entreprises, c'est-à-dire, le montant de la valeur finale supplémentaire nette (valeur combinée de l'augmentation du chiffre d'affaires et de la baisse des coûts), susceptible d'être créée du fait de l'adoption des technologies de l'IoT. Sur ce total, 9 500 Mrd USD proviendraient d'une meilleure efficacité à l'intérieur de chacun des secteurs et le solde et de 4 900 Mrd USD d'initiatives transverses à l'ensemble des secteurs. De façon plus précise, l'origine des 14 400 Mrd USD se trouve décomposée de la façon suivante :

• meilleure utilisation des ressources : 2 500 Mrd USD ;
• amélioration de la productivité des employés : 2 500 Mrd USD ;
• meilleure organisation de la chaîne d'approvisionnement et de la logistique : 2 700 Mrd USD ;
• meilleure valorisation du potentiel client : 3 700 Mrd USD ;
• innovation plus efficace et délai de commercialisation réduits : 3 000 Mrd USD.

Bien entendu ces chiffres n'ont de valeur qu'indicative et peuvent donner lieu à débat, d'autant plus que, comme les analyses du chapitre 2 le confirment, le rythme de mise en œuvre de l'IoT n'est pas aussi rapide que celui imaginé par Cisco au début de années 2010. Il reste que l'enjeu est considérable et c'est l'une des raisons qui ont amené la SEE à engager l'élaboration de la présente étude.

1.8. Pourquoi IoT 2018

La présente étude répond à la vocation de la SEE de faire connaître et de promouvoir les technologies porteuses d'avenir dans les domaines de sa compétence. L'Internet des objets apparait à cet égard comme particulièrement bien centré sur l'électricité, l'électronique et les technologies de l'information et de la communication qui constituent les fondements mêmes de la SEE.

L'étude est publiée en tant que numéro hors série de la REE, Revue de l'électricité et de l'électronique, qui depuis six ans publie dans chacun de ses numéros des dossiers sur les technologies à fort potentiel. Le sujet de l'IoT a paru suffisamment important pour être traité dans un numéro hors série à l'issue d'auditions menées dans le cadre du Cercle des entreprises de la SEE. La liste des entreprises ayant accepté de participer à ces auditions est donnée à la fin de ce rapport.

IoT 2018 a une vocation pédagogique : il a pour ambition d'informer le lecteur sur le concept d'IoT et sur les technologies qui permettent de le mettre en œuvre. Il a également vocation à servir d'outil de réflexion pour guider les travaux, considérables, qui restent à réaliser afin de permettre la généralisation de l'IoT à tous les secteurs concernés. On y trouvera en particulier des appréciations sur l'état d'avancement de certaines techniques et des recommandations sur les voies qui devraient être suivies.

Le travail réalisé n'a pas l'ambition de couvrir l'intégralité du sujet. Il s'est efforcé de se focaliser sur les sujets réellement spécifiques à l'IoT et par conséquent certains thèmes transverses tels que l'infonuagique, aussi importants qu'ils soient, ne sont évoqués que de façon subsidiaire.

Par ailleurs, deux segments très importants n'ont été délibérément que rapidement abordés :

- d'une part les applications « très courtes distances », reposant sur des technologies telles que les RFID, les NFC, les *Body Area Networks* (BAN) qui sont signalées sans être véritablement traitées. Il en va en particulier des techniques de paiement sans contact ;
- d'autre part les applications de mobilité rapide, typiquement la voiture connectée. Il est probable que le véhicule connecté jouera un rôle majeur dans le développement de l'IoT car il constituera un marché grand public pouvant jouer un rôle d'entraînement fondamental dans le développement des technologies IoT. En particulier la 5e génération de communications mobiles pourrait trouver dans le véhicule connecté le tremplin qui la fera adopter par les autres marchés de l'IoT. Ce point est reconnu et acté dans le présent Libre blanc. Cependant, les exigences à satisfaire dans le domaine de la mobilité, en termes de dynamique (avec des temps de latence de quelques millisecondes), de sécurité fonctionnelle et de cybersécurité, font que ce segment applicatif ne peut pas être traité sur le même plan que les autres domaines. Il est envisagé par la SEE d'y consacrer des développements spécifiques en 2018 et 2019.

Malgré ces exceptions délibérées, le travail accompli dans IoT 2018 couvre un domaine d'application considérable, incluant les systèmes rencontrés dans le bâtiment, la ville, l'industrie, l'agriculture, la santé, les infrastructures…

En particulier, sans atteindre le degré d'exigences requis par la mobilité, le cas de l'industrie est traité avec attention. C'est le domaine de "l'*Industrial Internet of Things (IIoT)*" qui est une pierre angulaire pour le succès d'initiatives telles que Industrie 4.0 en Allemagne ou l'Usine du futur en France.

IoT et IIoT : quelles différences ?

Le développement de l'Internet des objets (IoT) capte l'attention du grand public du fait de ses applications grand public aux objets de la vie courante. L'Internet industriel des objets (IIoT) soulève cependant un intérêt croissant de la part des industriels compte tenu de son aptitude à permettre une surveillance à distance et une optimisation plus poussée des processus industriels qui n'auraient pas été concevables il y a seulement 10 ans. Les principes de l'IoT et de l'IIoT sont similaires et on peut considérer l'IIoT comme une implémentation particulière de l'IoT. Il y a cependant des caractéristiques essentielles qui distinguent les applications industrielles des applications classiques :

- les objets connectés de l'IIoT doivent être industriellement résistants : résistance à la température, à l'humidité, à l'environnement électromagnétique, aux atmosphères explosives, etc.
- les systèmes de l'IIOT doivent être conçus pour être extensibles, géographiquement sur des distances souvent très grandes et en nombre d'objets connectés qui peuvent atteindre des milliers. Il peut en résulter des volumes de données considérables à traiter, d'où la nécessité de recourir à des formes d'architecture en fog computing ou edge computing ;
- les systèmes doivent être personnalisables en fonction des données propres à chaque installation alors que les applications de l'IoT sont en règle générale standard ;
- les moyens de communication doivent être conçus pour répondre à des besoins spécifiques : capteurs en zones dangereuses ou difficilement accessibles, d'où des exigences sur la durée des batteries ; contraintes sur la disponibilité, le taux d'erreur, la synchronisation et la dynamique des transmissions d'où la nécessité de recourir à des solutions particulières ;
- exigences très fortes en matière de cybersécurité, une cyberattaque réussie pouvant avoir des conséquences dommageables non seulement en termes de pertes, d'altération ou de divulgation des données mais aussi et surtout en termes d'atteinte au bon fonctionnement des procédés et de risque pour la sécurité des biens et des personnes.

Encadré 1-1 : IoT et IIoT.

1.9. Références

[1] IEC role in the IoT (2017). http://www.iec.ch/about/brochures/pdf/technology/iec_role_IoT.pdf

[2] The "Only" Coke Machine on the Internet". Carnegie Mellon University. https://www.cs.cmu.edu/~coke/history_long.txt

[3] That 'Internet of Things' Thing; Kevin Ashton (2009) - http://www.rfidjournal.com/articles/view?4986

[4] The Internet of Things – Cisco White Paper. Dave Evans (2011). http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[5] Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. (février 2017). http://www.gartner.com/newsroom/id/3598917

[6] Internet of things (IoT) – ISO/IEC JTC1 (2014) https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/Internet_of_things_report-jtc1.pdf

[7] ITU-T Recommendations – Overview of Internet of things (2012) http://handle.itu.int/11.1002/1000/11559-en?locatt=format:pdf&auth

[8] Pierre-Jean Benghozi, Sylvain Bureau, Françoise Massit-Folea. L'Internet des objets. Quels enjeux pour les Européens ? Rapport de la chaire Orange "Innovation and régulation", Ecole polytechnique et TELECOM Paris Tech. 2008. https://halshs.archives-ouvertes.fr/hal-00405070/document

[9] ISO/IEC 29161:2016 – Information technology -- Data structure -- Unique identification for the Internet of Things (2016) https://www.iso.org/standard/45240.html
[10] The Internet of Useless things – http://www.Internetofuselessthings.io/
[11] ISO/IEC CD 30141: 2016 – Information technology – Internet of Things Reference Architecture (IoT RA). https://www.w3.org/WoT/IG/wiki/images/9/9a/10N0536_CD_text_of_ISO_IEC_30141.pdf
[12] Joseph Bradley, Joël Barbier, Doug Handler – L'Internet of Everything, un potentiel de 14,4 trillion de dollars (2016) https://www.cisco.com/web/FR/tomorrow-starts-here/pdf/ioe_economy_report_fr.pdf

Liste des acronymes utilisés

3GPP : 3rd Generation Partnership Project
6LowPAN : IPv6 LoW Power wireless Area Networks
6TISCH : IPv6 over the TSCH mode of IEEE 802.15.4e
ABD : Anomaly Based Detection
ABP : Activation by Personalization
ACL : Access Control List
AES : Advanced Encryption Standard
AES CCM : AES With CCM mode (voir AES et CCM)
AH : Authentication Header
AID : Association IDentifier
AMQP : Advanced Message Queuing Protocol
AP : Access Point
API : Application Programming Interface
Arcep : Autorité de régulation des communications électroniques et des postes
ARP : Address Resolution Protocol
ASK : Amplitude-Shift Keying
ATIS : The Alliance for Telecommunications Industry Solutions
BAN : Body Area Network
BBR : Backbone Router
BE : Backhoff Exponent
BLE : Bluetooth Low Energy
BLE : Battery Life Extension
BNEP : Bluetooth Network Encapsulation Protocol
BPSK : Binary phase-shift keying
BR/EDR : Bluetooth Basic Rate/Enhanced Data Rate
BSS : Basic Service Set
CAD : Channel Activity Detection
CAN : Car Area Network
CAS : Chinese Academy of Sciences
CBC-MAC : Cipher Block Chaining-Message Authentication Code
CBOR : Concise Binary Object Representation
CCA : Clear Channel Assessment
CCM ou CCMP : Counter mode with CBC-MAC Protocol
CDMA : Code Division Multiple Access
CEI : Commission électrotechnique Internationale (voir aussi IEC)
CFRG : Crypto Forum Research Group
CIoT : Consumer Internet of Things
CoAP : Constrained Application Protocol
CoRE : Constrained Restful Environments
CPA : Correlation Power Analysis
CPS : Cyber Physical Systems
CSMA-CA : Carrier Sense Multiple Access with Collision Avoidance.
CSS : Chirp Spread Spectrum
CTR : CounTeR
CVC : Chauffage, Ventilation et Climatisation
DDE : Dynamic Data Exchange
DDoS : Distributed Denial of Service
DDS : Data Distribution Service
DES : Data Encryption Standard
DFS : Dynamic Frequency Selection
DHCP : Dynamic Host Configuration Protocol
DICE : DTLS In Constrained Environments
DIFS : Distributed Inter Frame Space
DMS : Distribution Management System
DMZ : DeMilitarized Zone
DNS : Domain Name System
DoS : Denial of Service ou Denial of Sleep
DPA : Differential Power Analysis
DPI : Deep Packet Inspection
DRX : Discontinuous Reception
DSSS : Direct-Sequence Spread Spectrum
DTLS : Datagram Transport Layer Security
EAP : Extensible Authentication Protocol
ECDSA : Elliptic Curve Digital Signature Algorithm
EC-GSM : Extended Coverage-GSM
EDGE : Enhanced Data rates for GSM Evolution
EIRP : Emitted Isotropic Radiated Power
eMTC : Enhanced Machine-Type Communication
ESP : Encapsulating Security Payload
ETSI : European Telecommunications Standards Institute
EUI : Extended Unique Identifier
EXI : Efficient XML Interchange
FCC : Federal Communications Commission
FFD : Full-Function Équipement
FTP : File Transfer Protocol
GMSK : Gaussian minimum-shift keying
GPRS : General Packet Radio Service

GRE : General routing Encapsulation
HART : Highway Addressable Remote Transducer Protocol
HMAC : Hash-based Message Authentication Code
HSM : Hardware Security Module
HSS : Home Subscriber Server
HTTP : HyperText Transfer Protocol
HTTPS : HyperText Transfer Protocol Secure
HWMP : Hybrid Wireless Mesh Protocol
IaaS : Infrastructure as a Service
IAM : Identity and Access Management
IBSS : Independent Basic Service Set
ICV : Integrity Check Value
IDS : Intrusion Detection Systems
IEC : International Electrotechnical Commission (voir aussi CEI)
IEEE : Institute of Electrical and Electronics Engineers
IETF : Internet Engineering Task Force
IF-MAP : InterFace to Metadata Access Points
IIC : Industrial Internet Consortium
IIoT : Industrial Internet of Things
IIPA : Industrial IP Advantage
IoE : Internet of Everything
IOPS : Input/Output Operations Per Second
IoT : Internet of Things
IoTC : Internet of Things Consortium
IP : Internet Protocol
IPSO : IP Smart Objects
ISA : International Society of Automation
ISC : Internet Systems Consortium
ISM : Industrial, Scientific, Medical
ISO : International Organization for Standardization (voir aussi OIN)
IT : Information Technology
ITU : International Telecommunication Union (voir aussi UIT)
JTC : Joint Technical Committee
LAN : Local Area Network
LECIM : Low Energy Critical Infrastructure Monitoring
LOADng : Lightweight On-demand Ad hoc Distance-vector routing protocol – next generation
LoRa : Long Range
LTN : Low Throughput Network
LPWAN : Low-Power Wide Area Network
LSEND : Lightweight Secure Neighbor Discovery Protocol
LTE : Long Term Evolution
LTE-U : LTE in Unlicensed spectrum
LWA : LTE-WLAN Aggregation
LWIP : LTE WLAN integration with IPSec tunnel
M2M : Machine to Machine
MAC : Media Access Control
MAN : Metropolitan Area network
MIC : Message Integrity Code
MIMOSA : Operations and Maintenance Information Open System Alliance
MPTCP : Multipath TCP
MQTT : Message Queue Telemetry Transport
MQTT-SN : MQTT for Sensor Networks
NAN : Neighbourhood Area Network
NAPT : Network Address Port Translation
NAT : Network Address Translation
NAT-T : NAT Traversal
NB-IoT : Narrow Band Internet of Things
NDP : Neighbor Discovery Protocol
NFC : Near Field Communication
NIST : National Institute of Standards and Technology
NLP : Natural Language Processing
NOMA : Non Orthogonal Multiple Access
NoT : Network of Things
OASIS : Advancing open standards for the information society
OCF : Open Connectivity Foundation
ODBC : Open Database Connectivity
OFDM : Orthogonal Frequency Division Multiplexing
OGC : Open Geospatial Consortium
OIN : Organisation internationale de normalisation (voir aussi ISO)
OLE : Object Linking and Embedding
OMG : Object Management Group
OneM2M : Standards for M2M and the Internet of Things
OPC : OLE for Process Control
OPC-UA : OPC Unified Architecture
O-QPSK : Offset quadrature phase-shift keying
OSS : Operations Support System
OT : Operational Technology
OTAA : Over-the-Air Activation
PaaS : Platform as a Service
PAN : Personal Area Network
PCE : Path Computation Entity
PCEP : PCE Protocol
PDSU : Physical layer Service Data Unit

PER : Packet Error Rate
PIRE : Puissance isotrope de radiation émise
PMR : Private Mobile Radiocommunications
PSK : Pre-Shared Key
PSK : Phase-Shift Keying
PSM : Power Saving Mode
PUF : Physical Unclonable Function
QAM : Quadrature Amplitude Modulation
RAN : Regional Area Network
RC4 : Rivest Cipher 4
REST : Representational State Transfer
RFC : Request For Comments
RFD : Reduced-Function Équipement
RFID : Radio Frequency Identification
ROLL : Routing Over Low-power and Lossy networks
RPC : Remote Procedure Call
RPL : IPv6 Routing Protocol for Low-Power and Lossy Networks
RPMA : Random Phase Multiple Access
RRC : Radio Resource Control
RSA : Rivest Shamir Adelman
RSPG : Radio Spectrum Policy Group
RSSI : Received Signal Strength Indication
RTU : Remote Terminal Unit
SaaS : Software as a Service
SBD : Signature Based Detection
SC-FDMA : Single-Carrier Frequency-Division Multiple Access
SDK : Software Development Kit
SEG : SEcurity Gateway
SEND : SEcure Neighbor Discovery
SIM : Subscriber Identity Module
SIS : Systèmes Intégrés de Sécurité
SKKE : Symmetric-Key Key Establishment
SLAAC : Stateless Address Autoconfiguration
SMB : Service Message block
SNMP : Simple Network Management Protocol
SoC : System on Chip
SPI : Security Parameter Index
SSID : Service Set Identifier
SSL : Secure Sockets Layer
STOMP : Streaming Text Oriented Messaging Protocol
SUC : System Under Consideration
T2TRG : IRTF Thing-to-Thing Research Group
TCG : Trusted Computing Group
TCP : Transmission Control Protocol
TCXO : Temperature Compensated Crystal Oscillators
TKIP : Temporal Key Integrity Protocol
TLS : Transport Layer Security
TPC : Transmit Power Control
TPM : Trusted Platform Module
TRNG : True Random Number Generator
TSCH : Time-Slotted Channel Hopping
TVWS : TV White Spaces
TWP : Target Wake Time
UDP : User Datagram Protocol
UIT : Union internationale des télécommunications (voir aussi ITU)
UMTS : Universal Mobile Telecommunications System
UNB : Ultra Narrow Band
UNII : Unlicensed National Information Infrastructure
UPnP : Universal Plug and Play
UPS : Uninterruptible Power Supply
USIM : Universal Subscriber Identity Module
UWB : Ultra-Wide Band
V2X : Vehicle to Everything
VPN : Virtual Private Network
W3C : World Wide Web Consortium
WEP : Wired Equivalent Privacy
Wi-Fi : Wireless Fidelity
WiMAX : Worldwide Interoperability for Microwave Access
WLAN : Wireless Local Area Network
WMAN : Wireless Metropolitan Area network
WPA : Wi-Fi Protected Access
WPAN : Wireless Personal Area Network
XML : Extensible Markup Language
XMPP : Extensible Messaging and Presence Protocol
ZLL : ZigBee Light LinK

Les auteurs

Présidence du groupe de travail

François Gerin

Après différentes activités dans l'industrie et les services, François Gerin a été pendant près de 20 ans directeur général adjoint de Siemens France, groupe qu'il conseille actuellement dans les domaines R&D et innovation. Depuis 2013, il est président de la SEE, où il a notamment créé le Cercle des entreprises qui a conduit à la mise en place du GT « Internet des objets ».
Depuis début 2017, il est président d'AFNOR Certification.

Auteur principal

Jean-Pierre Hauet

Jean-Pierre Hauet a dirigé au cours de sa carrière le laboratoire central d'Alcatel-Alsthom et occupé les fonctions de Senior Vice-President & Chief Technology Officer du groupe Alstom. Il est actuellement Associate Partner de KB Intelligence, président de d'ISA-France et rédacteur en chef de la Revue de l'électricité et de l'électronique (REE). Il est membre émérite de la SEE, membre de l'ISA standards & Practices Board et voting member du comité cybersécurité ISA99.

Analyses marketing et participation aux travaux

Suzanne Debaille

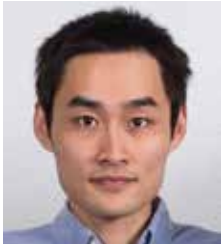
Docteur en mathématiques, Suzanne Debaille a eu un parcours professionnel International et opérationnel dans le domaine des réseaux et technologies de télécommunications.
Après des activités de recherche chez Orange Labs (CNET), elle crée la société de conseil Arcome, puis rejoint Vivendi Télécom International en tant que vice-présidente, directeur de la stratégie. Elle est ensuite nommée directeur des opérations Internationales d'outsourcing chez Alcatel-Nokia. Enfin, elle occupe les fonctions de directeur technique chez Thales Communication et Sécurité.
Elle poursuit actuellement des activités de conseil sur l'infogérance et sur la sécurité des réseaux informatiques et télécoms.

Relecture de l'ouvrage et validation

Alain Brenac

Alain Brenac, docteur ès Sciences et Ingénieur ENSIC, a mené une carrière de chercheur dans les laboratoires de France Télécom dans le domaine des composants et systèmes pour communications optiques puis au ministère de la recherche comme représentant national TIC auprès de la commission européenne. Il a ensuite apporté sa collaboration à la SEE, d'abord comme secrétaire général, puis comme administrateur et membre du comité de rédaction de la REE. Alain Brenac est membre émérite de la SEE et chevalier de l'ordre national du Mérite.

Contribution aux analyses techniques et aux annexes



Yihong Xu

Yihong Xu a participé à l'étude IOT 2018 dans le cadre d'un stage rentrant dans son cursus de formation d'ingénieur de Télécom Bretagne de l'Institut Mines-Télécom. Son concours a principalement porté sur l'identification et l'analyse des technologies de radiocommunication utilisées dans l'IoT ou en cours de développement.

Composition du groupe de travail

Actility	Nicolas Beaumer
Actility	Erika Gélinard
ACTEMIUM	Alexis Compagnon
ALTRAN	Didier Pagnoux
ARTERIA	Patrick Larradet
ATOS Worldgrid	Hervé Barancourt
ATOS Worldgrid	Alexis Coutarel
ATOS Digital Transformation & New Energy Services	Franck Freycenon
Bertin	Christophe Marnat
Bertin	Elie Znaty
Bouygues Télécom	Philippe Cola
CEA	Christophe Janneteau
CEA	Laurent Olmédo
Cisco Systems	Patrick Grossetête
Cisco Systems	Luc Imbert
Cisco Systems	Frédéric Géraud de Lescazes
EDF R&D	Julien Pestourie
ENGIE	Patrick Chanconie
ENGIE	Franck Lefebvre
Enedis	Alain Marty
Enedis	Pauline Gény
Enedis	Stéphane Ménoret
GE Energy Connections	Yasmine Fonda
Gimelec	Philippe Tailhades
IRT System X	Philippe Wolf
ISA-France et SEE	Jean-Pierre Hauet
La Poste	Benoît de Corn
Objenious (Groupe Bouygues)	Christophe Fouillé
Objenious (Groupe Bouygues)	Franck Moine
Qualcomm Technologies Inc.	Laurent Fournier
RTE	Philippe Lusseau
RTE	Bruno Meyer
RTE	François-Xavier Sardou

SEE	Suzanne Debaille
SEE	Jacques Horvilleur
SEE	Pierre Rolin
Siemens S.A.S	Jean Christophe Mathieu
Siemens S.A.S et SEE	François Gerin
Sigfox	Nicolas Lesconnec
SNCF	Amine Didioui
SNCF	David Sanz
Sopra-Steria	Alain Salmon
Sopra-Steria	Frédéric Dufaux
Sopra-Steria	Florent Brodziak
Télécom-Bretagne	Pr. Frédéric Cuppens
Télécom-Bretagne	Pr. Jean-Marie Bonnin
Télécom-Bretagne	Yihong Xu