Panorama de l'Internet des Objets V3

DigitalPlace

FUSION LABS
Internet des objets et services Cloud

orange™

SIERRA WIRELESS™

TELEGRAFIK
Services connectés intergénérationnels

OCCITECH
// INGENIERIE WEB

I.S.I.T

life.augmented

PANTZ AVOCATS

Auteurs :
Cyril Hlakkache - Orange,
Stéphane Monteil - Fusion Labs,
Matthieu Chaize - Telegrafik,
Etienne Zulauf - Occitech
Nicolas Damour - Sierra Wireless,
Lionel Gonzalez - Expert,
Alexandrine Pantz - Cabinet Pantz,
Laurent Vera, ST Microelectronics,
Frédéric Maraval, ISIT,
Thierry Le Gall, ISIT.

2018

Préface de :
Thierry Sachot
Président de la Cité de l'objet connecté

Contribution spéciale de :
Olivier Ezratty
Consultant en stratégies de l'innovation

Postface de :
Nicolas Demassieux
Senior Vice President,
Orange Labs Research

Sommaire :

Avant-propos

Une révolution est en marche. Depuis 30 ans, le réseau Internet a tissé le monde en reliant les Hommes. Mais, depuis quelques années, ce réseau s'étend aux objets : les parcmètres communiquent, comme les stations essence, les distributeurs de boissons, les alarmes, les capteurs de température, de position, de vitesse, etc.

L'événement **Innovation IT Day** (IITD) est la rencontre annuelle des acteurs de l'innovation où échangent les laboratoires de recherche, les jeunes pousses et les industriels. Dans le cadre de l'édition 2016, à l'initiative de membres de la commission innovation de DigitalPlace et d'une collaboration étendue (**Orange**, **Fusion Labs**, **Telegrafik**, **Occitech** et **Sierra Wireless**), s'est tenu un **atelier pour dresser le panorama de l'Internet des Objets** tant en termes économiques que techniques. C'est à la suite de ces échanges qu'est née l'initiative de rédaction de ce livre blanc.

Cette troisième version du document reflète l'ensemble des échanges et des débats ayant eu lieu lors des tables rondes de 2015, 2016 et 2017 qui accompagnaient le lancement des différentes version du document.

En 2016, il avait été identifié que la première version de ce document ne traitait que superficiellement des problématiques au combien essentielles que sont la sécurité et la place de la confidentialité des données personnelles. Ainsi la **seconde version** avait été complétée avec le développement de deux nouvelles parties rédigées avec l'aide d'experts des domaines concernés comme le **cabinet d'avocats Pantz.**

Pour 2018, nous avons décidé d'aller encore plus loin en développant trois nouveaux aspects de l'IoT : Le **hardware** avec l'aide de **STMicroelectronics** et la **sécurité des logiciels embarqués** avec la participation de la société **ISIT** et enfin des **cas d'usage** afin de profiter de retours d'expérience.

Sur cette base, l'**IITDay 2018** proposera un atelier ouvert à tous visant à présenter cette troisième version réalisée via une démarche collaborative qui sied bien à notre cluster, lieu permanent d'échanges de l'écosystème numérique en Occitanie.

Nous exprimons toute notre gratitude à **Cyril Hlakkache** pour avoir proposé et initié ce projet lors d'une Commission Innovation du cluster et à **Stéphane Monteil**, **Matthieu Chaize**, **Etienne Zulauf**, **Nicolas Damour**, **Lionel Gonzalez**, **Alexandrine Pantz**, **Laurent Vera, Frédéric Maraval** et **Thierry Le Gall** pour l'animation de l'atelier et la rédaction de ce document sur leur temps libre. L'esprit DigitalPlace en quelque sorte !

Fabien Gaiddon (Gaiddon Software) et **Olivier Nicolas** (Softeam e-Citiz)
Co-Présidents de la Commission Innovation du cluster **DigitalPlace**

Préface

L'Internet des Objets au cœur de la révolution numérique

Ce livre blanc dresse un **panorama actualisé du monde de l'Internet des Objets**, moteur d'une révolution numérique en marche. C'est une transformation qui concerne tous les domaines de notre vie en société incluant les domaines professionnels, publics ou privés. L'Internet des Objets (IoT) est porteur de mutations technologiques, économiques, politiques et sociales qui bouleversent les usages et le vivre ensemble. L'IoT favorise l'émergence de nouveaux services autour de la mobilité, de la santé, de la ville. Il renouvelle les modèles économiques des entreprises et des territoires. Il modifie leur gouvernance.

La collecte et la sécurité des données sont à la fois des opportunités et des risques qu'il convient d'identifier pour mieux s'en prémunir. Ce sont des enjeux à la fois individuels et collectifs, voire de souveraineté nationale, qu'il faut maîtriser pour favoriser le développement économique.

Nous sommes entrés dans l'ère de **l'économie du service et de l'usage**. Le client est informé et influent, il doit être écouté et impliqué.

Les impacts sont nombreux, particulièrement dans **l'Industrie du Futur**. L'automatisation diminue à court terme le nombre d'emplois à niveaux constants, mais elle engendre une meilleure compétitivité qui permet par le gain de parts de marchés de contribuer ainsi à augmenter la production à moyen terme. Les emplois créés ensuite sont plus qualifiés (pilotage des robots, maintenance, logiciels…).

Les tâches répétitives confiées aux robots permettent de libérer du temps pour les salariés pour créer **des suppléments de richesses et de nouvelles activités**. Le marché de l'Internet des Objets, encore émergent, fédère des entreprises, des territoires pour développer des filières d'excellence autour de cette thématique.

L'IoT en Pays de la Loire

C'est le cas pour le territoire angevin qui a inscrit l'Internet des Objets au cœur de son ambition économique. Son écosystème très dynamique compte plus de 900 entreprises et près de 7000 emplois dans la filière «numérique/électronique» dont de nombreux leaders (Eolane, Evolis, Valeo, Bull…), des entreprises à la pointe de l'innovation et des sociétés qui grandissent dans un esprit startup. **Labellisée French Tech en 2015** sur la thématique de l'IoT, Angers est devenue une référence nationale de l'Internet des Objets. C'est sur ce « terreau » favorable que la **Cité de l'Objet Connecté** est née en 2015 dans le cadre du plan

national « Objets Connectés ». Ce lieu novateur, unique en son genre, est une structure privée, portée par **l'entreprise Éolane** et dix-sept autres investisseurs. Elle est destinée à faire éclore des projets de start-up, de PME ou de grands groupes. Gary Shapiro lui-même reconnaît le caractère singulier de la Cité. Le directeur du plus grand salon d'électronique grand public, le CES de Las Vegas, évoque la Cité comme le seul accélérateur de start-up au monde se focalisant sur l'Internet des objets. Elle accueille des « makers » qui peuvent, en six mois, tester leur idée et trouver dans un seul lieu toutes les compétences techniques et les conseils au développement dont ils peuvent avoir besoin. Au sein de l'ancien bâtiment industriel entièrement réaménagé, situé tout près du parc des expositions d'Angers, les cerveaux des créateurs d'objets connectés sont en ébullition permanente. Les idées circulent, s'échangent, se confrontent…

Des Pays de la Loire à l'Occitanie

D'autres territoires se mobilisent également tel que **l'Occitanie via le cluster Digital Place**, parrain de ce livre blanc. Il organise chaque année **son Innovation IT Day (IITD) qui rassemble tous les acteurs de l'innovation**.

De nombreux exemples montrent que l'Internet des Objets confirme dès à présent l'énorme potentiel de développement **en France comme en Europe**, qu'il est capable de générer, en s'intégrant dans le cadre de notre transformation digitale.

Thierry SACHOT
Directeur Général d'Éolane
Président de la Cité de l'Objet connecté d'Angers

Présentation

À qui s'adresse ce livre blanc ? Il s'adresse en priorité à ceux qui, au sein de leur entreprise, s'apprêtent à lancer ou à contribuer à des projets mettant en œuvre de l'IoT. Bien que le contenu puisse être un peu difficile à aborder pour un lecteur néophyte, il reste accessible aux lecteurs curieux et intéressés par ce sujet d'actualité.

Quel est son objectif ? D'apporter un premier éclairage sur le sujet sous la forme d'un panorama, en abordant l'IoT sous différents aspects comme le marché et ses principaux freins, les technologies et les normes ainsi que les méthodes projets ou encore un éclairage juridique et la prise en compte de la sécurité des données.

Que doit-on en attendre ? Une fois ce livre blanc parcouru, vous aurez une vision plus large et plus détaillée sur l'IoT et vous pourrez alors décider d'aller plus loin en connaissance de cause, et ainsi approfondir les sujets précis qui vous sont vraiment utiles dans votre contexte.

Pourquoi une version 3 ? Les échanges ayant eu lieu lors des tables rondes organisées annuellement aux différentes éditions de l'**Innovation IT Day**, ont à chaque fois motivé le développement de nouvelles parties afin justement de répondre aux nouvelles questions soulevées par l'auditoire. C'est par le biais de ces rencontres avec nos lecteurs que cette dynamique d'enrichissement a donc trouvé son origine, justifiant successivement de nouvelles versions. Le succès rencontré par la première version du document (publié en mai 2016) nous a motivé à publier deux nouvelles versions proposant un contenu actualisé annuellement dans un domaine riche en actualités, mais aussi et surtout développant successivement plusieurs nouvelles parties dédiées à certains sujets particuliers comme la **sécurité**, le **juridique**, le **hardware** et l'**embarqué**. Pour développer ces nouvelles parties nous avons systématiquement accueilli de nouveaux contributeurs disposant d'une expertise dans ces domaines spécifiques.

Nous vous souhaitons une bonne lecture de cette nouvelle édition 2018 !

2. Le marché et sa dynamique

2.1. Introduction

L'Internet des objets, également appelé en anglais **Web of Things**[1] ou **IoT**[2], **M2M**[3] est représenté depuis quelques années comme une tendance lourde du marché. Elle est portée par des innovations technologiques majeures au cœur de la transformation numérique des entreprises, mais également à l'origine de nombreux nouveaux produits et services pour les particuliers.

Remarques :

- On peut noter que la **traduction française de l'IoT** n'a pas été choisie mot pour mot et le terme "Things", qui devrait textuellement se traduire par "Choses" en français, a laissé place au terme "**Objets**". Certains peuvent regretter cette traduction qui est plus orientée marché grand public (B2C) alors que l'IoT adresse aujourd'hui très fortement l'industrie et plus largement le marché B2B.

- aussi, le terme "**Internet**" de l'acronyme "IoT" peut ne pas toujours avoir sa place puisque les "Objets" ou les "Choses" ne sont pas nécessairement connectés au réseau Internet et peuvent rester sur des réseaux privés (LAN ou VPN). C'est pourquoi certains utilisent tout simplement la désignation "objets connectés".

- Parfois, certains **opposent l'IoT au M2M** et effectivement, les deux concepts sont très connexes. D'un côté, l'IoT se révèle être un concept qui se veut plus global où tous les objets de technologies très variées sont connectés à une plateforme Cloud via Internet, alors que du côté du M2M, ces machines se connectent directement en point à point via des technologies de type Wifi ou cellulaire, sur un système centralisé propriétaire et privé. La différence n'est pas évidente et actuellement le M2M a tendance à être inclus dans l'IoT qui est un terme devenu maintenant plus global permet de désigner un concept.

Le domaine se présente comme un nouvel eldorado, avec des prévisions commerciales gigantesques, projetant des milliards d'objets connectés dans les prochaines années. Des investissements importants sont réalisés de la part de sociétés majeures telles que Microsoft, IBM, Intel, Cisco, Google, Samsung, Philips, Amazon ou Orange.

---

[1] **Web of Things (Web des objets) :** désigne l'intégration de tout appareil interrogeable ou contrôlable à distance, dans le monde du World Wide Web.
[2] **IoT (Internet of Things) :** L'Internet des objets est un réseau d'objets physiques, dotés de technologies embarquées pour communiquer avec leur environnement local ou distant.
[3] **M2M (Machine-to-Machine) :** Technologies permettant des échanges entre machines, sans intervention humaine (par opposition aux Interfaces Hommes-Machines).

Qu'en est-il réellement ? Quels sont concrètement les domaines d'application ? Quels facteurs de développement et quels freins sont à l'œuvre sur ce marché ? Quels sont les enjeux à relever, les technologies, les standards, les compétences et les bonnes pratiques pour mettre en œuvre un projet ? Autant de questions auxquelles nous tentons de répondre dans la suite de ce document.

2.2. Segmentation du marché

Le marché du M2M et des objets connectés est segmenté par métier. Il se développe principalement via des applications verticales, avec des acteurs spécialisés. Les principaux domaines d'application sont les suivants :

- Énergie,
- Transports,
- Industrie (machines industrielles, logistique...) avec notamment le concept de l'**industrie 4.0**,
- Maison connectée (domotique...),
- Loisirs,
- Bâtiment connecté (tertiaire),
- Santé et bien-être,
- Commerce et distribution,
- Ville intelligente (Smart City).

Les secteurs de l'énergie et des transports sont historiquement ceux qui se sont le plus développés et qui ont constitué les plus forts volumes en termes de systèmes connectés et de chiffre d'affaires. Dans le domaine de l'énergie, les grands programmes nationaux de modernisation des infrastructures de distribution ont largement contribué au développement au travers des projets de télérelève de compteurs et de « smart grid[4] », avec des enjeux forts d'économies d'énergies. Dans les transports, les constructeurs et équipementiers se sont intéressés très tôt aux nouveaux services offerts par la connectivité, parfois incités par la réglementation : géolocalisation, information en temps réel, sécurité (eCall), infotainment (système fournissant de l'information et du divertissement), etc.

[4] **Smart grid :** Littéralement "Réseau électrique intelligent". Désigne l'optimisation de la production, de l'acheminement et de la consommation électrique par des outils informatiques. Il est créé dans le but de limiter les consommations superflues d'énergie et de réduire leurs effets sur l'environnement, et est partie prenante du concept de "ville intelligente".

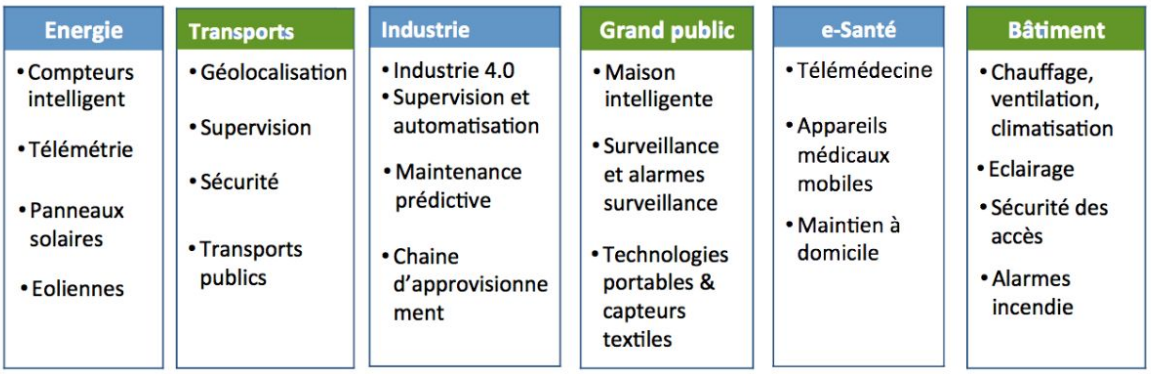


Illustration 1 : les segments de marché de l'IoT,
Source : Fusion Labs

Les autres secteurs B2B[5] et B2C[6] se développent également, avec parfois une moindre maturité, une forte fragmentation des solutions et des modèles économiques encore en devenir.

Le concept d'**Industrie 4.0** se présente comme une nouvelle manière d'organiser les moyens de production sous la forme d'usines intelligentes appelées "smart factories" ou "usines du futur". Ces usines sont capables d'une plus grande adaptabilité dans la production et d'une allocation plus efficace des ressources, ouvrant ainsi la voie à une nouvelle révolution industrielle.

2.3. Chaîne de valeur

La chaîne de valeur de l'Internet des objets est en correspondance avec la chaîne d'intégration technique des solutions. Elle implique :

- Les fabricants d'objets (devices hardware),
- Les fabricants de modules et passerelles de communication (Gateway),
- Les opérateurs de réseaux télécoms,
- Des éditeurs et intégrateurs de logiciels (middleware, plates-formes IoT et applications métier),
- Les prestataires de services métier.

[5] **B2B (Business to Business) :** Ensemble des activités d'une entreprise visant une clientèle d'entreprises.
[6] **B2C (Business to Consumer) :** Ensemble des activités d'une entreprise visant une clientèle de consommateurs.

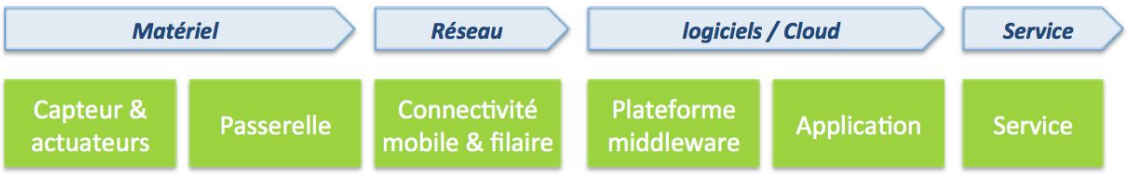


Illustration 2 : Chaîne de valeur IoT / M2M,
Source : Fusion Labs

La mise en œuvre d'un projet IoT de bout en bout fait intervenir et collaborer chacun de ces acteurs. De façon générale, on considère que la part la plus importante de la valeur se situe dans les logiciels et les services métier, notamment via l'analyse et l'exploitation des données collectées. La composante matérielle des solutions, en particulier celle permettant la connectivité, serait vouée à devenir une commodité à terme, du fait de la multiplication d'offres compétitives à faibles coûts. En pratique, les fournisseurs actuels de modules et de passerelles de communication poursuivent leur croissance et maintiennent leurs marges.

2.4. Acteurs représentatifs

La figure qui suit présente une sélection (non exhaustive) d'acteurs représentatifs du marché du M2M et de l'IoT :

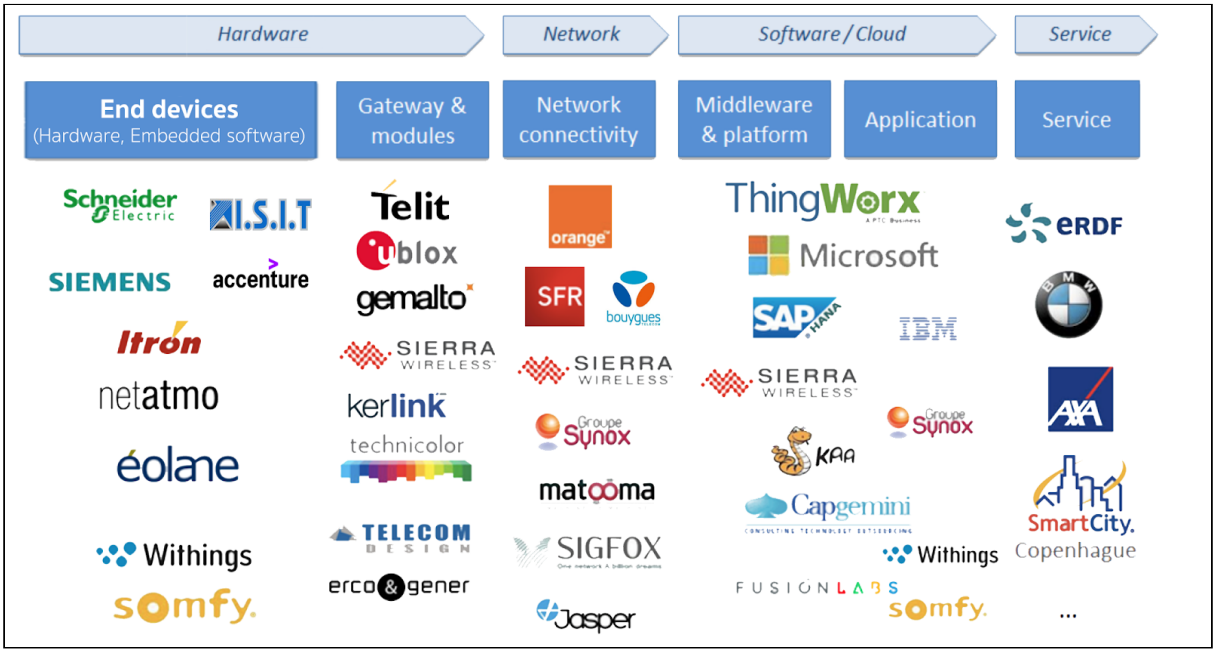


Illustration 3 : Quelques acteurs de l'IoT sur la chaîne de valeur
Source : Fusion Labs

Les **écosystèmes de startups** et les **PME innovantes** sont des acteurs importants, car nombreux ils sont porteurs d'innovation ou d'approches disruptives. Aujourd'hui, les grands acteurs ne vont plus sans les petits qui contribuent aux grands projets ou qui inspirent les

géants. Aussi, pour que ces écosystèmes soient audibles et visibles, les dispositifs d'incubation, de maquettage, d'accompagnement et d'accélération sont essentiels.

C'est par exemple du **Bizlab** du Groupe Airbus, d'**Orange Fab** du groupe Orange, **La cité de l'objet connectée** à Angers, l'**ACT 574** de la SNCF, la **Station F** aux Halles Freyssinet par Xavier Niel (PDG de Free), l'**IoT Valley** de la société Sigfox, le **FabLab Artilect** à Toulouse, et des **Villages by CA** du Crédit Agricole.

2.5. Modèle de maturité et d'adoption

La diffusion des technologies IoT sur le marché suit le modèle d'innovation théorisé par Everett Rogers en 1962. Celle-ci est représentée par une courbe montrant le niveau d'adoption de l'innovation par la population en fonction du temps. On distingue : Les innovateurs, très peu nombreux (2,5% de la population), les premiers adeptes (13,5%), La majorité précoce (34%) et la majorité tardive (34%) et enfin, les retardataires (16%).

Dans les années 90, Geoffrey Moore a complété cette théorie en se focalisant sur le marketing des produits high-tech. Il a notamment mis en évidence que l'étape la plus difficile était la transition pour passer du stade de l'adoption par les premiers adeptes au stade de la diffusion à large échelle au sein de la « majorité précoce » . Cette transition complexe est actuellement à l'œuvre dans le secteur du M2M et de l'IoT.

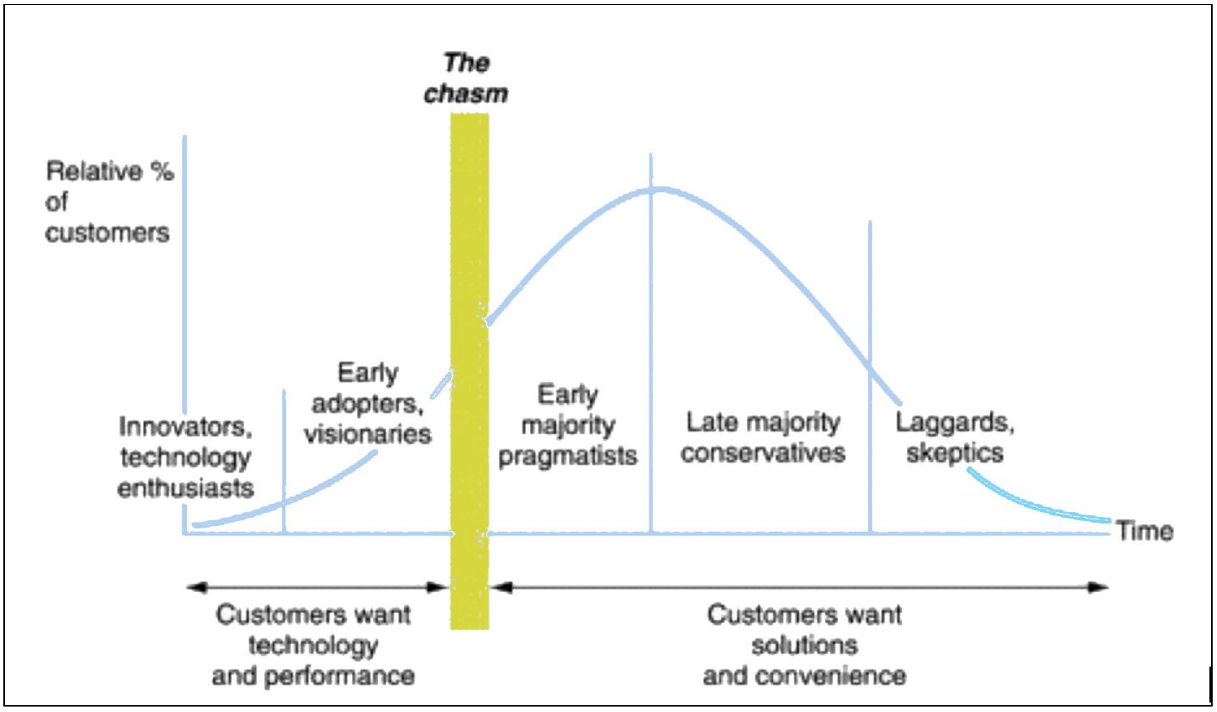


Illustration 4 : Courbe de Moore,
Source : Flickr savoirenactes.fr

Concrètement, le Gartner Group analyse chaque année au travers du « Hype Cycle » (voir **Hype Cycle 2017 version 2017**), le stade de maturité des technologies les plus prometteuses et les plus en visibilité. Dans cette étude, le plateau de productivité du M2M et de l'IoT serait atteint d'ici 2 à 5 ans.

2.6. Les moteurs du marché

2.6.1. Pour le grand public

Dans le monde du grand public, l'Internet des objets est encore perçu parfois comme un "gadget", à l'image par exemple des montres et des bracelets connectés. Il est cependant évident que l'IoT devient actuellement de plus en plus utile et nécessaire avec l'émergence de services à valeur ajoutée pour :

- **La santé** : télédiagnostic médical, surveillance et suivi avec par exemple l'émergence de dispositifs d'aide au maintien à domicile,
- **La domotique** : croissance importante du catalogue d'objets et de solution pour les particuliers permettant automatisation, surveillance à distance ou économies d'énergies,
- **Les Smart Cities** : digitalisation de la relation avec les administrés, gestion des stationnements et du suivi des transports, remontée d'informations pour les services techniques ou encore le partage d'information pour alimenter des dispositifs d'Open Data,
- **Les transports** : véhicules particuliers connectés et transports en commun,
- **Les loisirs** : en particulier dans le domaine du sport.

2.6.2. Pour les entreprises

Pour les entreprises, les moteurs du marché IoT sont les suivants :

- **Améliorer** l'efficacité des processus et des personnes,
- **Contrôler et réaliser** de l'assistance sur le matériel,
- **Développer** des systèmes de maintenance prédictive (sur les avions, les voitures, les machines ou les réseaux), des systèmes auto-adaptatifs en mode intégré, des services aux citoyens avec les villes intelligentes, appelées "Smart city".
- **Automatiser**, afin de sécuriser ou d'optimiser des activités,
- **Mettre en place de la traçabilité**, comme suivre sur du long terme la qualité d'un produit,
- **Apporter** des solutions innovantes pour le domaine de la Santé,
- **Proposer** des services d'infrastructure, comme les bâtiments connectés, appelés "Smart building",

- **Se positionner** sur le traitement intelligent des données, opportunités liées au "Big Data", via la collecte et l'analyse des données des capteurs,
- **Mettre en place** des approches **Open data**[7].

2.6.3. Les facteurs favorables

De manière générale, plusieurs facteurs favorables laissent présager de l'essor de l'IoT, en particulier :

- Les possibilités de **création de nouveaux services**,
- Les opportunités d'**optimisation des processus**,
- Les promesses de **réduction des coûts**,
- La **disponibilité croissante des technologies** (embarquées, réseaux, cloud...),
- Une **réduction progressive des coûts d'industrialisation** rendant ces solutions abordables,
- **L'appropriation croissante des nouveaux produits** par le grand public (Smart Home, objets wearable, mobilité, ...).

Aussi, ce qui rend l'émergence de l'IoT inévitable, c'est que cette technologie est le lien qui unit le monde réel au monde numérique. La transformation digitale passe par cette interconnexion entre notre réalité physique et la puissance du numérique, afin de proposer les services utiles et en rupture, une promesse portée par la digitalisation. Tisser un lien pour interconnecter est un prérequis pour être capable de mettre en place une intelligence globale via l'intégration de données transverses.

2.6.4 Introduction de l'IoT sur le marché des professionnels

L'expérience terrain acquise par les acteurs de l'IoT (opérateurs et intégrateurs) tend à démontrer que les clients finaux n'acquièrent pas ces technologies pour leur fonction directe de connectivité. En réalité, l'IoT se présente comme une brique technologique venant naturellement s'ajouter dans les solutions métier supportant les besoins de la transformation digitale des entreprises. Effectivement, on peut parfois observer entre grands groupes (ceci ne concerne donc pas le milieu de marché), une mutation notable dans la relation sur ce marché passant du mode client-fournisseur classique, où le client consomme simplement des produits sur étagère, vers un mode plutôt orienté partenaires, où ensemble, client et fournisseur, définissent une solution répondant maintenant à des **cas d'usage**. Et cette réponse, parfois inédite, inclut de plus en plus souvent la brique IoT dans la globalité de la solution proposée, car cette technologie permet d'offrir de nouvelles opportunités qui étaient auparavant inaccessibles.

Alors effectivement, même si le premier réflexe des **clients milieu de marché** est de solliciter des **démonstrateurs** et pour des **clients grand compte** des **Proof of Concept** basé sur une approche purement technologique de la brique IoT, c'est surtout et d'abord

[7] **Open Data :** Donnée numérique de nature privée ou publique, diffusée de manière structurée et ouverte à tous sans restriction technique, juridique ou financière.

pour comprendre, se rassurer et enfin s'approprier le concept, mais très rapidement, le besoin se transforme en un projet axé cas d'usage dans lequel l'IoT trouve naturellement sa place dans un service global allant de l'objet jusqu'aux applications métiers.

Ainsi, le marché évolue rapidement en prenant de la hauteur et il est fort à parier que très bientôt il sera perçu aussi simplement que la connectivité réseau devenue évidente dans le cadre des usages du monde digital.

2.7. Le ROI

La définition du modèle économique et la mesure du retour sur investissement sont les principales clés déterminant le succès des projets incluant de l'IoT. Les coûts sont mesurables, cependant, les gains sur un marché émergent, ne sont pas toujours faciles à déterminer.

Les principaux éléments permettant d'exprimer les gains sont :

- **De nouveaux revenus** (en particulier de services) : basés sur vos prévisions de vente, mais aussi basés sur une valorisation des données,
- **Des réductions des coûts** (fabrication, exploitation, maintenance) : basés sur des gains en homme / jour,
- **Des améliorations en termes de qualité** : mesurables sur les enquêtes client,
- **Une efficacité croissante** des processus et des personnes.

Il est donc essentiel de vous servir de ces leviers pour exprimer les gains qui sont nécessaires à la réalisation de votre "Business Case" et qui justifieront un arbitrage favorable au lancement de votre projet implémentant des technologies IoT.

Note : Concernant la **valorisation des données**, beaucoup estiment que c'est justement une des opportunités pour générer des revenus en plaçant ces données à la source du profit. La première approche est l'**Open Data** qui consiste à publier et partager ses données de manière gratuite (voir par exemple la démarche gouvernementale Open Data http://www.data.gouv.fr/fr/) . Cependant, la publication des données se présente aussi comme un service commercialisable par **l'exposition d'API** privées. Il est donc possible de les publier et les partager de manière rémunérée. Un bon compromis peut-être trouvé sur le modèle de Météo France sous la forme de deux gammes : une version limitée par adresse IP source et une **version premium** payante avec un niveau de service plus élevé https://donneespubliques.meteofrance.fr/**.**

La société SNCF est également un bel exemple de publication de données avec sa plateforme en ligne : https://data.sncf.com/ réalisée par OpenDataSoft et qui expose de nombreux jeux de données actualisés automatiquement ou manuellement.

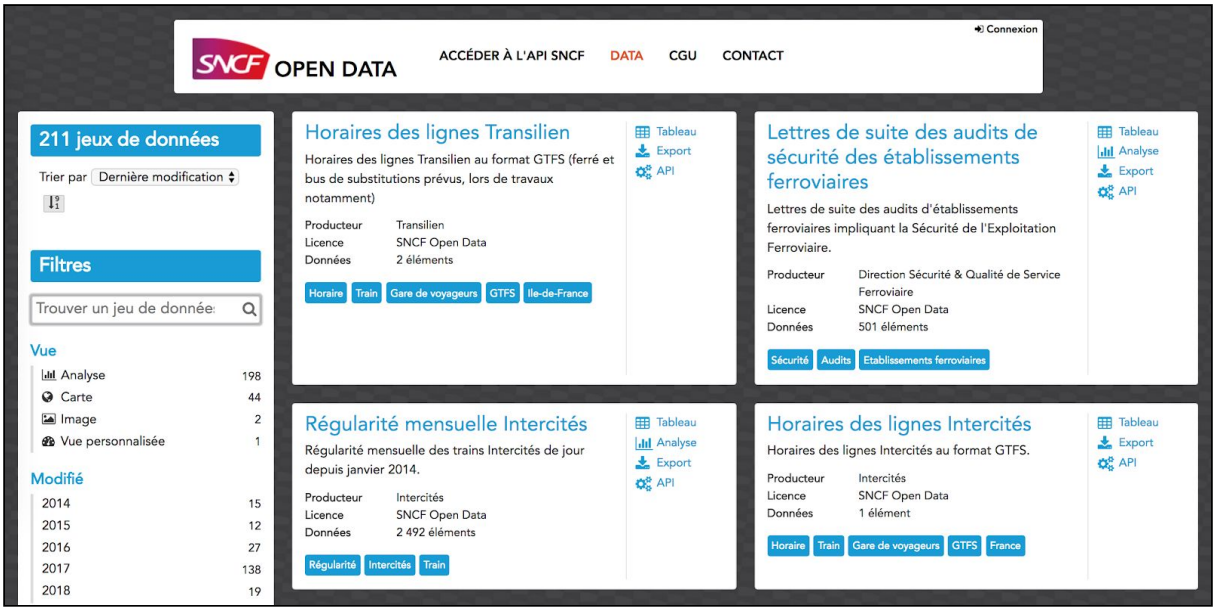


Illustration 5 : Site web https://data.sncf.com/ de la SNCF

Cet exercice de publication de vos données peut également avoir de l'influence sur votre manière d'envisager votre projet et l'orienter en priorité sur les axes qui apporteront le plus de bénéfices et le plus rapidement possible.

Une sécurité sur vos investissements réside également en votre capacité à savoir lotir intelligemment un projet à connotation innovante, très souvent mené en mode Agile. Cela permet d'offrir l'opportunité de tester le produit en cours de réalisation via les premiers livrables, et ainsi démontrer rapidement sa faisabilité et surtout que le ROI sera bien au rendez-vous.

Attention : **l'agilité** d'un projet ne consiste pas à mener un projet en totale improvisation sur un modèle Best Effort. C'est justement bien l'inverse puisque l'agilité demande une mobilisation totale des parties prenantes en suivant des méthodes de fonctionnement clairement définies. Alors, une des principales garanties de retour sur investissement repose aussi sur un engagement fort des contributeurs qui seront impliqués dans ce projet innovant. Un sponsoring de haut niveau peut être requis dans le cadre de grandes organisations pouvant par exemple être le **CDO**[8] (Chief Digital Officer) d'une entreprise qui permettra de garantir une mobilisation totale sur le projet.

[8] **CDO (Chief Digital Officer)** : Dirigeant responsable de la stratégie de transformation digitale de l'entreprise. Il fait partie du Comité Exécutif et dispose des pouvoirs nécessaires et suffisants pour accompagner cette transformation à tous les niveaux d'un grand groupe.

3. Les freins

L’IoT est un marché en en pleine croissance. Pour accompagner son développement et permettre d’accélérer pour atteindre un rythme à la hauteur des enjeux, il est nécessaire d’identifier ce qui ralentit l'expansion et pénalise les acteurs de cette révolution. Il est essentiel d’identifier et nommer clairement ces freins pour être en mesure de les lever. Voici en synthèse les principaux freins identifiés dans le domaine de l’IoT :

3.1. Manque de maturité des standards techniques

L’IoT manque cruellement d’un standard unifié permettant d’éviter la fragmentation actuellement observée. Les investisseurs, et donc les investissements, restent prudents tant que des questions se posent sur la pérennité des technologies et des équipements connectés actuellement disponibles. La différence des technologies est particulièrement visible sur le marché grand public entre les différents équipements, mais devient également très visible entre le monde professionnel et le monde grand public. Nous assistons en ce moment à l’émergence d’un IoT plus industriel dans le monde des professionnels qui est assez différent dans son ADN même.

3.2. Manque de maturité des usages

L’IoT impacte tous les domaines, les possibilités n’ont de limite que notre imagination, de ce fait, les usages proposés sont souvent totalement inédits. De ce fait, nous manquons nécessairement de recul et donc de maturité sur ces nouveaux usages (ex. bracelets connectés de surveillance médicale). Cependant, ce phénomène est commun à la plupart des innovations technologiques et ce frein est à relativiser.

Du point de vue des utilisateurs, il est parfois simplement nécessaire de provoquer l'usage pour permettre aux utilisateurs d’appréhender la technologie et de la démystifier afin de créer de l'appétence en connaissance de cause. La réussite est conditionnée par les premiers succès commerciaux, qui auront su tirer leur épingle du jeu en proposant des services pertinents accompagnés d’une bonne expérience utilisateur. Pour l’instant, beaucoup d’acteurs utilisent le label “IoT” pour lancer des objets qui n’apportent rien de plus (Exemple : Test de grossesse connecté…).

Du point de vue des professionnels, il est primordial de se lancer afin justement de progresser en maturité et pour cela les méthodes agiles sont particulièrement adaptées en démarrant par une étape préalable de démonstrateur (Proof Of Concept).

A chaque lancement d'une nouvelle application ou d'un nouveau service, on mesure un niveau d'acceptabilité. Cette notion complexe regroupe l'acceptabilité sociale et l'acceptabilité pratique.

3.3. Difficulté de gestion d'équipements matériels

Le domaine IoT est plus complexe que celui du Web, dans ce qui est de sa mise en oeuvre pour un projet précis. Cette complexité réside dans le fait qu'une solution IoT comprend des objets connectés qui sont matériels et diffusés dans le monde physique, ce qui induit à la fois des boîtiers, de l'électronique, du réseau et du logiciel. Les investissements et les compétences à mobiliser au lancement sont plus conséquents qu'avec des services purement logiciels.

Plusieurs aspects entrent en ligne de compte, telle que la construction, la livraison, le déploiement et la maintenance inhérents à la gestion d'équipements matériels. Cela demande à la fois de savoir mettre en place une organisation et des processus spécifiques, mais également d'imaginer des modèles de commercialisation permettant de rendre les services économiquement viables, sans oublier la logistique support et garantie.

La faible maturité des standards amplifie les risques d'inertie et d'adhérence technique. Cela implique de définir en amont une stratégie capable de s'adapter à des changements de contexte technologique pouvant intervenir à n'importe quel moment.

3.4. Acceptation difficile des nouveaux business models

L'évolution des modèles commerciaux, sous forme d'abonnements et avec des coûts récurrents, entraîne des réticences. Tout le monde n'est pas encore prêt à entrer dans un tel modèle de coûts et certains préfèrent l'achat en une seule fois, permettant une certaine sécurité dans la gestion des budgets et du prévisionnel associé. Il s'agit donc de passer d'un modèle à dominance CAPEX (dépenses d'investissement pour un matériel), vers un modèle à dominance OPEX (dépenses d'exploitation d'un produit ou service).

3.5. ROI difficile à démontrer

Le ROI n'est pas toujours évident à faire apparaître. Dans les méthodes de calcul du secteur numérique, beaucoup de paramètres subjectifs entrent en jeu, comme l'amélioration de l'image et de l'expérience utilisateur. Ces gains ne sont pas toujours facilement quantifiables en gains financiers. De ce fait, dans un contexte économique tendu, il n'est pas simple de mettre en évidence que les projets de transformation digitale incluant des objets

connectés sont prioritaires pour améliorer la productivité ou la performance d'une entreprise. Pourtant, le fait d'attendre peut faire perdre un temps précieux demain, car les objets connectés sont une réponse inévitable aux nouveaux défis qui nous attendent. L'intégration de ces objets dans votre quotidien, votre entreprise et vos activités nécessite d'être appliquée en situation réelle le plus tôt possible pour accumuler un maximum d'expérience et ainsi mieux agir et mieux investir demain.

3.6. Besoin de concepts innovants pour la gestion de l'énergie

Un autre élément technique clé pour le développement de l'IoT est l'énergie. Effectivement, les objets connectés demandent d'imaginer des systèmes d'alimentation en énergie innovants et adaptés au contexte. Ces objets peuvent se retrouver dans des environnements très variés, n'offrant que rarement la possibilité d'être reliés à une prise secteur ou alors dans des environnements où l'ajout de câbles ne pourra pas être réalisé pour des questions propres au contexte, comme dans l'aéronautique. Certains objets sont même coulés dans le béton pour plusieurs années. L'évolution de la performance des batteries embarquées, mais aussi l'innovation sur la bonne gestion de l'énergie, sont des points clés pour réussir à optimiser nos objets afin de les rendre éligibles à leur intégration dans l'environnement cible.

L'une des sources principales de consommation énergétique est la communication. Il est donc important d'optimiser les transmissions et réceptions de données. Pour cela, il faut imaginer des scénarios adaptés à chaque besoin et minimiser autant que faire se peut les émissions / réceptions de données. Certains objets devront disposer de l'intelligence embarquée capable de réaliser des calculs et des traitements en local avant de communiquer via le réseau afin d'économiser de l'énergie. D'autres objets utilisent des modes de communication très bas débit (LP WAN) peu gourmands en énergie, mais échangent de très faibles volumes de données très peu souvent.

3.7. Enjeux sécurité et cybersécurité

Dans un contexte où la transformation numérique intègre des services de plus en plus critiques comme pour la santé ou la finance, l'enjeu de sécurité vient s'ajouter à la liste des priorités. La distribution de ces objets à grande échelle, dans des environnements hétérogènes, engendre une complexité à sécuriser ces dispositifs, comme :

- La protection de l'accès physique à ces objets, par exemple les vols ou la connexion de dispositifs tiers sur l'objet,

- La sécurité des logiciels, par exemple les intrusions exploitant des failles, ou encore l'espionnage en utilisant des techniques de Man-in-the-middle[9] en écoute sur les différents canaux de communication réseau.

Cependant, le risque sécurité dans le domaine du numérique ne doit pas impliquer de "ne pas faire", mais plutôt de "faire dans les meilleures conditions possibles de sécurité". Alors, sécuriser une solution IoT peut être pensé comme l'élément final de la conception de la solution, comme un enrobage capable d'épouser le service, sans le perturber et proposant la meilleure sécurisation possible en fonction du service à délivrer.

L'amplification des risques de sécurité est effectivement une réalité dans le sens où le nombre de portes d'entrée s'est multiplié et dont l'hétérogénéité (hardware et logiciel avec différents systèmes d'exploitation) rendent extrêmement complexe la sécurisation. De ce fait, les attaques ou comme les exploits sont légions et souvent très médiatisés, par exemple :

- **En 2016, 500.000 caméras connectées chinoises ont participé à des attaques internet**. ce type d'attaque permet de générer des dénis (DDoS) de service en générant des flux vers une cible commune, saturant ainsi l'ensemble de ses ressources. On peut citer par exemple **l'attaque du blog du journaliste spécialisé en cybersécurité Brian Krebs**, qui a été ciblé par une attaque record atteignant un débit de 620 Gb/s

- **Le malware[10] Mirai** ou encore **le botnet[11] Hajime** visent des objets connectés via le port Telnet et les mots de passe par défaut des constructeurs ou des failles firmware, enrôlant ainsi les objets dans un réseau de botnet visant à réaliser des attaques à la demande comme des DDoS. Cet exemple démontre qu'il est maintenant aisé de construire de véritables armées à travers la planète permettant de réaliser des attaques de grande ampleur et préparées en toute discrétion.

- **En 2016, un criminel aurait réussi à lancer une cyberattaque visant les écluses du barrage de l'état de New York (USA)** visant à déclencher une inondation. Heureusement détecté, cet incident a démontré toute l'étendue des risques liés aux dispositifs connectés, ce qui sera par exemple le cas des Smart Cities.

Ce sujet est plus largement développé dans la **partie 8** dédiée à la sécurité de l'IoT.

[9] **Man-in-the-middle :** Attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication a été compromis.
[10] **Malware :** Logiciel malveillant développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté.
[11] **Botnet :** Contraction de « robot » et « network » est un réseau de bots informatiques qui sont des programmes connectés à Internet qui communiquent avec d'autres similaires pour l'exécution de certaines tâches comme des attaques collectives synchronisées.

3.8. Manque de cadre juridique solide

La diffusion de ces nouveaux dispositifs, intégrant souvent des capteurs d'informations environnementales, soulève également des questions et des réactions sur un plan juridique concernant l'utilisation de ces services et des données associées, comme :

- La protection de la vie privée : Les objets communicants peuvent être intégrés dans différents lieux, au plus près des personnes et parfois au plus près du corps. Ces dispositifs sont alors capables de collecter des informations privées, dont l'exploitation doit être cadrée pour qu'ils soient acceptables.
- Les risques sanitaires : Les équipements connectés intègrent un large panel de technologies radio, comme le Wifi, le BLE[11], le NFC[12], le LiFi[13] ou encore les ultrasons. L'émergence de certaines pathologies comme la sensibilité au rayonnement électromagnétique, qualifiée d'électro-hypersensibilité, ou encore la Malillumination (liée au scintillement des LED), demandent à mieux considérer ces risques dans la diffusion des objets connectés qui ont vocation à exploiter principalement des connexions sans-fil.

3.9 Manque de données et plateformes partagées

La promesse de mise en intelligence de l'ensemble des processus, comme dans la **Smart City** ou même demain les **Smart Country** (à l'échelle d'un pays où les villes communiquent entre-elles), demande de mettre en place un partage des données, à la fois entre les différents fournisseurs de service, mais aussi entre les différentes verticales (énergie, transport…). Pour que cela soit possible, il est nécessaire de développer des solutions permettant justement cette transitivité de la donnée afin de mettre en place des services intelligents de bout en bout. Pour cela, non seulement les données d'un domaine précis doivent être consommables par un autre domaine, mais elles doivent aussi être normalisées et accessibles via des méthodes et des protocoles standardisés. L'**Open Data** et les plateformes **Open Source**, ainsi que des standards documentés sont des besoins fondamentaux pour atteindre les objectifs des solutions digitales incluant de l'IoT. Cependant, ces ingrédients manquent encore cruellement et beaucoup de solutions propriétaires dominent pour le moment le marché. Des initiatives comme l'**OpenData France** http://www.opendatafrance.net/, **Fiware** https://www.fiware.org/ ou encore également la **Fondation Eclipse** https://iot.eclipse.org/cloud/ vont dans le sens de ces pré requis.

[12] **NFC (Near Field Communication) :** Technologie de communication sans fil en champ proche, à courte portée et utilisant des hautes fréquences.
[13] **LiFi (Light Fidelity) :** Technologie de communication sans fil basée sur l'utilisation de la lumière visible (optique) du spectre électromagnétique.

Note : **Fiware** est une **plateforme middleware Open Source** développée collectivement par une communauté d'experts. Le projet Fiware est géré sous la forme d'une fondation pilotée par la **Communauté Européenne**. Ce projet est l'un des plus prometteur en terme d'approche globale pour les Smart Cities et l'initiative est supportée par de grandes entreprises comme Telefonica et Orange.

3.10 Confiance des acheteurs en la pérennité de la solution

Le 15 mai 2016, la société Revolv acquise par Google en 2014 fermait définitivement ses services, rendant inutilisables les milliers de boîtiers qu'elle avait vendu et qui permettaient de contrôler différents appareils dans sa maison (fenêtres, serrures, lumières, etc.). Ces boîtiers étaient vendus $300 avec un abonnement aux services connectés "à vie"...

Ainsi donc, les objets IoT peuvent devenir parfaitement obsolètes tout en étant toujours parfaitement fonctionnels. Un paradoxe qui devrait certainement défrayer à nouveau la chronique dans le futur à maintes reprises. Il s'explique par les coûts récurrents de fonctionnement sur lesquels nous reviendrons, si l'éditeur n'est pas rentable il n'aura d'autre choix que de fermer ses services. Cela justifie d'ailleurs un abonnement pour utiliser l'objet plutôt qu'une licence "à vie" forcément à perte au bout d'un moment.

En tout état de cause, les clients potentiels seront de plus en plus sensibles à la fiabilité de l'entreprise éditrice, sur des garanties de maintien de ses services voire des proposition d'alternatives en cas de fermeture des services, comme la publication open-source du code permettant à d'autres de continuer à faire fonctionner les objets.

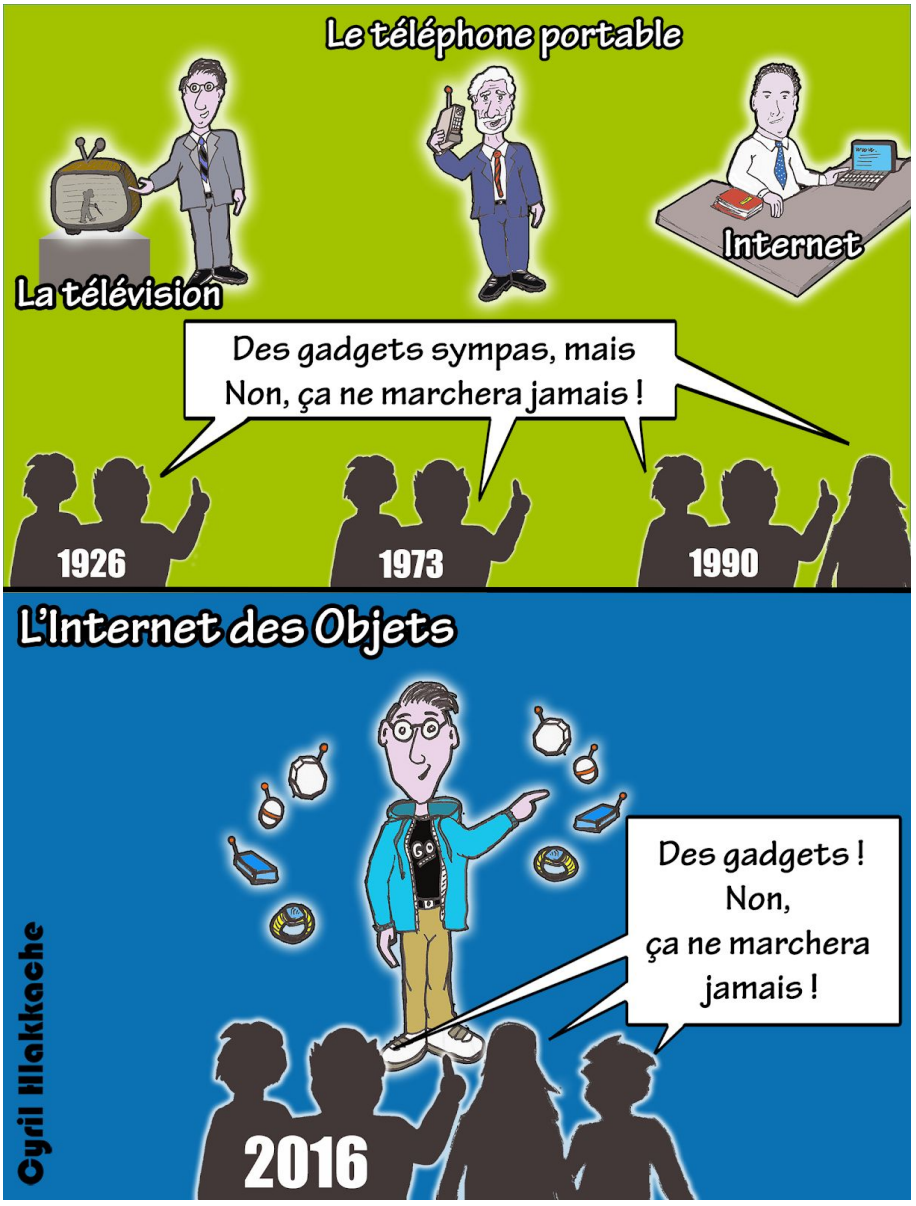
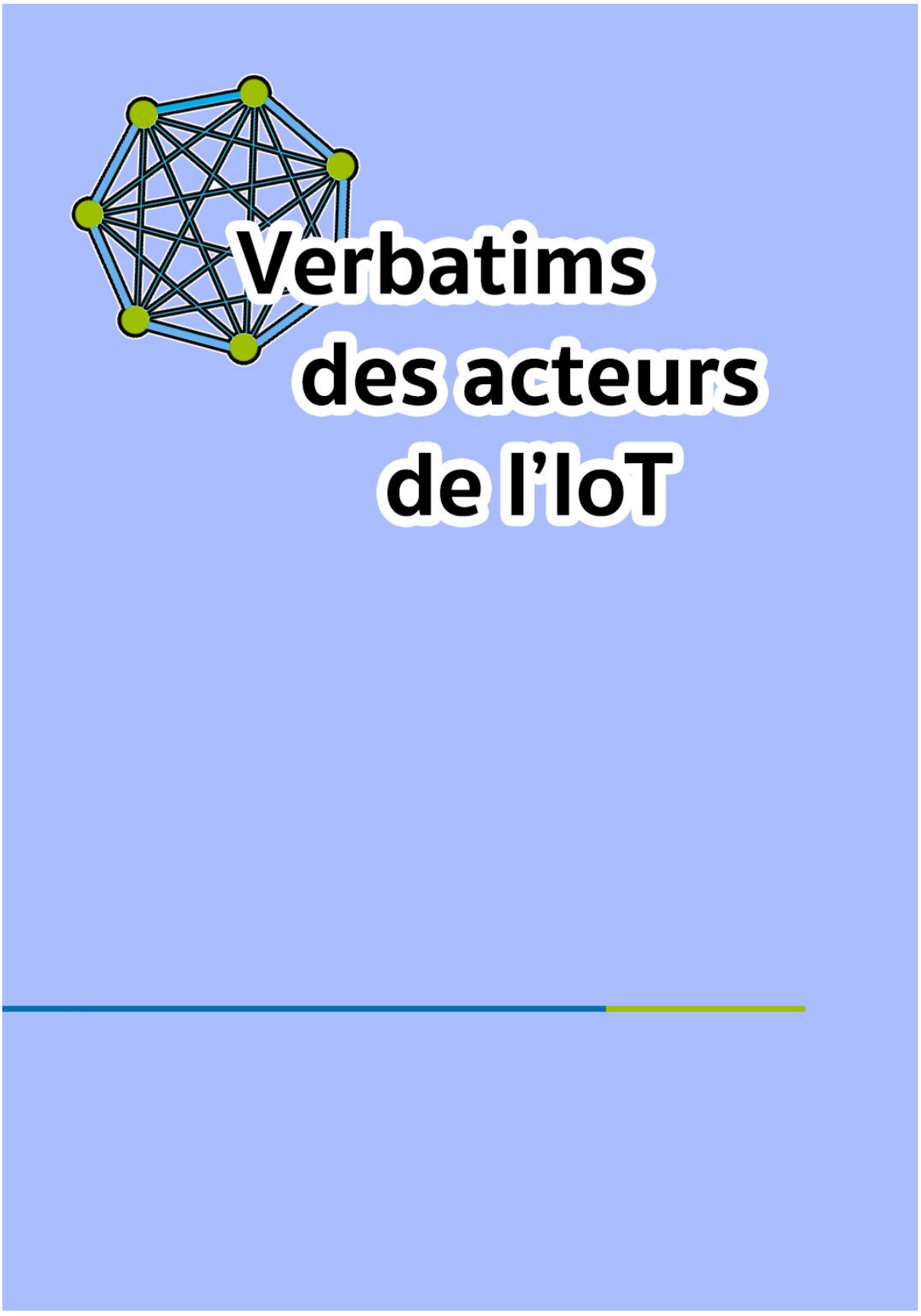


Illustration 6 : « Innovation et pessimisme » par Cyril Hlakkache - 2016



Emmanuel Ruiz, fondateur de **CopSonic** (Montauban, Occitanie) nous raconte :

"L'IoT aujourd'hui se confronte à 3 challenges majeurs lorsqu'il s'agit de l'IoT grand public:

1. ***La sécurité** (valable aussi pour l'Iot industriel),*
2. ***L'interopérabilité** (valable aussi pour l'Iot industriel),*
3. ***L'UX** (User eXperience).*

*Comme l'illustrait cet enfant de 11 ans (http://mashable.france24.com/) , l'IoT n'est pas sécurisé et les **ultrasons sont capables de s'hybrider avec le Bluetooth** pour rendre l'IoT plus sécure.*
Le canal audio dans l'IoT grand public commence à s'implanter de manière massive via Siri et autres Google assistant, lire l'article "Les ampoules connectées Ikea répondront bientôt à Siri et Google Assistant". Les senseurs utilisés pour interagir avec et entre des dispositifs existent déjà (speakers et microphones). Les ultrasons n'ont besoin que de cela pour fonctionner. Il n'y a pas besoin de s'appairer avec l'IoT grand public via les ultrasons donc l'UX sera plus fluide.
Aux USA un organisme privé cherche à fédérer les spécialistes d'ultrasons, car ils savent que ce canal sera utilisé dans un futur proche pour créer un standard et une norme de communication sans contact en champ proche.

*Allons-nous attendre à ce qu'on nous impose en Europe un nouveau standard de communication où bien allons-nous prendre les devants alors que **nous avons les compétences et l'expertise** en la matière ?"*

Emmanuel Mouton, CEO et Directeur Général de **Synox** (Montpellier, Occitanie) nous dit :

"Les projets d'objets connectés sont désormais passés dans une étape plus mature. Les industriels ont dépassé cette année le cap du Proof of Concept et entament leur transformation numérique grâce à l'IoT.

Pourtant de nombreux challenges sont encore à relever pour passer d'un modèle économique produit vers un modèle économique de service. Cette transformation requiert notamment d'acquérir de nouvelles compétences qu'ils n'ont pas encore forcément anticipé. Comment choisir les bons capteurs, comment gérer leur connectivité, où stocker la donnée et comment la valoriser auprès de leurs utilisateurs sont autant de questions à se poser pour industrialiser un service IoT.
A mon sens, les enjeux à venir vont principalement se porter sur les problématiques de sécurité et d'interopérabilité des systèmes pour que la confiance des utilisateurs et la valeur apportée à l'usage soient les clés de la réussite."

4. Les technologies

4.1. Architectures M2M / IoT

Une solution M2M est une chaîne intégrant différents systèmes techniques entre eux, depuis les équipements de terrain, jusqu'aux applications destinées aux utilisateurs métier. Sur le plan fonctionnel, les solutions M2M sont basées sur des architectures relativement génériques et reproductibles.

Dès 2010, un travail de standardisation et de définition des architectures M2M a été développé par l'**ETSI**[14]. Un des objectifs de cette organisation est de permettre le développement de l'Internet des objets via les principes d'interopérabilité et d'intégration horizontale. En 2012, l'ETSI a créé, avec d'autres organisations de normalisation régionales nord-américaines, japonaises, chinoises et coréennes, l'initiative "**OneM2M**" qui a pour objectif d'établir une norme mondiale pour les solutions M2M. D'autres activités de normalisation de ces architectures de l'IoT ont également vu le jour au niveau mondial à l'**ISO**[15] au sein de son "Joint Technical Committee 1", dédié aux technologies de l'information en général, ou encore au niveau européen dans l'**AIOTI**[16], mais tous ces travaux convergent finalement vers le même modèle d'architecture.

Le diagramme ci-dessous présente une vue synthétique et simplifiée de l'architecture M2M initialement définie par l'ETSI :

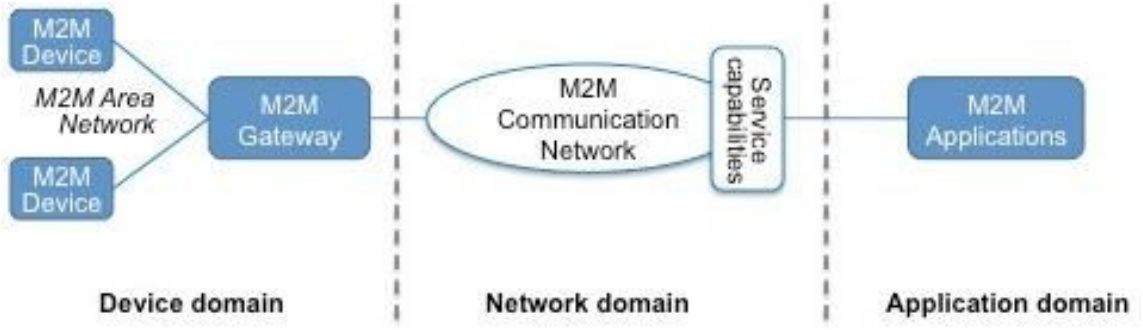


Illustration 7 : Modèle d'architecture M2M de l'ETSI
Source : Fusion Labs

[14] **ETSI (European Telecommunication Standardization Institute) :** Organisme de normalisation européen du domaine des télécommunications.
[15] **ISO (International Standardization Organization)** : Organisation Internationale de Normalisation, composée des différentes organisations nationales de normalisation de chaque pays comme l'AFNOR en France.
[16] **AIOTI (Alliance for Internet Of Things Innovation)** : Organisation européenne de promotion et de développement de l'Internet des objets pour un écosystème (entreprises, universités et citoyens) européen fort dans le domaine.

Les principaux composants de l'architecture sont brièvement présentés dans les paragraphes qui suivent.

4.1.1. Les objets ou équipements (devices)

Le but d'une solution M2M est de connecter des équipements de terrain au réseau, afin de transmettre des données et/ou de recevoir des commandes. Ces équipements peuvent être des capteurs effectuant des mesures (énergie, température, humidité ou présence), des contrôles binaires (contacteur porte et fenêtre), des actionneurs (ouverture de porte automatique ou démarrage d'appareil électrique) ou encore des systèmes plus évolués, tels que des automates programmables pilotant des machines. Ces équipements disposent le plus souvent de logiciel embarqué permettant de réaliser des traitements en local avant de transmettre les informations préalablement préparées.

Certaines sociétés spécialisées réalisent des **objets sur-mesure** plus complexes qui agrègent de nombreuses fonctionnalités via un ensemble de capteurs, de l'intelligence embarquée et des boîtiers adaptés à des contextes très spécifiques comme celui de l'industrie, de la marine ou encore de la santé. C'est le cas par exemple de la société d'électronique française **Eolane** ou encore du distributeur d'électronique **Snootlab** qui proposent leur expertise pour le développement d'objets particuliers.

4.1.2. Passerelle (gateway) ou modem

L'interconnexion des équipements au réseau Internet est mise en œuvre par des interfaces entre les équipements et une passerelle de communication (ou modem). Lorsque plusieurs équipements utilisent la même passerelle, il peut être nécessaire de mettre en place un concentrateur établissant une interface avec chacun des équipements et cette passerelle.
Certaines passerelles évoluées intègrent des interfaces multiples et des fonctions de concentrateur, par exemple via la gestion d'un réseau local (Ethernet, wifi, Zigbee, Z-Wave, BLE, etc.). À noter que cette passerelle n'est pas nécessairement un équipement distinct à proprement parler, mais peut être embarquée sur un équipement.

4.1.3. Réseau de communication

Dans les solutions M2M, les échanges de données entre la passerelle et le système central passent généralement par le réseau cellulaire (GPRS, EDGE, 3G ou 4G) d'un opérateur mobile. Certaines solutions peuvent utiliser un canal de communication filaire. Par exemple en domotique, la liaison primaire à Internet utilise le boîtier Internet de la maison

(ADSL, SDSL, câble ou fibre). Le réseau cellulaire peut alors constituer une liaison de secours en cas de rupture de la liaison primaire afin d'assurer une continuité de service.

4.1.4. Infrastructure de services

L'infrastructure de services fournit des fonctionnalités utiles pour le développement d'applications métier au travers d'interfaces de programmation (API). Elle va assurer la liaison entre les objets et les applications qui les pilotent. Elle est souvent basée sur une architecture de type "Cloud", permettant la montée en puissance requise à l'évolution du nombre d'objets à gérer.

De plus, les acteurs majeurs du "Cloud" (Amazon Web Services, Microsoft Azure, Orange Datavenue, ...) proposent des plates-formes destinées l'IoT à travers des solutions spécialisées (PaaS[17]). Elles vont également souvent gérer des problématiques "Big Data" de par la quantité de données à traiter et à archiver dans un contexte temps-réel.

Ce composant d'architecture peut être mis à disposition par un fournisseur (éditeur ou prestataire de services hébergés) ou bien il peut être implémenté de manière spécifique pour répondre directement aux besoins de l'application métier.

L'infrastructure est le principal poste, avec la connectivité, qui va générer des coûts récurrents inévitables à intégrer dans le calcul du ROI.

Illustration 8 : Panorama du marché des plateformes IoT (non exhaustif), Source : Fusion Labs

[17] **PaaS (Platform as a Service) :** plateforme cloud mettant à disposition un environnement d'exécution rapidement disponible et opéré avec un niveau de service défini.

4.1.5. Application métier

L'application métier met en œuvre les fonctionnalités utiles aux utilisateurs finaux. Il peut s'agir d'utilisateurs professionnels (superviseur de systèmes distants, e-santé, ville intelligente ...) ou grand public (domotique, activités sportives, loisirs, etc.). Elle peut être développée dans une multitude de langages de développement, qui sera choisi en fonction de l'environnement cible (ordinateur, mobile, tablette, montre connectée...), mais doit nécessairement pouvoir accéder aux données recueillies par l'infrastructure de services (API webservices).

On distinguera en général au moins deux applications : celle du fabricant pour gérer et superviser son parc d'objets, et celle de l'utilisateur, dévolue à la gestion de son ou ses objet(s) spécifique(s) et à recueillir le service. Pour certains usages, des déclinaisons "mobiles" (Androïd, iOS) seront à prévoir.

Selon les fonctionnalités proposées par l'objet, la complexité des applications peut être très variable. Plus le traitement logique à appliquer aux données recueillies est complexe, plus l'application le sera elle aussi.

Dans le cadre d'une solution IoT déployée en production, l'application est l'élément de la chaîne le plus simple à faire évoluer dans le temps puisqu'elle peut potentiellement être mise à jour.

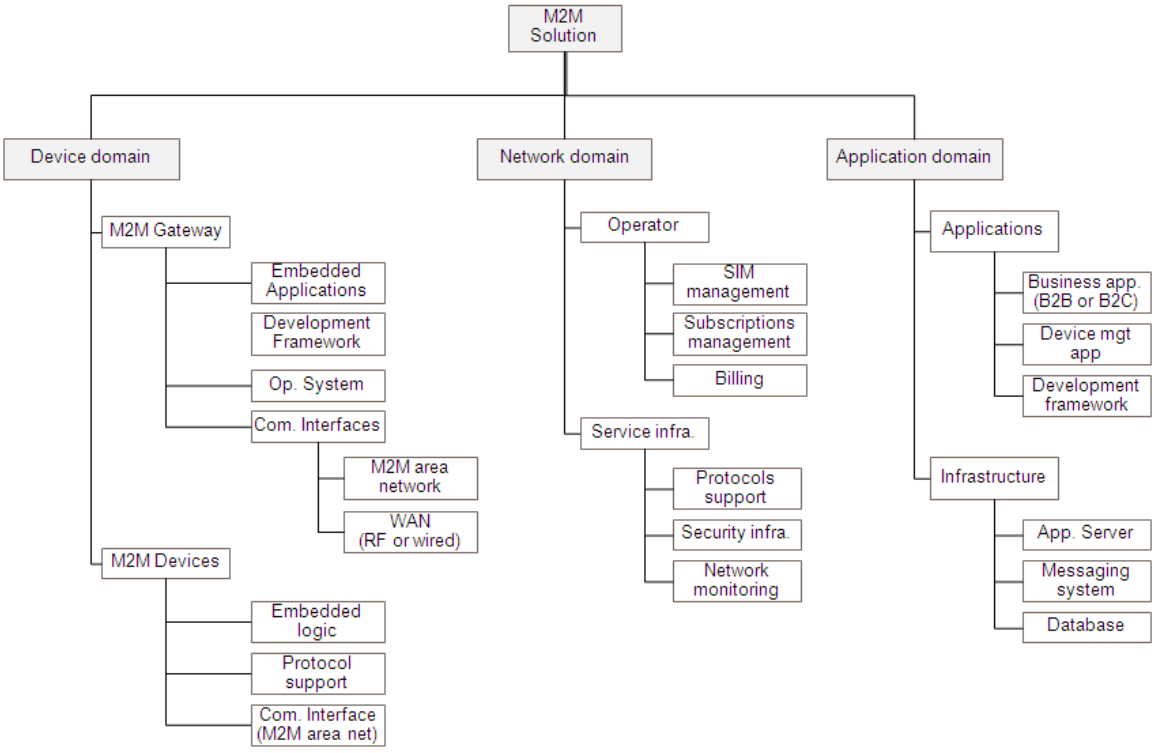


Illustration 9 : Organigramme des composants techniques des solutions M2M, Source : Fusion Labs

4.2. Les technologies

4.2.1. La connectivité WAN

Différentes solutions sont disponibles pour connecter les objets de terrain avec le réseau global, en particulier :

- **Les liaisons filaires :** Principalement via la technologie Ethernet ou fibre, connectés à un équipement de type routeur. Ce cas d'application est limité aux systèmes fixes, déployés par exemple dans des bâtiments d'entreprises, des infrastructures publiques ou des maisons connectées.
- **Les réseaux cellulaires traditionnels :** GPRS, Edge, 3G ou 4G (LTE), y compris les réseaux cellulaires LPWA[18] (Low Power Wide Area) : EC-GSM-IoT (2G), LTE-M[19] (4G LTE[20] catégorie M1), et NB-IoT [21](4G LTE catégorie NB1).
- **Les réseaux radio basse consommation dédiés :** LP-WAN (Low Power WAN), bas débit : les technologies SigFox, LoRa et RPMA-Ingenu (aux Etats-Unis) sont les trois implémentations principales à ce jour. On peut également citer Weightless ainsi que Qowisio sur ce créneau.
- **Les réseaux par satellite :** Permettant la connectivité dans les zones non couvertes par les réseaux terrestres (ceux-ci ne couvrant que 5% du globe).
- **Les approches hybrides :** Combinaison de plusieurs des solutions listées plus haut, avec sélection du support selon le contexte et les conditions de fonctionnement du système connecté.
- **Les approches « futuristes » :**
    - Le projet "Loon", partenariat entre Google et le CNES pour déployer des ballons stratosphériques offrant des services de télécommunication.
    - Le projet "OneWeb" consistant à proposer une constellation de satellites permettant un maillage global pour proposer une connectivité sur l'ensemble du globe.
    - Les projets de drones télécoms comme Facebook avec leur projet "**Aquila**" ou encore le projet équivalent de Google nommé **Titan Aerospace** (abandonné début 2017) ou Airbus avec leur drone stratosphérique HAPS (High Altitude Pseudo-Satellite) **Zéphyr**.

Note : Les géants du numérique n'hésitent pas à désengager de manière brutale des projets montrant des faiblesses en termes de rentabilité, c'est le cas par exemple de la box domotique Revolv de Google en 2016. C'est pourquoi les GAFA se permettent de multiplier les projets innovants visant à tester les modèles puisque leur agilité leur permet de savoir

[18] **LPWA (Low Power Wide Area)** : Réseau sans fils basse consommation et longue portée, optimisé pour l'Internet des objets.
[19] **LTE-M (Long Term Evolution for Machines) :** évolution de la 4G adaptée aux usages IoT.
[20] **LTE (Long Term Evolution) :** Terme générique pour la 4G.
[21] **NB-IoT (Narrow Band for IoT) :** Standard développé par le 3GPP reposant sur une technologie radio à bande étroite, évolution de la 4G adaptée aux usages de l'IoT.

abandonner si ce qui ne fonctionne pas. Avant de choisir une solution, surtout relativement nouvelle, il conviendra donc de bien intégrer comme facteur de risque la possibilité que cette solution soit abandonnée par manque d'intérêt ou de rentabilité à moyen ou long terme.

Illustration 10 : Passerelle M2M GX450 (4G, Ethernet, Wifi),
Source : Sierra Wireless

4.2.2. La connectivité LAN

Pour différentes raisons, on choisira parfois de ne pas relier les équipements directement au réseau global, mais d'interconnecter un réseau local de capteurs ou d'actuateurs[22] à une passerelle de communication longue distance. Ce réseau pourra être de type étoile (la passerelle est reliée en direct à chaque équipement local) ou bien de type maillé (mesh), permettant parfois à ces réseaux "locaux" de s'étendre sur des distances notablement plus grandes qu'initialement prévu. Un cas d'usage typique de ces réseaux locaux est celui de la maison et du bâtiment connectés (smart building), mais des applications existent également dans l'industrie, la santé, la ville intelligente, etc.

Les technologies et protocoles radios fréquemment utilisés à courte portée sont les suivantes :

- **Wifi** :
  - Caractéristiques techniques : IEEE 802.11a/b/g/n/ac, Fréquence : de 2,4 GHz à 6 GHz, portée : 300 m.
  - Description : Technologie commune, mais gourmande en consommation énergétique.
  - Particularités : Dédiés aux objets alimentés sur le secteur (en raison de la consommation énergétique élevée du wifi).

- **Wifi Halow** :

[22] **Actuateur :** Dispositif permettant d'actionner ou de piloter un système en lui transmettant une commande. Par exemple : démarrage de moteur, régulation de débit (eau, gaz), gestion du chauffage et de la climatisation, etc.

  - Caractéristiques techniques : IEEE 802.11ah, fréquence : 900 MHz, débit : de 150 kb/s à 18 Mb/s, portée : de 60 m. à 80 m.
  - Description : Validé par le consortium Wi-Fi Alliance en 2016. Il consomme moins d'énergie et traverse plus facilement les obstacles.

- **LiFi (Light Fidelity) ou VLC (Visible Light Communication)** :
  - Caractéristiques techniques : Fréquence : 670 THz à 480 THz. Portée : quelques dizaines de mètres.
  - Description : lumière visible comprise entre la couleur bleue et la couleur rouge diffusée par des LED en clignotement.
  - Particularités : Ne traverse pas les murs et n'émet pas d'ondes, elle n'est donc pas nocive pour les électrosensibles.
  - Effet indésirable possible : Malillumination.

- **BLE (Bluetooth Low Energy)[23] ou Bluetooth Smart** :
  - Caractéristiques techniques : Fréquence : 2,4 GHz, portée : quelques dizaines de mètres.
  - Description : Protocole radio basse consommation pour des profils d'utilisation multiples.

- **ANT** :
  - Caractéristiques techniques : Fréquence : 2,4 GHz, portée : quelques mètres.
  - Description : Protocole radio unidirectionnel pour capteurs notamment dans le domaine du sport (créé par une filiale de Garmin).

- **Z-Wave** :
  - Caractéristiques techniques : Fréquence : 868 MHz en Europe, 908 MHz aux États-Unis, portée : 50 m.
  - Description : Protocole radio basse consommation pour la maison connectée, soit la domotique.

- **ZigBee** :
  - Caractéristiques techniques : IEEE 802.15.4, portée : 100 m.
  - Description : Protocole radio basse consommation pour des profils d'utilisation multiples.

- **EnOcean** :
  - Caractéristiques techniques : Fréquence : 868 Mhz en Europe et 315 Mhz aux États-Unis, portée : 300 m.
  - Description : Solution propriétaire d'interrupteurs radio ultra basse consommation et surtout auto alimentés, comme par pression mécanique

[23] **BLE (Bluetooth Low Energy) :** Déposé sous le nom commercial de Bluetooth Smart, est une technique de transmission sans fil ouverte et qui complète le Bluetooth sans le remplacer, en proposant un débit identique au Bluetooth, mais avec une consommation d'énergie très inférieure, environ 10 fois moins.

(piézoélectrique) ou par énergie solaire. Cette technologie est utilisée pour la maison connectée, soit la domotique.

- **Ultrasons** :
  - Caractéristiques techniques : Fréquence : de 12 kHz à 1 MHz, portée : plusieurs dizaines de mètres.
  - Description : Communication par ultrasons, comme proposé par la société CopSonic : http://www.copsonic.com/
  - Particularités : ne traverse pas les murs, n'émet pas d'ondes électromagnétiques, elle n'est donc pas nocive pour les électrosensibles.
  - Effet indésirable possible : Peut entraîner une gêne lorsque l'ultrason est audible en dessous de 15 kHz, ou 20 kHz pour les plus jeunes. Surveiller la pression acoustique.

Notes :

- Le **WiGig** se présente comme le Wifi ultra rapide (802.11ad) normalisé par la **Wifi Alliance** permettant des débits jusqu'à 8 Gb/s.

- D'autres technologies contribuent à optimiser la connectivité et l'énergie en proposant des standards comme **6LoWPAN (IPv6 over Low Power Wireless Personal Area Network)** décrit par l'**IETF**[24] dans la RFC 4919. Ce standard définit les mécanismes d'encapsulation et de compression d'en-têtes permettant aux paquets IPv6 d'être envoyés ou reçus via le protocole de communication IEEE 802.15.4, permettant ainsi de rendre compatible le protocole avec l'environnement spécifique de l'IoT demandant une réduction de la consommation d'énergie et disposant d'une connectivité réduite.

On notera également qu'au-delà de ces technologies radio courte portée, d'autres technologies filaires, souvent développées pour des usages particuliers, sont également utilisées en réseau local relié via une passerelle au réseau longue distance. On citera par exemple des technologies comme **OPC**, **ModBus** ou **Profibus** dans le domaine du contrôle industriel, ou encore la technologie **CAN**[23], bien établie dans le monde industriel également, mais aussi dans le secteur automobile et celui de l'aéronautique. **KNX** ou **Konnex** sont des technologies de communication utilisées dans le domaine de la gestion de bâtiments (y compris la domotique). Enfin, on citera également les standards **PLC**[25] (courants porteur en ligne) utilisés notamment par le désormais célèbre compteur électrique intelligent Linky.

[24] **IETF (The Internet Engineering Task Force) :** organisme de normalisation international dédié à l'élaboration des standards Internet.
[25] **PLC (Power Line Communications) ou CPL (Courant Porteur en Ligne) :** Standard permettant de construire un réseau informatique sur le réseau électrique d'une habitation ou d'un bureau, voire d'un quartier ou groupe de bureaux.

4.2.3. Compatibilité des équipements et standardisation

Cette longue liste de technologies de communication amène un constat : se retrouver dans ce labyrinthe est un véritable casse-tête, c'est pourquoi il faut soit savoir bien identifier ses besoins pour sélectionner la ou les technologies adaptées, soit faire appel à des experts capables de sélectionner et assembler ces technologies pour répondre au mieux aux besoins.

En parallèle, la standardisation des technologies promet de simplifier cet environnement, car elle permet de consolider toutes ces options autour de quelques unes seulement. En cela, elle est un facteur déterminant pour le développement d'un marché de services et de produits technologiques. L'établissement et l'adoption de standards et de normes (ces dernières bénéficiant par rapport aux premiers d'un caractère plus officiel, étant liées à une décision politique et/ou juridique) largement partagés permet alors une mutualisation des technologies, une baisse des coûts par des économies d'échelle, et une sécurisation des investissements par l'assurance que les technologies utilisées sont à la fois éprouvées, stables et pertinentes pour l'objectif visé.

Le processus d'établissement et d'adoption de ces standards et normes, toutefois, prend du temps justement parce que, sur ce chemin, les différents acteurs cherchent, testent et éprouvent différentes options. Dans ce jeu de l'innovation, les plus actifs travaillent pour établir ces standards à la fois sur la base de leur pertinence technologique et économique, mais aussi parfois par d'autres moyens, y compris légaux, politiques, publicitaires, économiques... Ce n'est qu'au bout de ce processus de consolidation qu'il est possible de constater la stabilisation du paysage normatif autour d'un (cassettes VHS, norme DVD, protocole IP, etc.) ou plusieurs standards (réseaux cellulaires GSM et CDMA[19], réseaux électriques 110V-60Hz et 230V-50Hz, etc.) qui constitueront la base technologique du marché considéré.

Le marché de l'IoT est particulier au sens où il est à la convergence de différents mondes qui se rencontrent dans l'IoT : réseaux de télécommunications, informatique d'entreprise, informatique embarquée, mais aussi les différents secteurs de l'industrie qui deviennent "connectés" : automobile, banque, énergie, santé... Autant de raisons qui expliquent le caractère aujourd'hui encore très fragmenté du paysage normatif du marché de l'IoT. Il faut peut-être se rendre à l'évidence : cette consolidation semble décidément bien compliquée, ce qui s'explique sûrement par le caractère hautement concurrentiel de ce marché, sans compter que les différentes technologies ont souvent de bonnes raisons de coexister sans converger, que ce soit pour des questions d'adoption dans certaines industries ou tout simplement parce qu'elles répondent à différents besoins.

En la matière, la seule norme de communication qui semble vraiment faire consensus est le protocole IP et sa technique d'adressage, les adresses IP (IPv4 ou IPv6, plus durables dans le temps). Sur cette base, certains standards de l'internet, définis comme IP par l'**Internet**

Engineering Task Force (IETF) dans ses RFCs[26], sont réutilisés dans ce nouvel internet des objets. Il en est ainsi des protocoles TCP, UDP, SNMP, TLS, mais aussi de nouveaux standards plus dédiés à ce domaine comme CoAP[27] ou DTLS[28],. On voit de même des travaux à l'IETF pour utiliser les réseaux dédiés LPWAN comme LoRa et Sigfox avec ce protocole IP. Un autre acteur très connu de cet univers de l'internet est le **World Wide Web Consortium** (W3C), qui a défini les formats de données HTML et XML et s'intéresse maintenant au Web of Things. Le **consortium OASIS** peut également être cité dans cette catégorie, avec des protocoles de communication comme **MQTT[29]** ou **AMQP[30]** qui trouvent une application dans l'IoT.

Cela dit, malgré ces efforts de standardisation, il faut bien constater que ce processus reste très incomplet, et que la multiplication des protocoles de communication pose un problème de compatibilité entre équipements. Citons par exemple l'apparition de nouveaux protocoles tels que le BLE, le NFC ou le LiFi : ils ne sont pas immédiatement supportés par le parc d'équipements qui se renouvelle seulement au bout de plusieurs années. Le taux de compatibilité du parc ciblé est donc un facteur essentiel à considérer, car il conditionne le succès du déploiement d'une technologie.

Dans le cadre d'une entreprise, lorsque celle-ci gère le parc d'équipements de ses employés, il est possible d'associer le déploiement d'un nouveau service à une rénovation de l'ensemble des équipements mobiles des collaborateurs.

Dans le cadre des politiques BYOD[31], les solutions ne peuvent pas être basées sur une seule technologie, mais sur l'intégration de plusieurs standards afin de tendre vers une compatibilité totale avec l'ensemble du parc utilisateurs. C'est par exemple le cas de l'ultrason qui dispose d'un taux de compatibilité proche de 100% et qui pourra alors compléter un protocole comme le BLE ou le NFC disposant d'un taux de couverture plus faible, actuellement en dessous de 25% de l'ensemble des équipements en circulation dans le monde.

Enfin, au-delà des simples problèmes de compatibilité de technologies de communications "physiques", il reste aussi à donner du sens à ces données de façons communes : quel format pour ces données, quelle(s) unité(s), quel(s) référentiels ? On parle là de modèles de données, et les applications coexistant dans ces systèmes doivent se mettre d'accord sur

[26] **RFC (Requests For Comments) :** Série numérotée de documents officiels publiés par l'IETF décrivant les normes élaborées par l'IETF pour Internet.
[27] **CoAP (Constrained Application Protocol) :** Protocole de communication inspiré du protocole connu HTTP, mais destiné aux petites machines disposant de peu de ressources de calcul, et fonctionnant sur la base du protocole UDP au lieu de TCP (pour HTTP).
[28] **DTLS (Datagram Transport Layer Security) :** Protocole fournissant une sécurisation des échanges basée sur des protocoles en mode datagramme comme l'UDP.
[29] **MQTT (MQ Telemetry Transport) :** Protocole de messagerie publish-subscribe basé sur le protocole TCP/IP.
[30] **AMQP (pour Advanced Message Queuing Protocol) :** Protocole ouvert pour les systèmes de messagerie standardisant les échanges entre serveurs de messages.
[31] **BYOD (Bring Your Own Device) :** Pratique qui consiste à utiliser ses équipements numériques personnels, comme le Smartphone, l'ordinateur portable ou la tablette, dans un contexte professionnel.

les modèles de données supposés par ces applications. Ces modèles de données peuvent être définis par certains constructeurs, ou par certaines alliances industrielles comme on l'a vu dans le domaine de la télérelève de compteurs électriques avec la **norme COSEM** (référencée sous le code IEC 62056), qui permet aux compteurs électriques de toutes marques de communiquer leurs données de mesure électriques au même format.

4.2.4. Une réponse multi-technologique

La nature même du marché du digital implique que la réponse technique se plie au besoin des métiers et des utilisateurs et non l'inverse. Les cas d'usage conditionnent le choix des technologies et demanderont parfois de mixer les technologies pour répondre au besoin.

Ainsi, la solution proposée par un intégrateur IoT fera parfois appel à plusieurs briques technologiques pour répondre aux différents besoins de connectivité, c'est tout l'enjeu d'un intégrateur digital. Par exemple, pour répondre à un besoin spécifique, il peut être nécessaire d'implémenter une combinaison de Wifi, de LiFi, de LoRa et d'ultrasons, pour tirer parti de chacune de ces technologies.

Bien évidemment, apporter une solution multi-technologies augmente la complexité quant à la gestion de la sécurité de la solution et de sa maintenance.

4.2.5. Plates-formes de services M2M/IoT

L'utilisation de plates-formes de services IoT, également appelées middleware, facilite et accélère significativement la mise en œuvre et l'intégration de solutions.

Les principales fonctions de ces plates-formes sont les suivantes :

- **La gestion de flotte d'équipements ou d'objets**, appelée "Device Management", permettant :
    - Le provisioning : Approvisionnement, installation et configuration des objets,
    - La supervision du parc d'objets et de la connectivité,
    - Les mises à jour logicielles (software et firmware).
- **La gestion des messages et des données**, permettant :
    - La gestion des échanges entre les objets et le serveur :
        - Collecte des données émanant des objets (flux remontant),
        - Transmission de commandes du serveur vers les objets (flux descendant).
    - Le stockage et l'historisation des données,
    - Les notifications d'alertes,
    - La gestion des utilisateurs, des groupes et des droits d'accès.
- **L'implémentation et l'intégration des applications métier** :
    - La configuration et la gestion des règles et des scénarios métiers permettant de générer des actions spécifiques en fonction des données collectées,

    - Les outils,
    - Les API coté serveur, comme coté objet, via la mise à disposition d'agents embarqués,
    - Les applications, souvent développées en mode agile, faisant généralement appel à des SDK[32] mis à disposition par le constructeur d'une plateforme donnée ou d'une technologie donnée.

De nombreuses solutions sont aujourd'hui disponibles sur le marché, en particulier :

- **Les plates-formes des fournisseurs de matériel communicant** : Sierra Wireless, Telit, Digi, ...
- **Les plates-formes des opérateurs télécoms** : Orange (LiveObject), Deutsche Telecom, ...
- **Les plates-formes d'éditeurs ou de sociétés de services** : PTC/ThingWorx, Capgemni-Sogeti, ...
- **Les plates-formes des fournisseurs d'infrastructure Cloud** : Microsoft Azure, AWS, OVH, ...
- **Les plates-formes Open Source** : DeviceHive, OpenIoT, Fiware (Smartcity), ThingSpeak, Nimbits, Kaa, ...

À ce niveau de la couche de services, comme on l'avait vu au niveau des technologies de communications, on constate que des travaux sont en cours pour définir des standards de services, afin de faciliter la communication entre ces différentes plateformes, ainsi qu'avec différents équipements de terrain.

Ainsi, l'organisation **oneM2M** développe un standard pour une couche de services communs de l'IoT au-dessus de la couche de stricte communication. De même, l'**Open Mobile Alliance**, un groupe originellement attaché à la gestion et la configuration à distance des téléphones portables, développe aujourd'hui des standards spécifiques pour les services de l'IoT comme le standard **LightweightM2M** (abrégé en LWM2M). Il est à noter que ces deux standards, oneM2M et LightweightM2M, sont prévus pour être compatibles entre eux, le premier ayant un périmètre plus étendu que le second, et le second ayant l'avantage de la simplicité.

[32] **SDK (Software Development Kit) :** Kit de développement informatique proposant un ensemble d'outils permettant de faciliter le développement d'un logiciel sur une plateforme donnée.

4.3. La gestion de l'énergie des objets connectés

4.3.1. Usages

Le marché des objets connectés se développe à partir d'usages très variés, dont une part de plus en plus importante concerne des dispositifs autonomes et sans-fil : les capteurs pour la maison connectée, les objets portables (wearable technology), les balises de géolocalisation, les capteurs environnementaux, les systèmes embarqués non intrusifs, etc. Ces équipements disposent de leur propre source d'alimentation (batteries rechargeables ou piles) et communiquent par des protocoles radios optimisant la consommation énergétique.

Le principe général est de permettre à l'équipement de fonctionner « en veille » la plupart du temps et de réveiller ses fonctions consommatrices uniquement lorsque l'usage prévu le nécessite, par exemple : la transmission de données à fréquence régulière ou l'envoi d'une alerte sur un événement critique. Les contraintes d'usage peuvent nécessiter de concevoir des systèmes à même d'être opérationnels pendant une ou plusieurs années, sans remplacement ou recharge de batterie.

4.3.2. Technologies

Les solutions permettant de répondre à ces enjeux impliquent d'avoir une approche globale lors de la conception du système, en partant de l'analyse précise des usages, des fonctionnalités requises et des différents organes techniques mis en œuvre. Des simulations, puis des tests de consommation d'énergie, sont effectués sur des prototypes pour valider ou ajuster la conception. Les axes d'optimisation les plus courants impliquent en particulier :

- De maximiser la réserve énergétique embarquée (la batterie), dans la limite des contraintes physiques,
- De limiter les phases de fonctionnement les plus consommatrices (optimisation des scénarios opérationnels et de l'algorithmique embarqué),
- De réduire la consommation lors des communications sur le réseau local ou distant.

La frugalité énergétique et l'impact environnemental sont des thèmes fortement liés à l'IOT. Cela représente un gisement d'innovations : comme par exemple les technologies de "**energy harvesting**[33]", ou l'émergence du "low tech".

[33] processus par lequel de l'énergie est tirée de sources externes (solaire, éolienne, thermique, vibratoire, cinétique, chimique, etc.) en quantités infinitésimales, puis emmagasinée pour servir au fonctionnement autonome d'appareils portables de petite taille.

De manière générale, le service le plus consommateur en énergie est la transmission de données. C'est pourquoi, dans certains cas, les objets connectés ont tout intérêt à pouvoir réaliser des opérations de traitements en local afin de réduire le volume à transmettre et d'optimiser ainsi les communications. Les objets connectés ne sont pas toujours de simples capteurs et ils ont vocation à embarquer une certaine intelligence afin d'assurer une gestion optimisée de leur autonomie.

Le troisième point a donné lieu à de nombreuses solutions techniques basées sur des protocoles de communication sans-fil à faible consommation. Ces protocoles permettent, soit des communications longue distance « Low Power Wide Area Network » (LPWAN), soit des communications locales avec une passerelle établissant la connectivité au réseau global, comme expliqué plus haut dans la section 4.2.

4.4. Le hardware, les systèmes embarqués - le choix des composants électroniques

Les fabricants de hardware et de semi-conducteur sont au cœur du déploiement de l'Internet Des Objets. Un objet connecté est typiquement composé d'une ou de plusieurs cartes électroniques (PCB Printed Circuit Board) sur lesquelles sont montées des composants incluant:

- Un circuit de connectivité
- Un microprocesseur pour effectuer des calculs
- Des capteurs pour digitaliser les informations tels que les vibrations, température,
- accélération, pression, position…
- Des batteries couplés ou non à des circuits de régulations

Ces fonctions peuvent aussi être combinées dans un composant, les fonctions de connectivités et de calculs peuvent par exemple être intégrées dans un produit de type ASSP (Application Specific Standard Product). Le nombre de combinaison étant potentiellement infinie, la difficulté pour les fabricants de semi-conducteurs consiste à apporter des solutions couvrant un très large éventail technologique et à apporter des offres pertinentes pour le marché très fragmenté de l'Internet Des Objets.

Il existe en effet aujourd'hui une grande diversité de technologie RF pour connecter des objets. Certaines sont établies telles que le WIFI, le BLE, les modules M2M (3G ou 4G), Zigbee et d'autres sont en cours de déploiement (Sigfox, LoRa, Thread, NB-IoT).

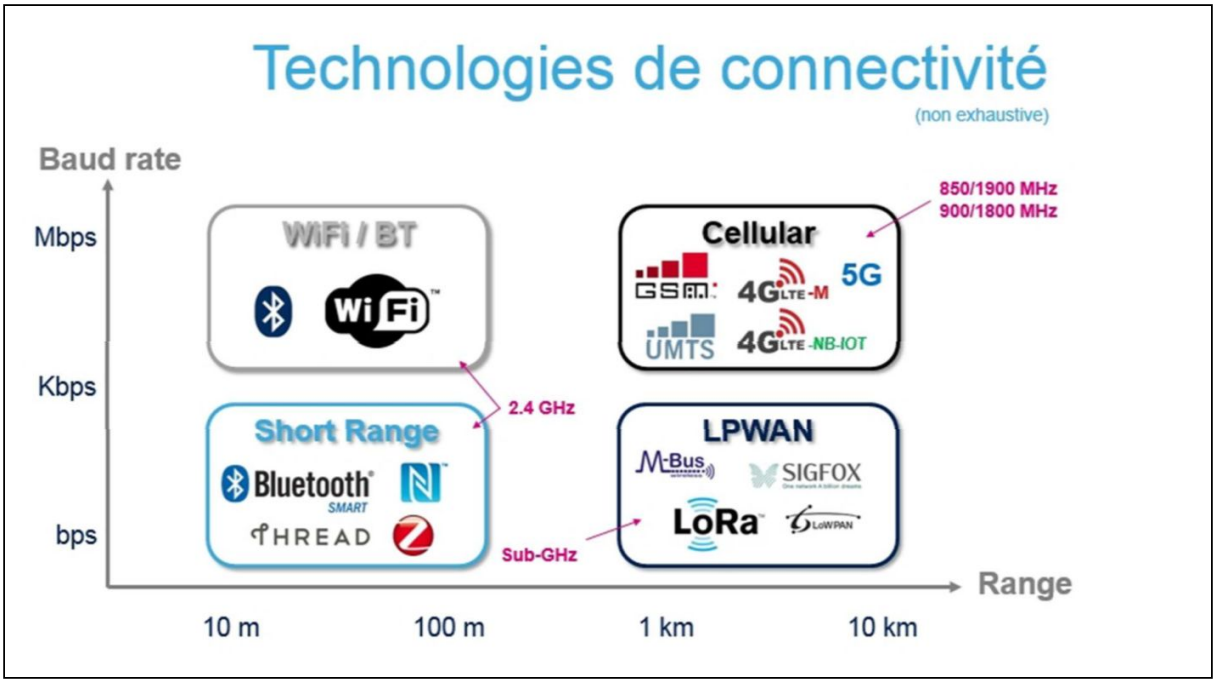


Illustration 11 : Technologies de connectivité,
Source : ST Microelectronics

Afin de déterminer la bonne stratégie d'investissement, chaque constructeur de hardware cherche à savoir quelle technologie dominera le monde de l'IoT. Une approche typique pour comprendre ou s'oriente le marché consiste à segmenter le marché et à analyser les grandes tendances par segment.

Dans le la maison connectée (domotique), on a déjà assisté à un déploiement important d'objets basés sur des technologies WIFI ou Bluetooth, profitant des réseaux centrés sur la box internet familiale, ou sur le téléphone portable. Cependant, afin de palier à certaines limitations du WIFI ou du BLE en terme de portée ou de consommation, on assiste à une hybridation de ces technologies avec d'autres déjà existantes tels que des réseaux Sub-GHz (déjà utilisés dans les commandes de portails, volets roulants, alarmes...). Les bandes Sub-GHz (433/868 MHZ pour l'Europe) sont libres d'utilisation, d'une technologie simple et peu coûteuse, facile à mettre en œuvre. En revanche, il n'existe pas de protocole mondial dominant. Les acteurs bien implantés dans la maison connectée déploient leur propre protocole ou s'associent avec d'autres fabricants dans des initiatives plus larges.

Dans un segment de marché de la logistique (« asset tracking »), la couverture mondiale ou régionale d'un réseau couplé à une fonction GPS ou de localisation via le réseau, permettent d'obtenir de bons résultats pour remonter des informations de positionnement, de température, d'humidité, mesurer les chocs encaissés.... On assiste à de nombreux déploiements basés sur des réseaux cellulaires classiques à base de module Machine to machine (M2M) ou basés sur un réseau d'un nouveau genre, déployé par un opérateur qui ne vient pas la téléphonie mobile, Sigfox. Bien entendu, contrairement à l'utilisation d'une technologie WIFI ou BLE, le déploiement d'une flotte d'objets connectés dépendant d'un

opérateur réseau (Orange, Sigfox...) va nécessiter de mettre en place un contrat de service avec un ou plusieurs opérateurs.

Deux exemples de services logistiques IoT innovants visant des marchés différents et basés sur des approches de connectivité différentes ParcelLive by Hanhaa – UK et Livingpackets - France

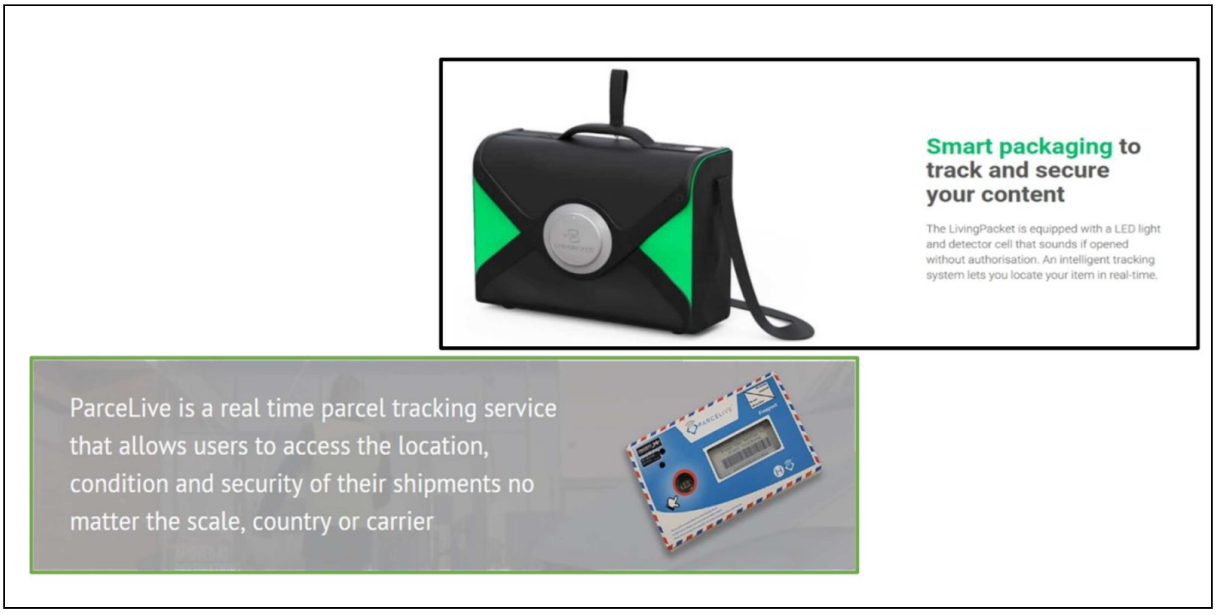


Illustration 12 : Tracker,
Source : ST Microelectronics

Le segment de la Smart City (ville intelligente) a pour sa part d'autres besoins. Un compteur d'eau doit embarquer une batterie la plus économique possible avec une durée de vie la plus longue possible afin de minimiser les coûts liés au service de maintenance (changement de batteries). L'objectif est en fait d'avoir une batterie d'une durée de vie équivalente à celle du compteur. Le besoin de bande passante est faible, quelques octets par jour sont suffisants. Des technologies telles que LoRa, Sigfox ou réseau Sub-GHz propriétaires apportent une réponse appropriée. Utiliser un réseau propriétaire va nécessiter de déployer sa propre infrastructure (Gateway, répéteurs, antennes). C'est envisageable pour couvrir des zones limitées et très denses (par exemple pour couvrir des zones urbaines, ou des zones hors réseau), mais pour couvrir des zones vastes à l'échelle d'un pays ou d'un continent, il faudra dépendre d'un réseau déjà établi. Les bandes ISM[34] Sub-GHz (Bande Industrielle Scientifique et Médicale) sont fragmentées et différentes d'un continent à l'autre. Un objet utilisant ces bandes devra donc s'adapter en fonction de la région dans laquelle il se situe. Il est à noter que le réseau Sigfox, une fois déployé au niveau mondial, permettra d'avoir un opérateur unique et disposera d'une solution relativement simple pour se connecter sur les différentes zones géographiques.

[34] **Bande ISM :** Bandes de fréquences qui peuvent être utilisées dans un espace réduit pour des usages industriels, scientifiques, médicales ou domestiques. Pour l'Union Européenne, le niveaux limites sont décrits dans la norme EN 55011.

Un exemple de déploiement d'infrastructure propriétaire dans le monde du Smart Lighting avec la solution de Telensa (Royaume-Uni)

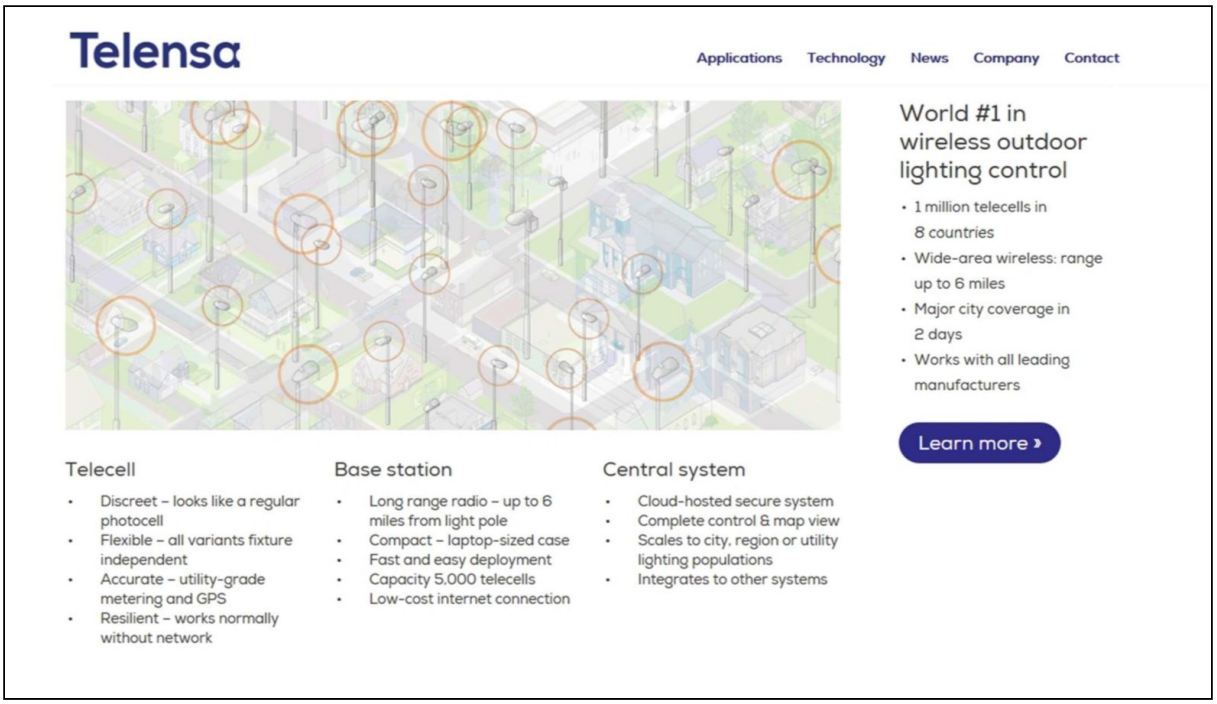


Illustration 13 : site web société Telensa,
Source : https://www.telensa.com/

Il apparait clairement de ce rapide tour d'horizon de quelques segments de l'IoT que la diversité technologique va perdurer. Toutes les technologies de connectivité répondent à des problématiques différentes. Le choix de la connectivité est un choix stratégique, il répond avant tout à des besoins applicatifs et de business model. Aucune technologie ne dominera entièrement le marché de l'Internet Des Objets, il faut se préparer à offrir des solutions extrêmement diversifiées.

Une fois le choix de la connectivité validé, les societé qui désirent déployer des objets connectés sont confrontés à des choix en termes de puissance de calcul dont doivent disposer les Objets connectés. La connectivité permet de remonter des informations vers des serveurs et de stocker des données dans le cloud. Mais quelles sont les données qui doivent être stockées et comment doit-on dimensionner la puissance de calcul disponible au niveau des capteurs, au niveau de la Gateway ou au niveau du cloud afin d'obtenir une architecture simple, efficace et évolutive? Encore une fois, il n'y a pas de solution unique. Un capteur de température connecté aura probablement besoin de peu de calcul local. Il suffira de remonter des informations de température d'une manière régulière et de visualiser à partir de données stockées sur un serveur ou dans le cloud. Cependant dans la plupart des applications la frontière entre processing local ou dans le cloud n'est pas aussi simple. Un véhicule autonome est composé de nombreux sous-systèmes eux-mêmes autonomes ou sous contrôle d'une puissance de calcul basée dans le véhicule. Il est bien évident que la détection d'un piéton, d'une ligne blanche, d'un feu de circulation ne peut pas se faire dans le cloud mais localement.

Le machine learning qui est un des domaines de l'**Intelligence Artificielle**[35] (souvent résumé en IA ou AI en anglais) est une technologie en plein développement et il existe de nombreuses initiatives pour être en capacité de porter des réseaux de neurones sur des serveurs, des microprocesseurs et même de simples microcontrôleurs. On parle de Edge AI et de cloud AI, le cloud AI utilisant la puissance de serveurs localisés dans le cloud, le Edge AI utilisant des puissances de calculs à la périphérie du cloud, c'est-à-dire soit sur une Gateway soit le microcontrôleur applicatif . L'Edge AI se déploie de plus en plus rapidement utilisant des données provenant de capteurs d'images, de microphones, ou même provenant de capteurs telles que vibrations, pressions, mouvements... Un microcontrôleur à bas coût basé sur un cœur Cortex-M est en capacité d'offrir des solutions de machine learning pour des capteurs de mouvements, de pression, de vibration. Les traitements sur image nécessitent des puissances de calcul bien plus importantes, qui vont nécessiter des microprocesseurs.

La société **@-Health** basée en France propose le service CardioNexion qui consiste en l'association d'un dispositif médical unique et connecté à un système d'évaluation en temps réel des risques de pathologies cardiovasculaires. La collection de données est faite aux moyens de capteurs embarqués dans des vêtements, des algorithmes de Deep Learning sont exécutés sur des serveurs

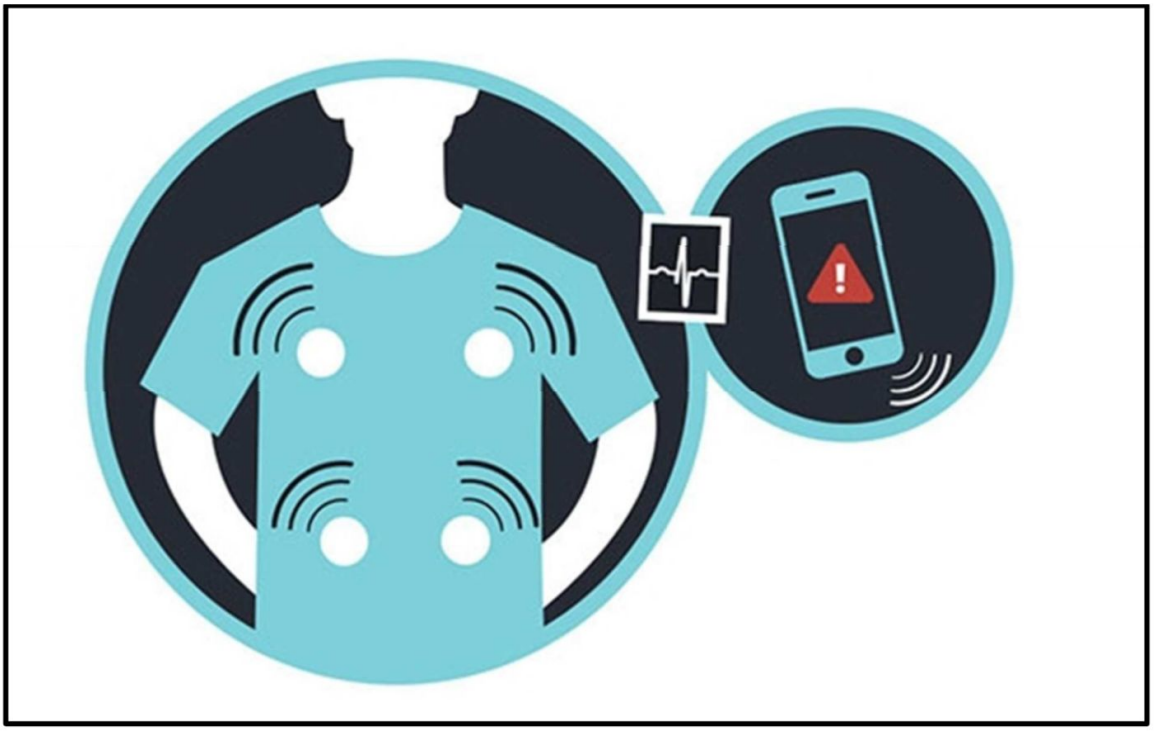


Illustration 14 : Société @-Health,
Source : http://www.healthcardionexion.com/

[35] **Intelligence artificielle** (**IA**) : « l'ensemble de théories et de techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence ».

L'IoT est une révolution qui impacte aussi les fabricants de hardware dans le cycle de développement des produits (combinaison hardware / Software). L'accès à distance au produit après son déploiement sur le terrain crée une zone de flou entre la conception et l'industrialisation du produit. En effet, la capacité de modifier le code applicatif qui tourne sur le microcontrôleur du produit permet à la fois d'améliorer le produit après son déploiement mais aussi d'offrir de nouveaux services. Ces capacités nouvelles s'accompagnent du besoin de définir une stratégie pour la gestion de la « flotte » produits, de sa sécurité afin de minimiser le risque de piratage et de sécuriser/authentifier les échanges de données et de la mise à jour du firmware. Il sera notamment important d'évaluer le type d'attaques potentielles (cyber ou physique) et s'assurer que le cout d'une attaque soit supérieur à la valeur des données récupérées par les hackers.

Face à ces nombreuses incertitudes et face et l'évolution rapide des technologies qui sont utilisées par les objets IoT, il est important pour les fabricants d'objets connectés de déployer une stratégie de développement produit qui permettent de ré utiliser l'investissement en Recherche et Développement. Il est essentiel de concevoir des produits modulaires, de définir des couches logicielles et des API (Application Programming Interface) de bien séparer la couche applicative de la couche de gestion des piles de communication, ce qui permettra de faire évoluer un produit rapidement pour supporter de nouveaux standards ou changer de protocole de communication. Pour la connectivité et dans la phase de prototypage, l'utilisation de module présente l'avantage d'être facilement intégrée dans un produit existant et de ne pas nécessité de nouvelles certifications.

Le module Murata CMWX1ZZABZ supporte les standards LoRa et Sigfox.

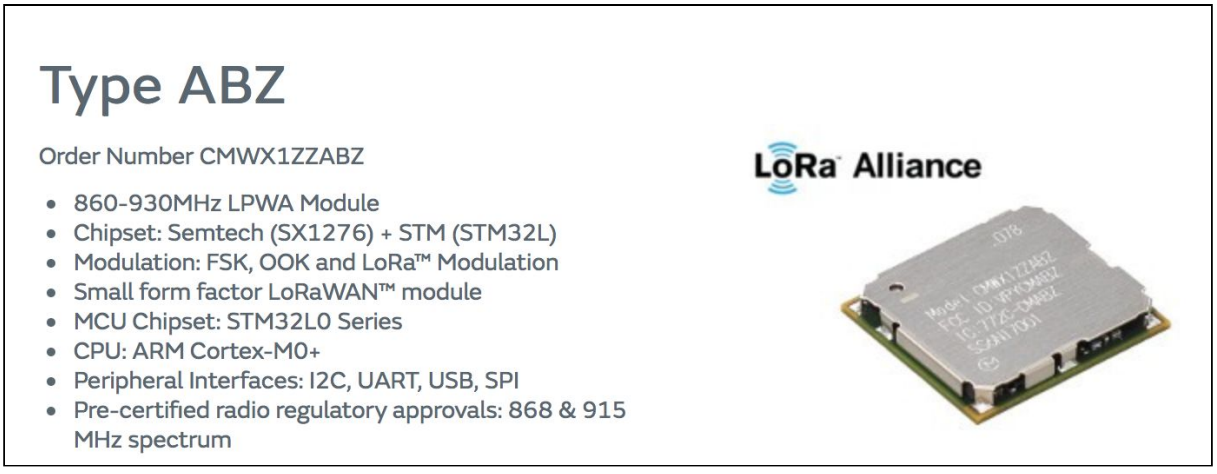


Illustration 15 : LPWA module type ABZ de Murata,
Source : https://wireless.murata.com/

Finalement, le plus important pour les fabricants de d'objets connectés est de bien s'assurer de la pérennité des composants avant de les sélectionner. Les fabricants de semi-conducteurs doivent justifier de volume important afin de pouvoir pérenniser la production de leurs composants et de garantir une productivité. Traditionnellement, il y a deux façons d'atteindre cet objectif pour un fabriquant de semi- conducteur.

- Travailler avec des leaders qui justifient de volumes très importants sur des produits dédiés ou ASSP (Application Spécifique).

- Travailler sur des composants génériques dont les spécificités couvrent de nombreux marchés, qui une fois les volumes cumulés offrent non seulement une grande stabilité de production une grande indépendance mais aussi.

Pour une application IoT, dont le développement, l'industrialisation et le déploiement vont prendre énormément de temps, il est important de sécuriser ces approvisionnements en choisissant des composants « Commercial Off The Shelf «, disponibles en ligne, chez de nombreux distributeurs, largement utilisés et dont on est sûr que les volumes ne sont pas dépendants de quelques gros donneurs d'ordre. Pour commencer un projet, il conviendra de regarder l'historique d'un composant, la durée de vie commerciale sur laquelle s'engage le fabricant et la disponibilité des composants sur les sites distribution en ligne comme Farnell, Digikey, Mouser et Radiospare qui sont spécialisés dans la distribution en ligne en faible volume sur de nombreuses références. ST par exemple s'engage à maintenir en production le STM32 pour une durée de 10 ans, engagement qui est renouvelé chaque année et cela depuis 10 ans déjà.

Mouser dispose de plus de 48 000 références de produits semi-conducteurs dans la catégorie « Embedded Processors & Controllers » dont les plus populaires sont commercialisés Microchip, STMicroelectronics, NXP, Texas Instrument et Cypress semiconductor

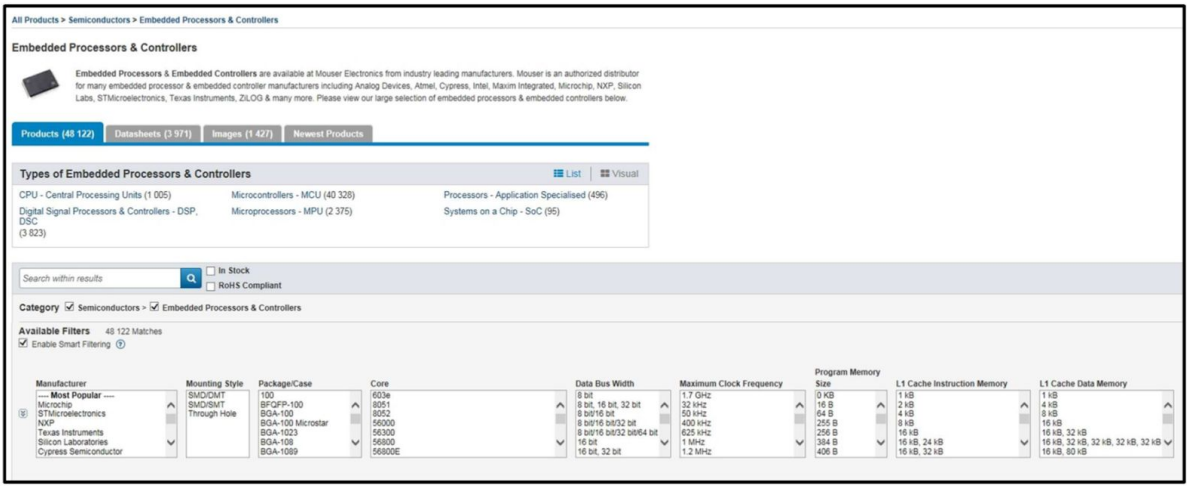


Illustration 16 : Embedded Processor and Controllers,
Source : ST Microelectronics

L'investissement dans le logiciel embarqué représente l'immense majorité des efforts à fournir sur un objet connecté et est très souvent sous-estimé. A titre d'exemple, une montre connectée représente en fonction de la complexité de la montre un investissement logiciel embarqué allant de quelques dizaines de « homme année » à quelques centaines de « homme année ». Dans ces conditions, le choix du processeur sur lequel repose l'investissement est fondamental. La société ARM (« Advanced Risc Micro »), basée à

Cambridge au Royaume Uni, propose depuis une dizaine d'années une offre de Cœur de microprocesseurs appelé Cortex-M et qui couvrent la plus grande partie des besoins applicatifs, depuis le marché du 8 bit jusqu'au marché des microcontrôleurs 32 bit les plus performants incluant des capacités de traitement du signal.

La famille de cœur ARM Cortex-M, inclue le cortex-M0/M0+, le Cortex-M3, le Cortex-M4 et le Cortex- M7 qui répondent à des segments de marchés différents

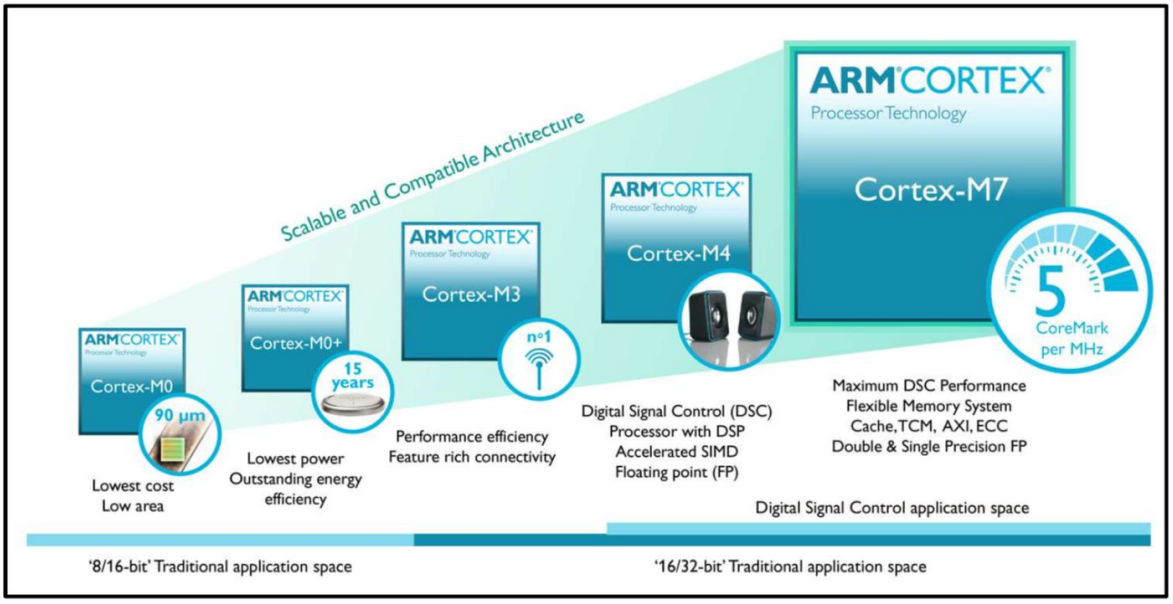


Illustration 17 : ARM Cortex-M Family 32-bit,
Source : https://www.arm.com/

STMicroelectronics a été le premier fabricant de semi-conducteur majeur à faire le choix d'utiliser les cœurs Cortex-M dans ses familles de produits microcontrôleurs. De nombreux fabricants ont depuis rejoint cette stratégie notamment NXP semiconductor, Silicon Labs, Renesas, Cypress ou encore Microchip via le rachat de la société Atmel.

Basé sur l'architecture ARM, de nombreux écosystèmes voient le jour, de nombreux projets sont en cours de déploiement, chaque écosystème ayant ses propres spécificités.

ARM propose la solution Mbed pour adresser le marché de l'IoT. Au niveau de l'embarqué, Arm Mbed électronique est basé sur une couche système d'exploitation appelé Mbed OS (OS comme operating system soit système d'exploitation) conçu pour l'internet Des Objets. 130 cartes électroniques sont certifiés Mbed, parmi lesquelles 42 de STMicroelectronics, 27 de NXP, 10 de Nordic Semiconductor, et 4 de Silicon labs....L'offre Mbed de ARM inclue donc un grand nombre de fabricants de microcontrôleurs.

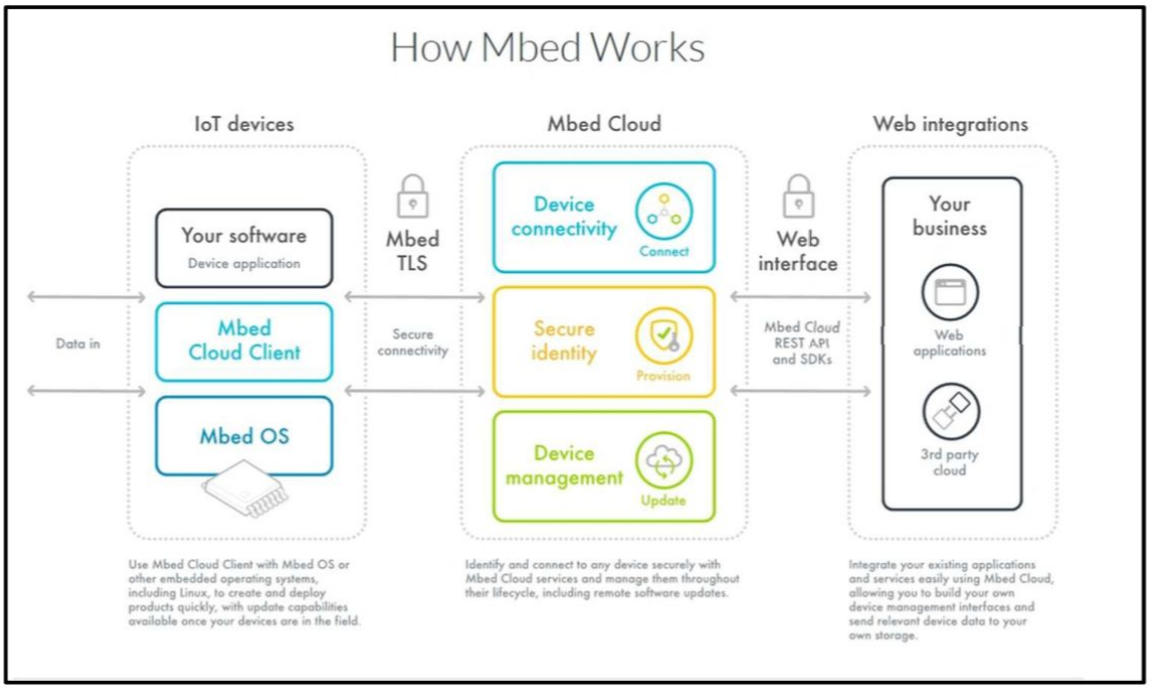


Illustration 18 : How Mbed Works,
Source : https://www.mbed.com/

Amazon Web Service qui est le leader incontesté des services de Cloud Computing propose des solutions basées sur son offre Amazon FreeRTOS. Amazon FreeRTOS est un système d'exploitation pour microcontrôleurs qui facilite la programmation, le déploiement, la gestion d'objets et d'établir une connexion sécurisée entre les objets et des services du cloud AWS. Les partenaires fournisseurs de matériels sont Microchip, NXP, STMicroelectronics et Texas Instrument.

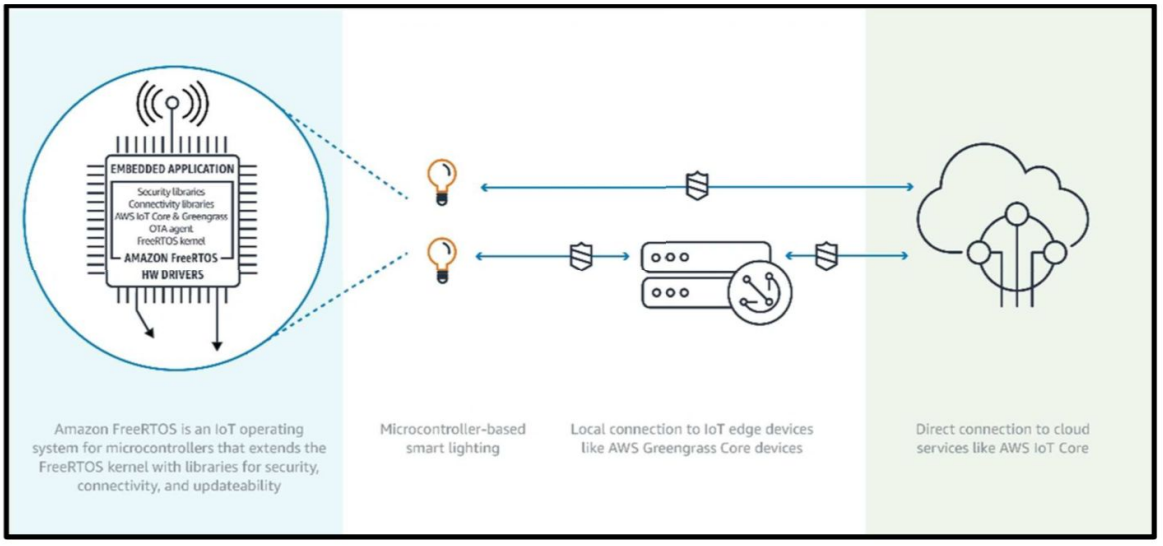


Illustration 19 : Amazon FreeRTOS,
Source : https://aws.amazon.com/

Finalement, STMicroelectronics propose un écosystème centré autours de l'environnement de développement STM32 CUBE. Le STM32 CUBE est une approche modulaire proposant de nombreuses façons de programmer le STM32, depuis des couches dédiés aux experts de l'embarqué jusqu'à des niveaux d'abstractions qui permettront aux débutants de facilement réaliser un projet, une Proof Of Concept. ST travaille avec de nombreux partenaires afin de mettre à la disposition des développeurs des solutions complètes visant à accélérer le time to market. Par exemple, ST propose des solutions complètes pour adresser les marchés LoRa, sigfox, M2M... Voici quelques exemples de solutions proposés aux développeurs pour adresser le monde de l'IoT et accélérer le "time to market" :

Les kits P-L496G-CELL01 and P-L496G-CELL02 sont des kits destinés à simplifier le développement d'objet IoT sur des réseaux 2G/3G et LTE. Les kits sont provisionnés avec une carte SIM Emnify, permettant une connexion au cloud en quelques clics dans 133 pays... Ces deux kits sont basés sur le microcontrôleur STM32L4 et des MODEMS Quectel.

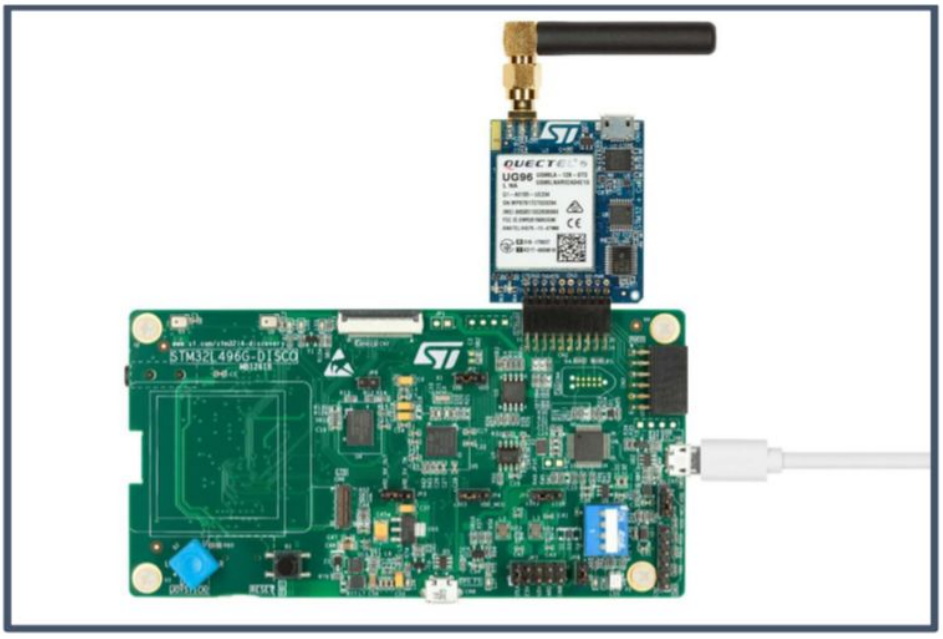


Illustration 20 : P-L496G-CELL01,
Source : ST Microelectronics

Le B-L072Z-LRWAN1 est un kit composé du module Murata CMWX1ZZABZ-091 qui permet de se connecter aussi bien aux réseaux LoRa et Sigfox. Le Module de Murata est composé du microcontrôleur STM32L0 et d'une radio Semtech.

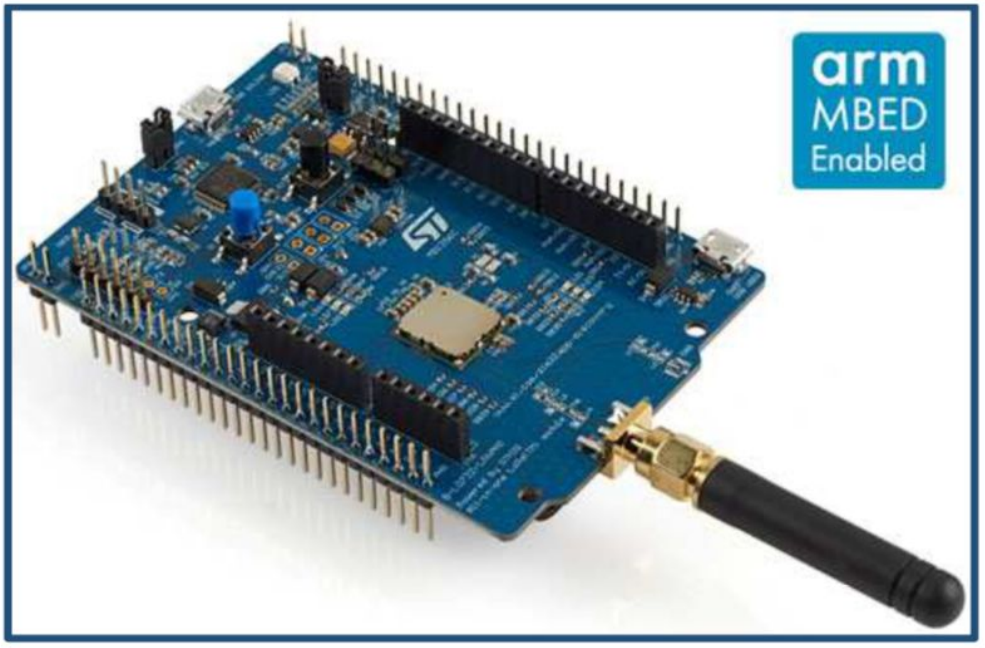


Illustration 21 : B-L072Z-LRWAN1,
Source : ST Microelectronics

Enfin le kit B-L475E-IOT01A est un kit qui fournit un connectivité WIFI pour lequel ST fournit des « connecteurs » aux clouds de de partenaires tels que Amazon AWS, Microsoft Azure , IBM Watson.

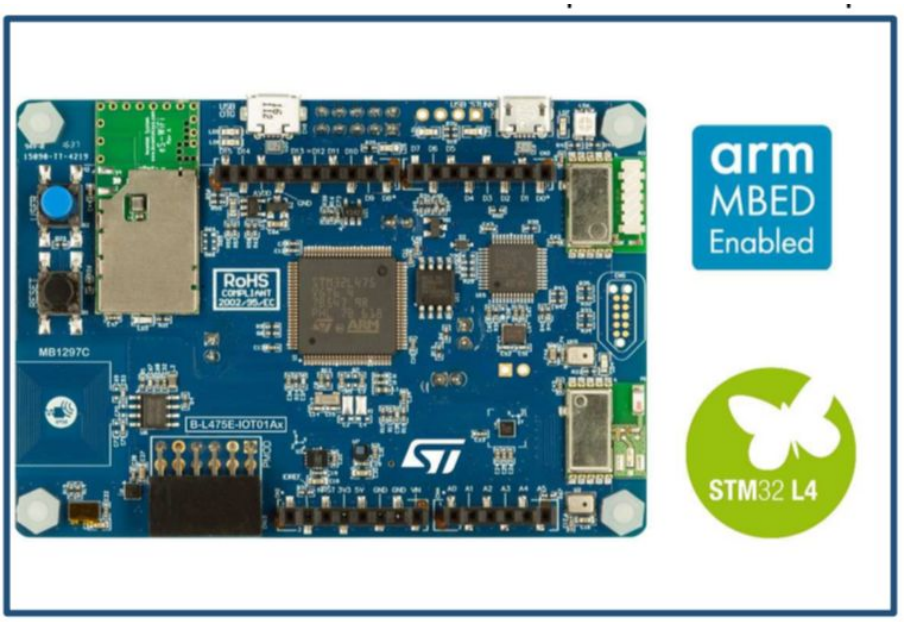


Illustration 22 : B-L475E-IOT01A,
Source : ST Microelectronics

En résumé, le choix des composants est un choix essentiel pour développer et commercialiser avec succès un objet connecté. Un objet connecté est avant tout composé de nombreuses lignes de code; la connectivité c'est en premier lieu du logiciel. Pour un

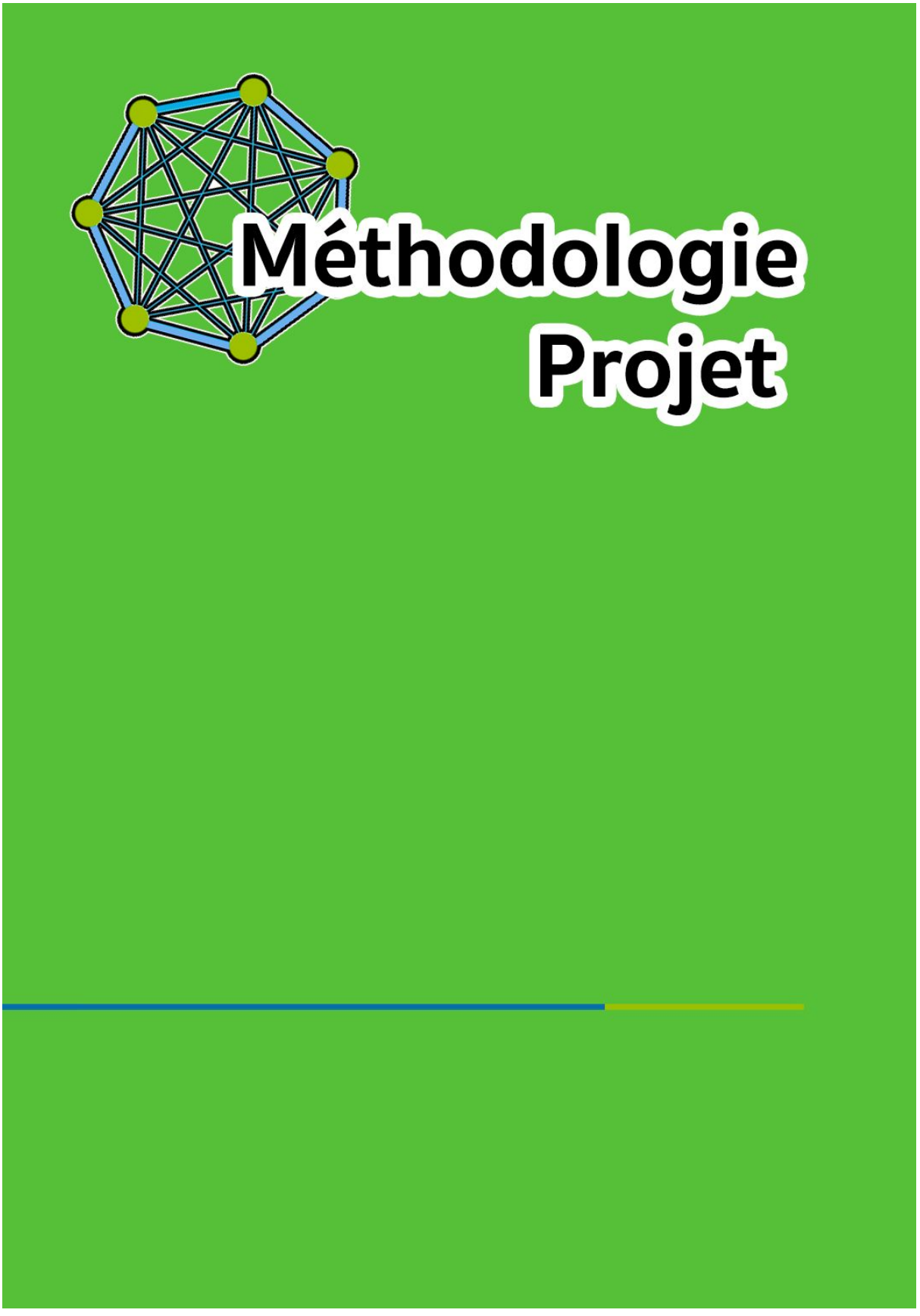
fabricant d'objets connectés, la plus grande valeur, la plus grande différenciation réside dans le logiciel. Avant de chercher à optimiser le matériel, il faut sélectionner des composants qui évoluent rapidement, qui bénéficient d'une roadmap (feuille de route) et d'un écosystème riche. La capacité de développer et d'adapter des produits rapidement est essentielle pour s'imposer sur le marché des objets connectés. Dans ce marché en plein développement, la vitesse d'exécution et de développement feront la différence.

4.4. Quelles perspectives sur le long terme ?

Après avoir assisté à une multiplication des tentatives, nous assisterons à une sélection naturelle autour de quelques normes qui auront fait leurs preuves par le terrain et qui auront su fédérer les énergies nécessaires pour être standardisées.

Il ne faut pas avoir peur d'investir aujourd'hui sous prétexte que les normes ne sont pas clairement établies et stabilisées, car l'Internet des objets relève avant tout des usages et moins des technologies à proprement parler, même si elles restent importantes.

Si pour répondre à un besoin, l'IoT semble être une solution pertinente, les investissements réalisés seront toujours valorisés à moyen et long terme. En effet, en cas d'évolution technique à intégrer, la maturité et les compétences développées sur ces projets donnera un temps d'avance et permettra d'aller plus vite.



5. Méthodologie projet

La compréhension des enjeux liés à l'IoT décrits dans les parties précédentes, détermine en grande partie le choix de l'approche méthodologique. L'IoT émerge dans un nouveau contexte :

- **Le choc des cultures** entre les parties prenantes (hardware vs digital), le temps des cycles de développement, ainsi que les contraintes logistiques et réglementaires.
- **L'émergence de nouveaux business models** face aux traditionnels, et la constitution d'écosystème. Effectivement, l'accélération de la mutation du contexte est favorisée par l'émergence de nouveaux acteurs comme les startups, les structures d'accueil, d'incubation et d'accélération ou encore les programmes de transformation digitale des entreprises obligées d'évoluer en rupture du fait d'un marché en attente d'agilité et de fluidité. De cet écosystème émane une logique d'**Open innovation** où les grands groupes acceptent par exemple de partager ces problèmes auprès de PME ou startups (plus libres pour pivoter) capables de proposer des solutions innovantes que l'on peut qualifier de disruptives permettant d'accéder à de nouveaux marchés de manière totalement différente.
- **La maturité et le renouvellement** des technologies, des niveaux de performances et des volumes de données.

Les questions auxquelles nous allons tenter d'apporter des réponses dans cette partie sont : *Quels sont les niveaux de l'organisation qui sont impactés par l'IoT ? Comment engager une transition vers ces technologies IoT ? Quelles sont les dimensions d'un projet IoT ? Et comment se construit une solution IoT ?*

5.1. Stratégique d'entreprise : à quoi peut ressembler la feuille de route de transformation digitale de votre entreprise ?

La **stratégie digitale** (incluant les technologies IoT) de votre entreprise doit fournir une vision, des objectifs et des principes directeurs. Elle peut décrire la façon dont les alliances et les écosystèmes de partenaires stratégiques devront être développés. Enfin, la stratégie digitale pilote la gestion du portefeuille d'opportunités, ainsi que la planification de la gestion budgétaire et la feuille de route.

Idéalement, l'entreprise implémente un traitement "en entonnoir" des opportunités : Détection, évaluation et enfin lancement. Concernant plus précisément les projets IoT, elle peut mettre en place un "**centre d'excellence IoT**" qui apportera des compétences de conseil et de gestion du changement spécifiquement lié au domaine et pourra aussi réaliser un **audit de maturité IoT** qui aidera une organisation donnée à mieux comprendre où elle se trouve en matière d'adoption de cette technologie.

Pour les très grandes entreprises (plus de 1000 salariés), il est particulièrement intéressant de déployer une **plateforme IoT partagée en interne** ouverte à toutes les équipes des différentes directions. Cette plateforme pourra alors être mutualisée et utilisée par l'ensemble des projets afin d'accompagner l'innovation, mais aussi favoriser l'émulation et la collaboration entre les différentes entités pour la création de nouvelles solutions. Cette plateforme partagée (Back-end, front-end, connexion avec le système d'information d'entreprise et possibilité d'interrogation et d'exposition d'API) est particulièrement stratégique dans un grand groupe afin d'éviter la multiplication des coûts engendrés par la réplication de telles plateformes, permet de mieux gérer les risques au niveau de la qualité et de la sécurité des données, mais aussi et surtout, cela présente l'avantage de disposer d'une vision globale sur les projets IoT menés au sein de l'entreprise et de proposer d'éventuelles synergies afin d'accélérer et même d'aller plus loin.

Concernant les données, il est stratégique d'aborder les projets de transformation digitale du point de vue de la donnée, car c'est un point clé dans un modèle de type "Data Driven", soit des **modèles pilotés par les données**. Certains s'accordent à dire que la donnée est le nouveau pétrole, alors il est devenu essentiel de proposer une nouvelle organisation autours de ces données afin d'en assurer l'intégrité, la qualité et aussi la sécurité. Et tous les projets IoT sont d'importantes sources de données. Envisager la création d'un "Data Lake" partagé, tant que possible, permet justement de participer à la maîtrise de la localisation des données, de leur protection, de leur unicité en évitant les duplications, mais aussi de contribuer à leur utilisation pour justement les valoriser. De plus, le fait d'organiser l'ensemble des projets de transformation digitale autour de ces mêmes données permet de fédérer les initiatives, pour ensuite accélérer par l'interconnexion des services développés, pour mettre en place de nouveaux modèles d'un niveau plus global où les données sont transitives d'un service à l'autre.

Le schéma suivant illustre les différentes composantes d'une exécution de la stratégie :

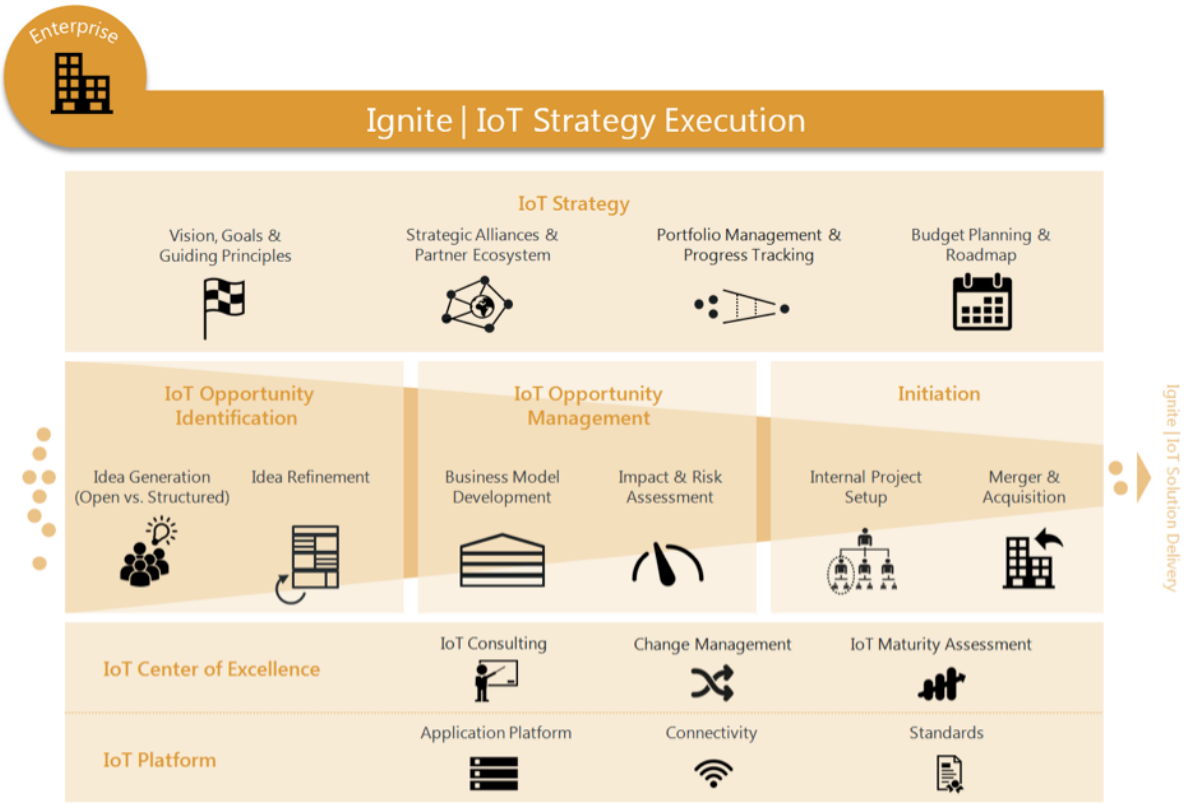


Illustration 23 : Ignite IoT Strategy Execution Methodology,
Source : www.enterprise-iot.org

Déployer chacun des dispositifs évoqués ci-dessus n'est absolument pas un passage obligé. Cependant, il ne faut pas sous-estimer l'importance de mettre d'accord toutes les parties prenantes sur une stratégie commune. Ainsi, savoir communiquer efficacement votre stratégie est un prérequis important pour atteindre vos objectifs.

Il est évident que les grandes entreprises, dont l'activité est essentiellement technologique comme Orange, Symantec ou encore IBM, peuvent éprouver des difficultés à viser un alignement global des projets, du simple fait d'un nombre d'acteurs trop important, éparpillés au quatre coins du monde, mais aussi, car les initiatives sont très nombreuses. Dans le cadre d'un tel contexte, la stratégie globale doit être apportée par une personne coté Comité Exécutif, par exemple le CDO (Chief Digital Officer), afin de donner la légitimité aux différentes divisions de décliner, et c'est alors au sein de ces Directions que cette rationalisation pourra se décider en fonction de la compatibilité entre les différents projets. Bien sur, le Comité Exécutif peut décider de financer le déploiement de cette fameuse plateforme transverse mutualisée pour favoriser l'émergence d'initiatives IoT. Le plus important dans un grand groupe reste principalement la définition du cap et de la stratégie globale d'innovation et de transformation numérique de l'entreprise. Une fois cette cible définie, les différentes divisions savent ensuite comment interpréter cela dans leur propre contexte afin de contribuer à l'atteinte de ces objectifs communs.

5.2. Au niveau opérationnel, à quoi peut ressembler une démarche projet IoT ?

De manière générale, Le cycle de vie générique d'un projet IoT s'articule finalement comme la plupart des projets en 3 phases : **l'étude** (Plan), **le déploiement** (Build) puis enfin **l'exploitation** (Run). Cependant, dans le détail d'un projet IoT, une de ses principales caractéristiques est de combiner plusieurs disciplines très différentes :

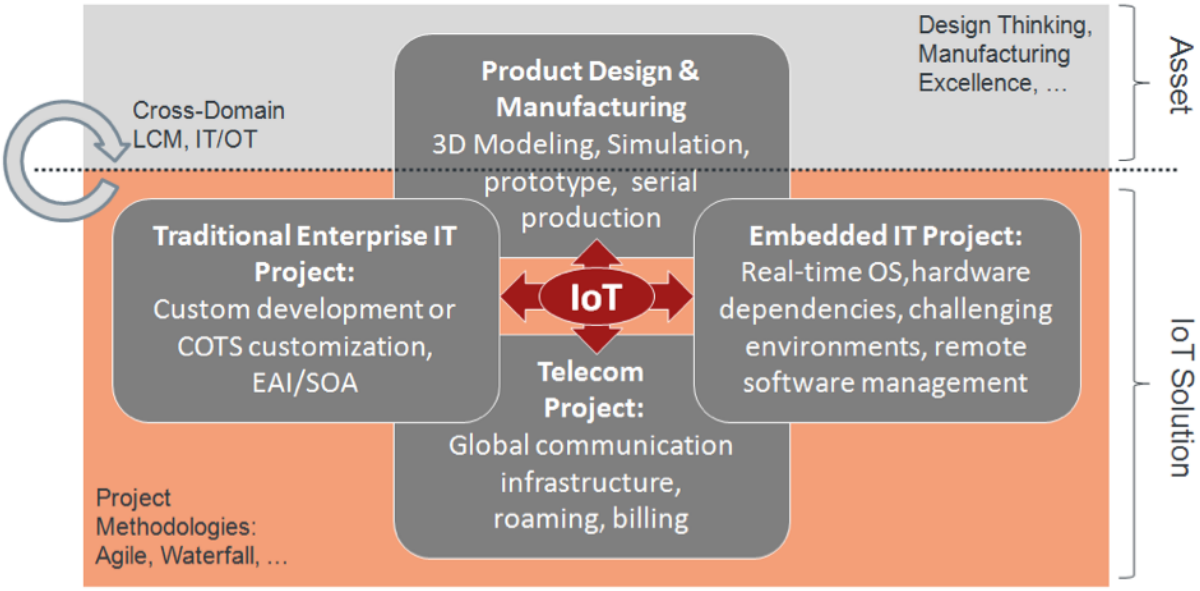


Illustration 24 : Multi dimensions of IoT project Management,
Source : www.enterprise-iot.org (CC BY 3.0)

Comme illustré ci-dessus, un seul projet IoT intègre :

- La conception du **produit** ou du **service**,
- Le conception des **objets matériel** (Hardware, boitier…)
- Le développement des **logiciels embarqués** (Software),
- La **connectivité** (réseaux et télécoms),
- Le **développement d'applications** d'entreprise et leur intégration,
- La **sécurité** inter-domaines.
- La définition et la mise en place du modèle de **support** et de **maintenance**

Sa structure s'organisera selon 7 groupes de travail, en charge de réaliser les livrables du projet :

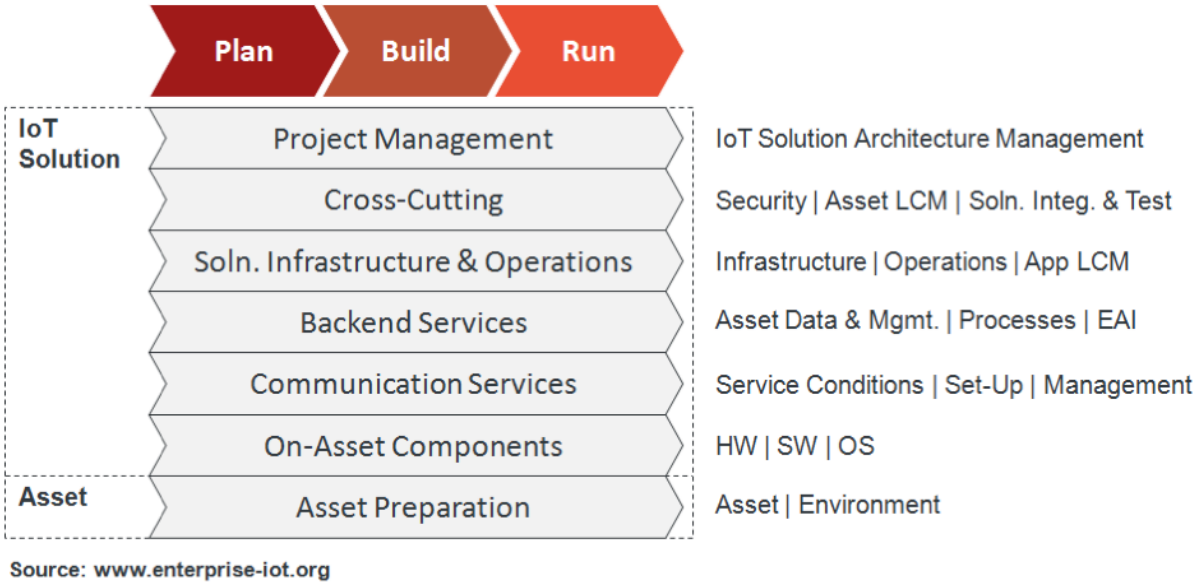


Illustration 25 : IoT Project workstreams,
Source : www.enterprise-iot.org (CC BY 3.0)

La phase de lancement donne lieu à une conception initiale, suivant 3 axes, décrits dans l'illustration suivante :

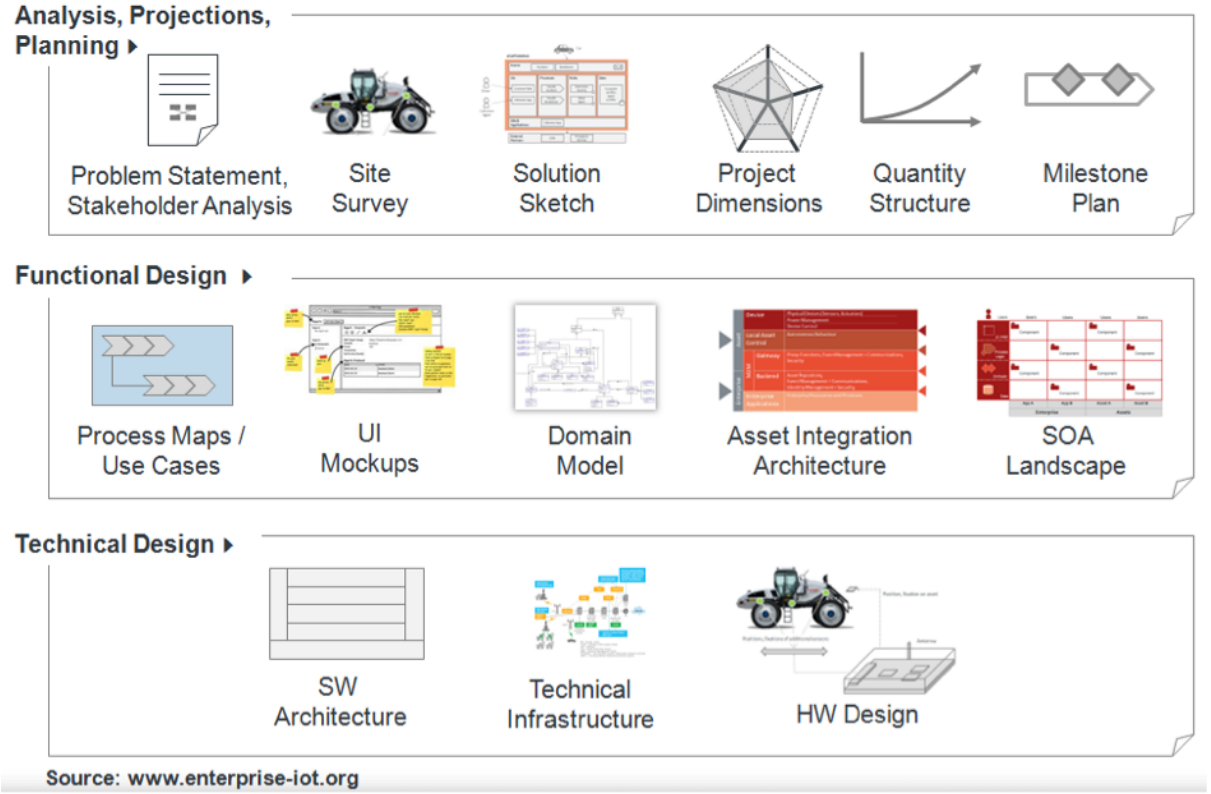


Illustration 26 : Ignite Initial Solution Design, Source : www.enterprise-iot.org (CC BY 3.0)

Le chef de projet se doit d'évaluer tous les aspects importants de la solution IoT à construire, le schéma de mesure présenté en *Figure 13* est un bon outil pour réaliser cette évaluation.

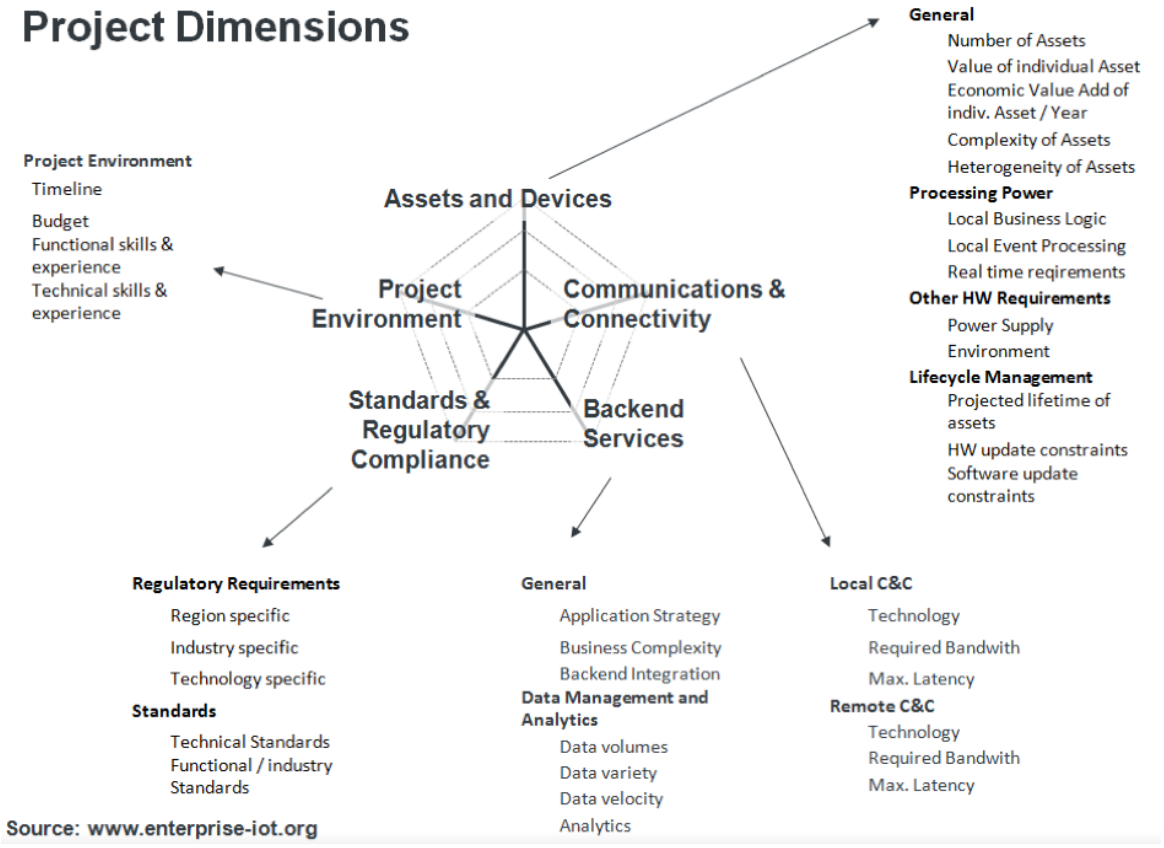


Illustration 27 : Mesure de dimensions projet,
Source : www.enterprise-iot.org (CC BY 3.0)

Les résultats de cette évaluation permettront d'identifier les zones critiques, les risques du projet et les entrées nécessaires aux décisions d'architecture et de conception.

5.3. Questions / Réponses

- ***Pourquoi passer par une étape de réalisation d'un démonstrateur ou d'un Proof of Concept ?*** Simplement pour convaincre votre client, en interne ou vis-à-vis d'investisseurs en illustrant concrètement un cas d'usage. Cela est particulièrement important dans la cadre des sujets innovants relevant du monde digital puisque la nouveauté des solutions demandent un important accompagnement des clients afin de rendre le sujet plus concret. En touchant du doigt les solution ils peuvent ensuite se projeter dans des usages métiers qui leur seront utiles. Cela est vrai pour l'IoT comme pour les technologies Big Data afin de sortir de la communication marketing et passer à des démonstrations terrains factuelles.

- ***Y'a t'il une différence entre la notion de démonstrateur et de Proof of Concept ?*** Pour certains les deux sont équivalents, mais pour d'autres, les démarches sont différentes puisque l'une précède souvent l'autre. Le démonstrateur se résume à un simulateur que l'on peut montrer à son client ou sa hiérarchie pour illustrer une technologie ou un service. Le Proof of Concept est la démarche suivante qui vise à décliner en pilote cette technologie ou ce service chez le client final dans un contexte réel, mais sur un périmètre réduit. Le démonstrateur est donc simplement une présentation concrète et démonstrative de la solution et n'engendre aucun coût pour le client alors qu'un Proof of Concept est souvent une démarche payante suivant les moyens nécessaires à engager. Étant donné que les intérêts entre client et fournisseurs sont mutuels alors les coûts sont parfois partagés et donc réduit par le fournisseur qui accepte fréquemment d'endosser la moitié des coûts engagés.

- ***Quel est le dimensionnement idéal d'un démonstrateur (Proof of Concept) ?*** Il est recommandé de choisir un nombre limité de fonctionnalités, de se baser sur un calendrier court entre 3 et 6 semaines et de se doter d'un budget 5 à 30 K€ suivant la complexité du démonstrateur et des compétences internes existantes. Cela à partir du moment où les composants utilisés pour ce test sont disponibles. Effectivement, le projet peut être totalement différent en terme d'investissements s'il s'agit de créer un nouveau type d'équipement (hardware, software et boitier). L'utilisation de matériels de prototypage bon marché, comme les cartes Arduino ou Raspberry Pi ou encore l'usage d'imprimantes 3D pour réaliser les boîtiers, représentent généralement une bonne approche afin d'éviter des délais et des investissements trop élevés de production d'un nouveau type de device uniquement pour un POC.

- ***Recommandez-vous l'adoption d'une nouvelle approche méthodologique (Agile[4]) ou plutôt une conservation des pratiques de l'organisation ?*** Dans un marché émergeant, difficile de savoir exactement quelles seront les attentes des futurs utilisateurs. Il convient donc d'appliquer une démarche "Lean Startup[36]" permettant de minimiser les risques et de rester en contact avec ses utilisateurs pour concevoir son produit de manière incrémentale avec des hypothèses validées. Il s'agira donc de développer le service par itération en entretenant un grande intimité avec la personne représentant le besoin, à savoir le product owner. En appliquant l'agilité aux développements matériels et logiciels, la logique est respectée et permet d'avoir rapidement un prototype, puis un service qui évoluera régulièrement. Attention, faire de l'agile ne signifie pas faire dans l'improvisation. Les étapes préalables d'expression du besoin, de spécifications techniques et fonctionnelles ainsi que le découpage en stories puis en tâche, sont inévitables pour convenir des objectifs du service. Ces étapes doivent être réalisées avec beaucoup d'attention et formalisées de manière à donner une base solide au projet qui pourra ensuite être

[36] **Lean Startup :** Approche spécifique de démarrage d'une activité visant à réduire les cycles de conception et commercialisation des produits, à mesurer régulièrement les progrès réalisés, et à obtenir des retours de la part des utilisateurs. Dans cette optique, les entreprises, en particulier les startups, cherchent à concevoir des produits et services qui rencontrent au mieux la demande de leurs clients, avec un investissement initial minimal.

réactualisé en fonction de l'évolution du projet au moment des revues de sprint et des livrables.

- ***À quoi ressemble la « dream team » pour conduire un projet IoT ?*** Cette équipe de rêve devrait être composée d'un chef de projet, d'un Business Analyst, d'un architecte solution, d'un Designer, de Développeurs et d'experts métier des domaines adressés. Il s'agit ici de fonctionner en équipe intégrée cross directions organisée autours d'un projet plutôt que des organisations d'entreprise. Mais ce sera avant tout la capacité à coopérer, à apprendre et à faire évoluer leur pratique individuellement comme collectivement qui fera toute la différence.

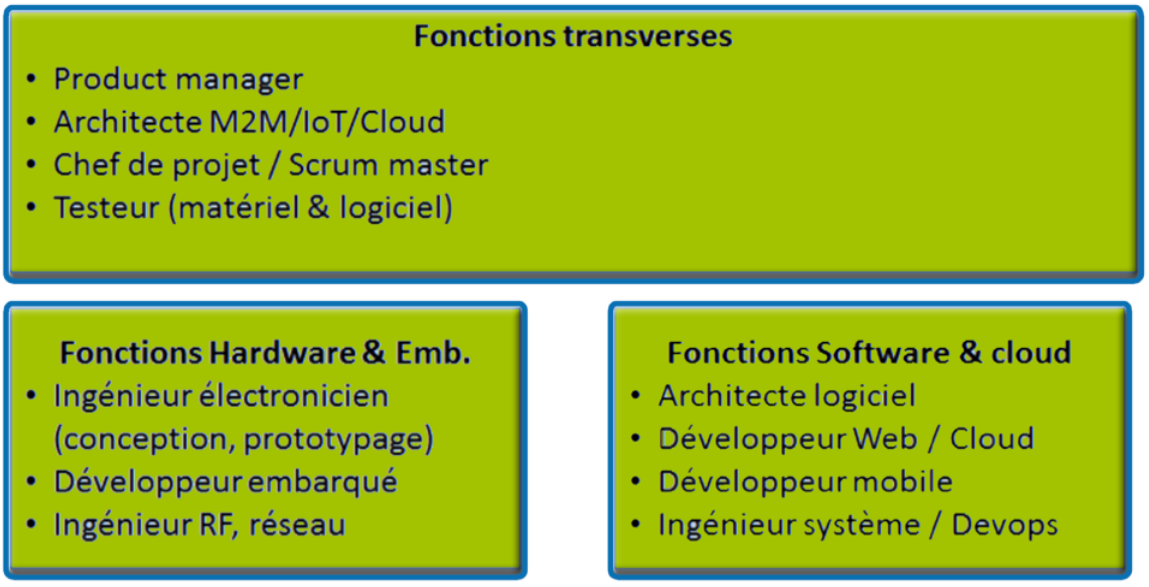


Illustration 28 : Panorama des compétences projet, Source : Fusion Labs

Par ailleurs d'autres fonctions classiques sont impliquées à différents stades du projet, en particulier : le marketing, la production en charge du déploiement, la logistique, les achats/sourcing ainsi que le SAV.

C'est ici que l'on peut voir intervenir les méthodes **DevOps**[37] visant à l'alignement de l'ensemble des équipes sur un objectif commun. Cette méthode est née de la volonté de diffuser et adopter les méthodes agiles. Elle vise principalement à aligner les équipes de développement avec les équipes de maintenance en charge de l'infrastructure, mais on peut étendre et transposer le concept plus globalement entre les équipes en charge de la construction d'une solution et celles qui vont ensuite la déployer puis l'opérer sur le terrain. Ce type de méthode est particulièrement bien adapté aux projets relevant de la transformation digitale tel que ceux de l'IoT qui intègrent de nombreux composants pour

[37] **DevOps :** Développeur opérationnel, ayant à la fois une vision sur la mise en œuvre de logiciels et sur leur déploiement et leur exploitation en production (infrastructure). Il a une vision globale et supprime les frictions entre les deux univers.

délivrer le services de bout en bout : du hardware, du logiciel embarqué, de la connectivité, du stockage, de la sécurité et du web.

Globalement, l'offre de formation sur le sujet s'est étoffée et il est maintenant possible de former ses collaborateurs et plus largement ses équipes afin de mener efficacement ce type de projet.

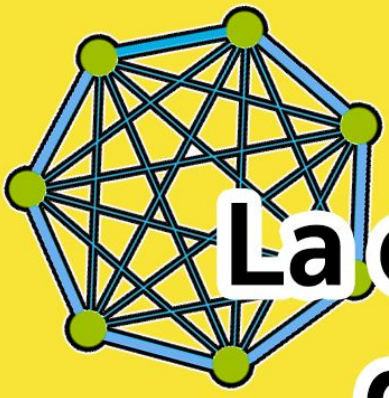
- ***Est-ce que le prototypage d'un service IoT inédit est une étape compliquée ?***

Dans le développement d'un nouvel objet connecté ou même d'un nouveau service basé sur un certain nombre d'objets, l'étape de prototypage s'impose pour tester et se projeter. Lorsque l'objet nécessaire au service n'existe pas à l'échelle industrielle, il devient inévitable de passer par une étape de prototypage matériel (Hardware) qui peut se révéler être laborieuse pour certains. Effectivement, le développement d'une maquette logicielle est souvent plus aisée qu'une maquette hardware. Celle-ci revient souvent plus cher en temps comme en équipement et fait appel à des compétences spécifiques comme l'électronique, la mécanique, le logiciel embarqué ou encore la modélisation et impression 3D.

Illustration 29 : "Hardware, the Hard Way" par Cyril Hlakkache (2018)

Cette étape ne doit pas être négligée et sous estimée afin justement de ne pas être pris au dépourvue lors de cette étape préalable importante. Il est donc recommandé de bien spécifier l'attendu (technique et fonctionnel), d'étudier précisément l'ensemble des possibilités pour réaliser ce prototype (capteurs, plateformes, logiciel embarqué, modèle 3D, retour d'expérience…) et enfin de bien s'entourer pour minimiser le risque et donc les coûts.

Il est par exemple recommandé de faire appel à des partenaires comme les fablabs professionnels, des regroupements d'experts comme à l'IoT Valley ou encore d'aller rechercher des financements d'aide auprès d'organismes. C'est par exemple le cas de Madeeli avec les chèque innovations : *"Petite entreprise, vous avez besoin de vérifier la faisabilité d'un projet avant de lancer votre innovation ? Le chèque innovation permet à des PME de bénéficier d'un accompagnement adapté dans le cadre d'un premier projet d'innovation. Il est prescrit par les acteurs du Réseau pour innover en région RDTI. D'un montant moyen de 7500€, la subvention est financée par la Région Occitanie / Pyrénées-Méditerranée."* (voir : https://www.madeeli.fr/actualites/boite-outils-cheque-innovation/).



La collecte des données

6. Stratégie de collecte et traitement des données

6.1 Les données

Les données sont contenues dans la charge utile des paquets remontant des objets connectés au travers du réseaux vers votre solution applicative, plus précisément dans votre back-end. Ces charges utiles sont appelées Payload et chaque constructeur d'objet peut proposer des contenus très différents pour des capteurs ayant pourtant une même fonction comme un capteur de température par exemple. De ce fait, collecter la donnée demande d'une part de savoir la décoder puis ensuite de l'interpréter. Parfois, dans de larges écosystèmes, pour une même fonction, vous pouvez être confronté à un parc d'objets de fonction identique, mais de marques ou constructeurs variés, de ce fait, pour agréger, utiliser ou comparer ces données, une phase de **normalisation de la donnée** peut devenir nécessaire avant de les intégrer.

Pour que cette normalisation soit rendue plus facile, publier des librairies explicitant la grammaire à utiliser pour exploiter les charges utiles de chaque objet est important afin de faciliter le travail des opérateurs, fournisseurs de services et des intégrateurs de solution digitale qui devront composer avec un parc d'objets hétérogènes et dont le catalogue global atteint déjà des dimensions gigantesques du fait des incroyables opportunités que l'IoT proposent aujourd'hui.

Ainsi, collecter la donnée c'est aussi **préparer la donnée** avant qu'elle ne rejoigne vos systèmes de stockage alimentant les applications délivrant le service aux utilisateurs.

6.2. Quelles données faut-il récupérer des objets ?

Lors de la conception de l'objet connecté, il peut être utile de lui faire envoyer bien plus d'informations que celles dont vous pensez avoir besoin initialement.

D'une part, car il sera compliqué d'ajouter de nouvelles sondes une fois votre objet déployé. Si vous imaginez de nouvelles fonctionnalités liées à des données que vous ne récupérez pas encore sur les premiers objets déployés, il sera quasi-impossible pour vous de les mettre à jour. Cela pourra alors être une source de déception pour les premiers utilisateurs dont l'objet sera rapidement devenu obsolète face aux nouvelles versions.

D'autre part, une fois que vous aurez amassé un grand nombre de données émanant de l'ensemble de votre parc, vous pourrez en extraire des indicateurs de grande valeur. Que ce soit sur le comportement statistique de l'objet (pannes, autonomie réelle, etc...) ou sur son usage (fréquence et horaires d'utilisation, géolocalisation, types de connexion, etc...), vous pourrez éventuellement en tirer des avantages stratégiques.

Toutefois, des limitations liées à la connectivité (volume de données échangeable et coût des échanges sur certains réseaux) et à la consommation d'énergie induite par ces échanges, peuvent de facto restreindre le spectre de données utiles que vous déciderez de remonter depuis l'objet.

Le choix réside en un bon équilibre entre optimisation technique et perspectives du service que vous souhaitez délivrer. Il est donc important d'avoir une vision stratégique du développement de vos services sur au moins 6 mois et au mieux sur les années à venir, ceci afin d'anticiper les besoins de données à remonter par vos objets que vous allez déployer chez vos clients.

6.3. Pour en faire quoi ?

On distingue deux types d'analyses :

- **L'existant** ("Business Intelligence") qui vous renseigne sur le fonctionnement actuel de vos objets et permettra par exemple de générer des tableaux de bord,

- **Le prédictif** ("Machine Learning") ayant pour objectif d'anticiper les pannes et prédire les usages.

L'extraction de ces informations se fait par le biais d'algorithmes qu'il faudra soit développer spécifiquement, soit utiliser sous forme de services SaaS (comme Microsoft Azure Stream Analytics ou Google Prediction API) qui proposent une capacité de compréhension et d'adaptation aux données fournies ainsi qu'une puissance de calcul importante (et adaptée à la tâche !).

C'est également à ce niveau que l'on peut introduire de l'Intelligence Artificielle afin justement d'utiliser les données pour alimenter un raisonnement, permettant d'en faire des déductions dans l'objectif de prendre les bonnes décisions. C'est par exemple le cas des Smart cities qui pourront, à terme, faire appel à des systèmes autonomes de prise de décision. La société IBM propose une solution d'Intelligence Artificielle nommée **Watson** exposant des API permettant ainsi d'utiliser cette puissance en mode SaaS.

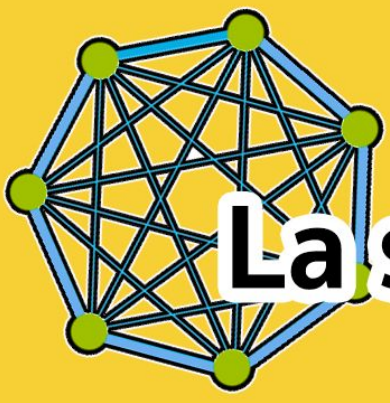
Attention : plus vous collecterez de données, plus vous aurez besoin d'espace disque pour les stocker. Sur un parc de milliers d'objets, il peut vous falloir des téraoctets par semaine ! La puissance de calcul alors nécessaire pour les traiter sera tout aussi importante. De plus, si vous ne faites aucun usage de ces données, le coût et l'empreinte carbone de leur stockage pourraient vite devenir embarrassant. Il y a donc un curseur à placer en termes de collecte et de rétention des données.

6.4. Synthèse

Il faut sélectionner méticuleusement les données à récupérer, en privilégiant les événements bas-niveau qui permettront de reconstituer par déduction logique sur la partie logicielle les événements haut niveau, tout en permettant d’en extraire d’autres informations utiles si besoin.

Aussi, pour que cette donnée soit exploitable dans le cadre d’un écosystème d’objets très variés, il est inévitable de normaliser cette donnée pour la rendre transitive et compatible dans l’ensemble de la solution.

De plus, la collecte de certaines données peut nécessiter un accord des utilisateurs si ces données révèlent des informations sur leur vie privée.



La sécurité

7. La sécurité des objets connectés

7.1 Un état des lieux préoccupant

Depuis plus de deux ans et l'intérêt croissant des éditeurs et consommateurs pour les objets connectés, ces nouveaux équipements se sont fait connaître aussi rapidement pour l'innovation qu'ils apportent que pour les enjeux qu'ils posent en matière de sécurité et notamment la vitesse avec laquelle leur sécurité est mise à mal. L'année 2016 a été particulièrement prolifique sur le plan des exemples d'objet connecté compromis en nous apportant un inventaire très varié donnant parfois le vertige :

- Différents vendeurs de serrures connectés dont les équipements peuvent être ouverts en capturant et rejouant les séquences d'authentification.

- Plus de 70 modèles de voitures connectées permettant à des degrés divers de prendre le contrôle de certaines fonctions à distance, par exemple les véhicules Jeep.

- Divers équipements d'électroménagers, allant du réfrigérateur au lave-linge. Sur les objets personnels, les plus troublants restent la possibilité de prendre le contrôle à distance d'un fusil connecté (et de changer la trajectoire de la balle pour l'amener vers une autre cible).

- Différentes versions de caméras IP, écoutes-bébés connectés, et autres enregistreurs ouverts sur internet en gardant le mot de passe constructeur par défaut.

Au-delà de l'anecdote que ces exemples peuvent représenter, le dernier cas est une illustration de l'intérêt croissant que les attaquants portent aux objets connectés. En utilisant une liste restreinte de 68 mots de passe par défaut de différents modèles de caméra IP, et en prenant le contrôle de plus de 100 000 équipements, les équipes contrôlant le botnet « Mirai » ont été capables de lancer, entre autres attaques :

- Un déni de service mesuré à 1Tb/s (record du monde à ce jour) contre l'hébergeur français OVH,

- un déni de service mesuré à 620 Gb/s contre un site spécialisé en sécurité informatique,

- un déni de service sur Dyn, un service de nom de domaine, rendant difficilement accessible plusieurs grands services comme Facebook et Twitter pendant plusieurs heures. On les soupçonne également d'avoir tenté de couper l'accès internet d'un pays d'Afrique sans succès jusqu'à maintenant, mais les tentatives continuent.

Une recherche rapide sur des outils comme Shodan ou Censys, outils de recherche de tout ce qui est connecté, permet de se rendre compte de l'étendu d'objets ou services laissés connectés sans authentification, amenant même au développement d'outils comme vncroulette[38], qui vous connecte de manière aléatoire sur toutes sortes d'interfaces allant de la caisse enregistreuse au contrôle de processus industriel sur des centrales électriques.

Les objets connectés représentent pour les attaquants, toujours en recherche d'efficacité économique, un terrain de jeu intéressant pour plusieurs raisons :

- Ce sont des plateformes logicielles très stables et identiques sur tous les objets du même type (même marque et modèles). Contrairement aux plateformes PC traditionnelles qui sont beaucoup plus hétérogènes, cela rend l'écriture d'un hack beaucoup plus efficace puisqu'il pourra fonctionner sur l'ensemble des équipements vulnérable sans gros effort de recherche. Une même vulnérabilité peut donc permettre de prendre le contrôle de plusieurs milliers de dispositifs très rapidement.

- La sécurité n'est pas une priorité pour beaucoup de fabricants d'équipement, qui n'appliquent pas les bonnes pratiques élémentaires en laissant des mots de passe par défaut et des ports ouverts sur leurs dispositifs sans justification pour le service rendu à l'utilisateur.

- Il y a peu ou pas de supervision de sécurité sur ces dispositifs qui sont branchés puis oubliés tant qu'ils rendent le service souhaité.

- La difficulté de mettre à jour les systèmes et logiciels de beaucoup d'objets connectés rend l'infection, et donc le contrôle par l'attaquant, beaucoup plus pérenne dans le temps[39].

- Suivant le type d'objet, il permettra aux attaquants de mettre en place toutes sortes d'activités criminelles, allant du botnet traditionnel pour des attaques de masse à la capture de données à des fins d'extorsions, d'espionnage, ou de revente de données personnelles.

7.2 Une maturité à construire

Cette apparente facilité pour les attaquants de prise de contrôle sur les objets connectés peut s'expliquer de plusieurs manières. De manière générale, la pression économique pesant sur les entreprises, souvent des startups, pour être les premiers sur le

[38] Sur vncroulette, voir cet article pour un résumé
[39] Sur ce sujet, une illustration très pertinente est la démonstration du hack de téléviseurs connectés via les canaux de diffusions numérique, permettant le mise en place d'un malware résidant dont la suppression coute plus cher que le remplacement du dispositif sur 90% des téléviseurs récents.

marché et présenter une réelle innovation sur le plan de l'usage, se fait au détriment d'un certain nombre de contrôles s'appliquant habituellement sur les projets informatiques. La sécurité, mal prise en compte, est rapidement considérée comme un frein à l'innovation et au développement du projet, et reléguée à une version ultérieure.
La tendance à la mise au point de nouveaux objets en s'appuyant sur des composants du marché peut également expliquer cette absence de prise en compte de la sécurité dans la fabrication des objets, les efforts se faisant principalement sur l'intégration des composants pour fournir le service désiré, en considérant que chaque composant peut assurer sa propre sécurité.

De manière plus générale, les problèmes de sécurité rencontrés par les objets connectés s'expliquent par le manque d'intégration de la sécurité dès les phases de conceptions des objets et services, du manque de culture sur la sécurité des équipes de conception, mais aussi par le manque de standard et de solutions proposées par les spécialistes de la sécurité qui pourrait permettre d'appliquer de manière simple des principes de sécurité à l'ensemble du projet, de la conception à la fabrication et mise en production.

Pourtant, la sécurité des objets connectés devient un enjeu majeur pour l'ensemble de la filière lorsque l'on réalise que cela représente un frein à l'adoption de ces technologies aussi bien par le grand public que par les entreprises.

Au niveau des particuliers, la méfiance est de mise aussi bien sur le plan de l'exposition des données personnelles et de la vie privée, qu'au niveau de l'utilisation qui peut être faite des données collectées. La méfiance par rapport au déploiement des compteurs électriques intelligents, parfois basés sur des rumeurs plus que des faits concrets en sont des exemples tout comme les questions sur l'utilisation des données de santé collectées par des équipements médicaux ou des traceurs personnels dans le cadre de leur fonctionnement en est un autre.

Au niveau des entreprises, le manque d'expertise sur les sujets de sécurité lors de la conception ou l'utilisation d'objet connecté entraîne une certaine prudence des décisionnaires. Les risques à évaluer se situent en premier lieu au niveau de l'impact pour l'image de marque de l'entreprise, mais seront bientôt rattrapés par la mise en place du **Règlement Général sur la Protection des Données** (**GDPR**[40] en anglais) et par le **Référentiel Général de Sécurité** (**RGS**). Cette nouvelle réglementation a pour but de renforcer la protection des données personnelles au sein de l'Union Européenne, avec comme objectif affiché de redonner aux citoyens le contrôle de leurs données personnelles, tout en simplifiant l'environnement réglementaire des entreprises.

[40] **GDPR :** Nouveau **règlement européen sur la protection des données personnelles** qui entrera en vigueur en mai 2018. Il constitue le nouveau texte de référence européen en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne. Il propose les notion de « **Privacy by Design** » et de « **Privacy by Default** ». Pour mettre en place ces concepts, l'outil indispensable est l'évaluation d'impact sur la vie privée nommée **EIVP** ou **PIA** en anglais. Pour plus de détail, nous vous conseillons de lire : Étude d'impact sur la vie privée (EIVP/PIA), Méthode sur le site du CNRS.

L'impact de ce nouveau règlement sur l'ensemble de l'écosystème de l'IoT devrait apporter, lors de sa mise en place en 2018, une réponse claire au consommateur inquiet de l'utilisation de ces données. Il impose également à chaque acteur de la chaîne d'être en mesure d'apporter des réponses en termes de protection :

- **Au niveau des fournisseurs de composants**, sur la sécurité du composant, sa capacité à protéger des données stockées ou en mouvement, à s'intégrer dans la chaîne de production de manière authentifiée.

- **Au niveau des fournisseurs de plateforme et de ses sous-traitants**, de s'assurer de la protection des données qu'ils stockent et des services qu'ils hébergent et de l'utilisation des données uniquement par des acteurs clairement identifiés.

- **Au niveau des fournisseurs de service et de solutions IoT,** ils doivent s'assurer d'une sécurité de bout en bout, car leur responsabilité directe sera engagée en cas d'incident, avec des conséquences financières importantes dans le cadre du RGDP.

7.3 La nécessité d'une sécurité de bout en bout

Comme décrit précédemment, les environnements IoT sont des environnements hétérogènes complexes, demandant la mise en place de mesure de sécurité couvrant l'ensemble de l'écosystème qui comprend l'équipement connecté, la plateforme de service Cloud et la connectivité entre les différents éléments, et doit supporter un environnement ou les ressources sont souvent limités de par la nature des devices IoT qui n'ont souvent pas la puissance nécessaire pour supporter les solutions de sécurités traditionnelles. De plus, il serait trompeur de penser qu'il existe des solutions magiques pouvant couvrir simplement tous les périmètres de l'IoT. La sécurité doit être exhaustive à tout le périmètre, car les attaquants sont bien équipés pour découvrir le maillon faible et l'exploiter. Bien sûr, certains principes de sécurité de l'IT traditionnelle peuvent s'appliquer à l'IoT, mais l'IoT engendre également des besoins spécifiques qu'il conviendra de traiter systématiquement en s'appuyant sur ces cinq piliers: **protection de l'infrastructure, protection des communications, protection de l'utilisateur, gestion des équipements, supervision de l'écosystème**.
Ces piliers doivent être combinés pour former les fondations de l'architecture de sécurité permettant d'atténuer l'impact de la plupart des menaces pesant sur l'internet des objets. L'objectif ici n'est pas d'apporter toutes les réponses possibles sur un sujet vaste, mais de donner des pistes permettant de redonner confiance en la capacité d'arriver à un internet des objets plus sûr.

7.3.1 Sécurité intrinsèque

Contrairement à l'IT traditionnelle, la plupart des devices IoT sont des dispositifs à environnements fermés. Les clients ne peuvent pas choisir d'ajouter une couche de sécurité après avoir acquis la solution qui est contrôlée par le fournisseur. Pour cette raison, la sécurité doit être pensée dans les équipements dès la conception, par une approche « **secure by design** ». Dans cette approche, la sécurité n'est plus un complément qui pourrait se faire à posteriori, mais bien partie intégrante du processus de fabrication.

C'est à l'industrie de la sécurité de prendre le virage de cette sécurité intrinsèque en apportant une nouvelle approche par composants à des technologies classiques : intégrité, chiffrement, authentification, prévention des intrusions, mise à jour sécurisée, etc.
Par rapport aux plateformes traditionnelles, le fait d'intégrer la sécurité dès la conception permet de **profiter d'une meilleure intégration entre le matériel et le logiciel** pour bénéficier au niveau de la sécurité de certaines fonctions apportées par les fabricants de composants matériels comme le stockage des certificats et clefs de chiffrement dans des environnements d'exécution de confiance[41], permettant une meilleure protection des communications, du système ou des données. Cependant, l'importance de cette intégration ne doit pas cacher qu'il ne s'agit que de la première ligne de défense qui doit s'étendre à la gestion de l'authentification, l'infrastructure OTA, et les modules d'analytique orientés sécurité et anomalie.

7.3.2 Protection des dispositifs

La protection des devices eux-mêmes dans le contexte de l'IoT est particulièrement importante lorsque l'on considère que beaucoup de ces solutions peuvent être déployées dans des endroits sans possibilité de contrôle fort sur l'accès physique à ces dispositifs. Cela ouvre la porte à toutes sortes de possibilités d'attaque, comme le reverse-engineering des systèmes et applications, communications et processus d'authentification. Le dispositif doit donc devenir la première ligne de défense en apportant ses propres mécanismes.

Protection au niveau du dispositif.

Les techniques classiques de diminution de surface d'attaque peuvent s'appliquer pour la protection du device en propre : Durcissement du système, liste blanche d'applications autorisées, cloisonnement (sandboxing) des applications, chiffrement, contrôles basés sur la réputation, restrictions sur les communications en entrée et sortie. Certaines solutions permettent de rajouter au niveau du système des vérifications du comportement des applications, des protections contre les attaques au niveau de la mémoire, tout en gardant le contrôle du device. Elles peuvent aussi fournir des mécanismes d'envoi d'information et d'alerte en cas d'actions non autorisées comme le branchement d'un dispositif externe sur le device.

[41] Sur les TEE et Trustzone, voir en ici en anglais ou en français. Les TEE ne sont qu'une des possibilités offerte en matière de sécurité d'un meilleure intégration logicielle et matérielle

L'utilisation d'une combinaison de ces différentes techniques doit se faire en accord avec les contraintes en ressource inhérente à l'application IoT protégée (manque de puissance, de mémoire, de stockage, consommation d'énergie limitée, manque de connectivité vers internet, etc.)

Système et applications de confiance

Une des premières étapes pour la protection d'un device est de s'assurer qu'il ne démarre et ne fasse fonctionner que du code pour lequel il a été conçu. Pour le système, cela passe par l'utilisation des fonctions de secure-boot fournies par les fabricants de matériel. De manière similaire, pour les applications de haut niveau, on peut facilement mettre en place des mesures pour vérifier l'authenticité du code et n'accepter que des applications venant de sources de confiance. On peut ainsi signer l'ensemble de la chaîne logicielle depuis les systèmes, drivers et applications.

Une fois que ces fonctions sont en place, la difficulté peut venir de la gestion des clefs et le contrôle d'accès à ces clefs nécessaires pour gérer l'ensemble de ces logiciels. Sur ce point, il existe aujourd'hui des services en ligne permettant de gérer de manière efficace, industrielle et à grande échelle la signature du code, la révocation de ces signatures et les clefs permettant la gestion de l'ensemble.

Pour des raisons d'efficacité énergétique, on peut aussi s'intéresser à des approches plus fines de signature des composants critiques plutôt que d'imposer la signature systématique de tous les blocs logiciels.

Gestion des dispositifs

Comme mentionné plus haut, plusieurs raisons poussent à mettre en place une bonne gestion des dispositifs dès la conception du service. Les dispositifs seront attaqués, des bugs seront à corriger, des vulnérabilités découvertes ; et ces dispositifs devront être mis à jour via des processus **OTA**[42] (Over The Air). Cependant mécanismes de mises à jour OTA ajoutent suffisamment de complexité pour qu'elles rebutent un certain nombre d'acteurs qui décident de s'en passer sans en mesurer les risques.

Les bénéfices d'une bonne gestion des mises à jour dépassent pourtant le simple cadre de la sécurité :

- **Mise à jour** de la configuration,
- **Gestion** de la sécurité et du contrôle d'accès,
- **Récupération de données** de télémétrie pour analyse orientée sécurité,

[42] **OTA (Over The Air) :** Technologie permettant d'accéder aux données d'une carte SIM à distance. Elle permet par exemple à un opérateur de téléphonie mobile de mettre à jour le contenu ou d'introduire un nouveau service sur tout un lot de cartes SIM de manière rapide, efficace et peu coûteuse.

- **Supervision** de fonctionnement correcte du système,
- etc.

Toutes les tâches ci-dessus doivent pouvoir se faire de manière sûre et sécurisée, ce qui est facilité de nos jours par l'émergence de standards pour la gestion des logiciels, l'inventaire des firmwares et la revue de configuration de chaque dispositif, avec des solutions disponibles chez plusieurs vendeurs s'appuyant sur des formats telle que ceux promus par l'Open Mobile Alliance. On fera attention cependant à ce que la solution choisie permette la gestion d'un parc montant à plusieurs dizaines ou centaines de millions de dispositifs.

D'un point de vue de la sécurité pure, les mises à jour OTA permettent de maintenir des mécanismes comme des listes noires d'adresses IP, nom de domaines, ou réputation d'un exécutable à bannir, ou à l'inverse de confirmer des listes blanches de code exclusivement autorisé ou de certificats à révoquer. Elles permettent aussi de collecter des informations de télémétrie qui viennent s'inscrire dans un cadre d'analyse de sécurité et de détection des menaces.

En fonction des ressources, on privilégiera à minima une mise à jour complète à distance du dispositif si l'environnement ne permet pas des mises à jour fines afin de garantir les corrections de failles inévitables sur le long terme.

7.3.3 Protection des communications et authentification

Authentification entre les composants

La protection des communications passe par le chiffrement des données en mouvement et l'authentification des communications. La mise en place d'un modèle de confiance (trust model) basé sur des certificats permet l'interopérabilité des différents composants de l'architecture d'un service IoT via l'utilisation de certificat fort géré par des autorités de certification pérennes.

Le besoin d'authentification dans le contexte de l'IoT est encore plus marqué pour des raisons évoquées par ailleurs, avec des accès physiques difficiles à contrôler. Il devient alors particulièrement dangereux d'accepter des communications de devices ou de services non authentifiés, puisque les attaques de type man-in-the-middle sont facilitées par la dispersion des équipements et le manque de contrôle au niveau physique. L'utilisation d'une authentification forte mutuelle entre les différents composants de l'écosystème (capteur, device, service, etc.) permet de se protéger contre ce type d'attaque.

La mise en place d'une authentification mutuelle à base de certificat est aujourd'hui facilitée par de nombreux standards existants comme SCEP[43], ou OCSP[44] permettant une gestion

[43] **SCEP (Simple Certificate Enrollment Protocol) :** Protocole simple d'enregistrement de certificat développé par Cisco Systems.

OTA des certificats. Ces protocoles d'authentification mis en place dans le cadre de communication TLS[45] ou DTLS[46] facilitent l'échange de clef pour le chiffrement de la communication des données.

Dans certains cas, il peut être acceptable, si la donnée n'est pas sensible, de n'utiliser qu'un mécanisme de signature des données pour limiter la consommation de ressources induite par le chiffrement. Cela peut être le cas notamment entre un capteur et un collecteur de données, mais la signature est également recommandée pour garantir la validité des données de bout en bout.

Cependant, depuis l'élaboration de nouveaux algorithmes de chiffrement basés sur les courbes elliptiques, le coût en ressource du chiffrement a fortement baissé avec des vitesses de chiffrement jusqu'à 10 fois plus rapide que les algorithmes précédant, rendant le chiffrement des données abordable même sur des processeurs à faible puissance. Le chiffrement des données doit donc être systématiquement étudié et devenir la norme, l'échange de données en clair l'exception pour des données non sensible en cas de manque de ressources.

Authentification des acteurs du service

Au-delà de l'authentification des différents composants de l'écosystème entre eux, la mise en place généralisée de certificats gérés centralement permet de contrôler les niveaux d'accès et les rôles des différents acteurs devant accéder au service. Un bon exemple de ces besoins s'illustre par les besoins de la distribution d'énergie au particulier contrôlée par des Smart Meter. Dans ce type d'écosystème, les acteurs sont :

- Le consommateur,
- Le fournisseur d'énergie,
- Le transporteur d'énergie,
- Le fabricant du Smart Meter,
- Le fournisseur de la plateforme de gestion des Smart Meter,
- L'autorité de régulation (s'il y a lieu).

Dans cet environnement, tous les acteurs n'ont pas tous le même rôle ni les mêmes besoins d'accès aux informations. Notamment, on peut imaginer que l'accès à distance au Smart Meter soit limité :

- **Au transporteur d'énergie** pour superviser la distribution,

[44] **OCSP (Online Certificate Status Protocol) :** Protocole Internet utilisé pour valider un certificat numérique X.509 et qui est standardisé par l'IETF.
[45] **TLS (Transport Layer Security) :** Protocoles de sécurisation des échanges sur Internet.
[46] **DTLS (Datagram Transport Layer Security) :** Protocole fournissant une sécurisation des échanges basés sur des protocoles en mode datagramme. Le protocole DTLS est basé sur le protocole TLS et fournit des garanties de sécurité similaires.

- **Au fournisseur d'énergie** pour superviser la consommation en temps réel et alerter le consommateur dans le cadre du service fourni,

- **Au fournisseur de la plateforme de gestion** (s'il s'agit d'un acteur différent du transporteur) pour la supervision de l'infrastructure, la collecte des données et la mise à disposition du consommateur.

Dans ce cadre, la mise en place d'une gestion des authentifications par certificat permet de répondre de manière flexible non seulement aux besoins de contrôle d'accès de chaque acteur en fonction de son rôle, mais aussi d'apporter la souplesse nécessaire pour répondre aux besoins du marché de la distribution d'énergie.

En effet, si le consommateur décide de changer de fournisseur d'énergie, on s'imagine mal lui demander un accès physique à son habitation afin de procéder à des travaux de changement de compteur. Une gestion par certificat permet, par simple révocation du certificat du fournisseur précédent[47] et mise en place du certificat du nouveau fournisseur, de gérer le changement de fournisseur de manière efficace sans toucher à l'infrastructure en place.

7.3.4 Supervision du service

Il faut bien évidemment considérer que malgré l'exhaustivité des mesures décrites plus haut, elle ne peut peuvent être considérer comme une garantie complète qu'un attaquant ne pourra prendre le contrôle de tout ou partie de 'l'infrastructure IoT. Pour cette raison, une stratégie de contrôle des menaces la plus complète requiert la mise en place de module d'analyse de sécurité pour ajouter des fonctions de détections aux fonctions de protection décrites précédemment. Ces modules d'analyse peuvent s'appuyer sur la télémétrie récupérée depuis les dispositifs IoT et équipements réseaux déployés dans l'infrastructure pour donner de la visibilité sur ce qui se produit sur l'ensemble de l'écosystème, y compris les menaces les plus furtives.

Fournissant des moyens de détection d'égale importance, la supervision et l'analytique orientées sécurité peuvent aussi offrir une couverture pour les environnements plus anciens (type ICS – Industrial Control System par exemple) qui ne peuvent être modifié que difficilement pour rentrer dans un cadre de sécurité intrinsèque.

7.4 Des pistes pour l'avenir de la sécurité des objets

[47] La révocation d'anciens droits est souvent sous-estimée : beaucoup de serrures connectées garde les droits de leurs anciens propriétaires même si un nouveau compte de gestion leur est associé. Mais qui irait acheter une serrure connectée d'occasion ?

Malgré les mesures décrites précédemment, les environnements IoT demandent d'explorer de nouvelles voies pour offrir de meilleures garanties de sécurités, notamment pour permettre la connexion d'environnement critique.

7.4.1 Détection d'anomalies

Les environnements IoT étant des environnements contraints, les déviations de ce qui a été mis en place peuvent être rapidement identifiées. L'idée de la détection d'anomalie est d'inclure des modules d'analytique dédiés capable de détecter le plus rapidement possible toutes ces déviations. La grande variété des environnements industriels et des protocoles IoTs peuvent rendre ce problème difficile, mais de nouvelles techniques basées sur du machine learning offrent des pistes prometteuses.

Au-delà de ces capacités de détection spécifique, la détection d'anomalie doit aussi permettre d'apporter des réponses adaptées aux types d'attaque et aux environnements ciblés. Si l'on prend l'exemple des voitures connectées, la question se pose de que faire en cas d'attaque massive sur un parc de voiture. Il est difficile d'envisager d'arrêter l'ensemble des voitures ciblées, mais l'on ne peut non plus prendre le risque de dommages dus à une prise de contrôle massive. Les modules de détection d'anomalie couplés à du machine learning doivent permettre à terme de prendre des décisions fine en prenant compte de paramètre de l'attaque et de la situation de chacun des véhicules ciblés.

7.4.2 Éducation des utilisateurs

Au niveau des consommateurs, le rétablissement de la confiance passe par une meilleure éducation et une meilleure information. L'éducation doit se faire sur les précautions d'usage à prendre dans la mise en place d'objet connecté et peut se faire lors de l'activation du service en imposant des précautions d'usage comme la modification du mot de passe par défaut. Elle peut se faire aussi par le développement de solution apportant de la visibilité sur l'ensemble des objets connectés au domicile de l'utilisateur afin de le guider dans sa prise de contrôle des données et services utilisés par ces objets.

L'éducation des utilisateurs passe aussi par une meilleure information sur les données utilisées par ces services. Ici, des standards sont à développer afin que chaque service IoT à destination du grand public puisse communiquer de manière homogène sur l'utilisation faite des données personnelles.

7.4.3 Déclaratif des objets

Une des pistes émergentes afin d'assurer une meilleure cohésion des objets connectés et de leur sécurité serait une approche basée sur l'obligation pour chaque objet se connectant à l'écosystème de passer par une étape de déclaration pour annoncer les services utilisés et les interactions attendues avec le reste de l'infrastructure. La mise en

place d'un répertoire des objets, ou si l'on pousse le modèle jusqu'au bout, un répertoire du tout (Directory of Everything), incluant les dispositifs, systèmes, utilisateurs, et tous les composants des services avec une définition claire des rôles de chacun, permettrait d'améliorer la détection des anomalies et les échanges de données entre les services pour des services à valeur ajoutée combinant un ensemble de services IoT. Cette vision aujourd'hui demande le développement de standards et une adhésion des industriels qui reste encore à créer.

7.4.4 Blockchain et IoT

Mises en lumière par le développement des cryptomonnaies, les architectures de type Blockchains ont pris de l'importance dans d'autres cas d'usage ayant des besoins en anonymisation des échanges ou en décentralisation de la relation de confiance. Cela inclut la possibilité de réaliser des échanges contractuels de manière intelligente sans tiers de confiance, la distribution des espaces de stockage dans le cloud, et plus généralement des échanges basés sur des relations point à point où la diminution des intermédiaires peut faire gagner en efficacité sans nuire à la sécurité.

La blockchain suscite de l'intérêt dans le domaine de l'IoT car elle apporte:

- **La possibilité d'une administration décentralisée :** l'absence de centralisation apporte la possibilité d'une croissance plus maîtrisée et une meilleure robustesse du service, tout en favorisant des échanges point à point entre divers éléments de l'écosystème IoT plutôt que des relations 1-N. Cela permet d'éliminer des points de latences et réduit les risques de maillons faibles dans l'architecture de gestion de l'écosystème IoT.
- **L'anonymat :** la possibilité de rassurer l'utilisateur final sur la possibilité de ne pas exposer son identité dans la plupart des échanges tout en assurant les échanges de données nécessaires au bon fonctionnement du service. L'actualité récente autour des réseaux sociaux et des compteurs intelligents prouve la sensibilité d'une partie de la population sur ces sujets.
- **La sécurité des échanges :** Par nature, la blockchain assure la sécurité des échanges entre les différentes parties, même si l'infrastructure servant à ces échanges n'est pas digne de confiance, et ce dans des environnements hétérogènes impliquant de multiples acteurs.

Cependant, malgré quelques expériences prometteuses mises en place sous forme d'expérimentation comme la création d'un **Smart grid**[48] entre une cinquantaine de participants à Brooklyn, ou les initiatives lancées par de grands industriels comme la Trusted IoT Alliance pour promouvoir l'utilisation de la Blockchain, il reste encore beaucoup d'obstacle à surmonter avant d'aboutir à une réelle généralisation de ces technologies:

[48] **Smart grid :** Réseau électrique intelligent consistant en un réseau de distribution d'électricité qui favorise la circulation d'information entre les fournisseurs et les consommateurs afin d'ajuster le flux d'électricité en temps réel.

- **Ressources en processing :** la blockchain étant basée sur le mining, ou la résolution de challenge cryptographique complexe, elle demande des ressources en processing généralement absentes des infrastructures IoT, et particulièrement sur les éléments émettant les données. Cependant, de récentes avancées sur des algorithmes de mining moins gourmand autour des cryptomonnaies (ethereum par exemple) représentent des pistes intéressantes, mais non encore confirmées.
- **Latence induite:** la création des blocs de confiance peut prendre du temps et dans le cas des algorithmes utilisés par le Bitcoin, plus les acteurs sont nombreux et plus ce temps est important. Cette latence peut être rédhibitoire dans la plupart des environnements IoT.
- **Montée en charge :** le Bitcoin, basé sur les technologies de blockchain les plus répandues actuellement, montre de sérieux problèmes de montées en charge; chaque nouvel entrant apportant un besoin exponentiel en processing donc en latence des échanges, augmentant les deux premiers problèmes décrits ci-dessus. Dans des environnements IoT comportant potentiellement des dizaines ou centaines de millions d'acteurs, cela peut s'avérer désastreux.
- **Augmentation des besoins en bande passante:** la blockchain apporte une validation décentralisée des échanges, mais aussi une augmentation du nombre d'échanges et d'interlocuteurs. Les environnement IoT utilisant des réseaux à faible capacité d'échange de données sont à écarter à l'heure actuelle.

En conclusion, bien que prometteuses sur le papier, les technologies de la blockchain ont encore leurs preuves à faire avant de se voir généralisées dans l'IoT.

7.5 IoT et IIoT, une nouvelle classe de systèmes embarqués : Risques, enjeux et solutions

De nos jours les objets connectés (IoT), simples « gadgets » ou systèmes industriels complexes (IIoT), sont partout et tous ces équipements entrent dans la catégorie des systèmes embarqués (embedded systems), leur point commun étant d'être connectés à des réseaux ouverts. Si cette connectivité est un plus en termes de fonctionnalités, elle n'est pas sans risque, notamment dans le domaine de la sécurité, et plus particulièrement de ce qu'on classe en cybersécurité. Afin d'assurer la sécurité de ces produits, il devient crucial de bien comprendre les risques et d'adopter les bonnes solutions pour s'en prémunir. Voici quelques éléments issus d'une récente étude Gartner (Mars 2018) : *près de 20% des organisations ont observé au moins une attaque en direction de l'IoT au cours des trois dernières années. Pour se protéger contre ces menaces, Gartner prévoit que les dépenses mondiales en sécurité IoT atteindront 1,5 milliard de dollars en 2018, soit une augmentation de 28% par rapport à 2017. D'ici 2021, la conformité à la réglementation deviendra le principal facteur d'adoption de la sécurité IoT.*

7.5.1 Risques et enjeux

Les enjeux

Les enjeux sont multiples, mais pour beaucoup, ils sont avant tout financiers. Avec rapidement plusieurs milliards d'objets connectés et une explosion dans les services associés, cela représente des dizaines milliards de dollars en chiffre d'affaires. Naturellement liés à la quantité d'objets qui seront déployés et au business généré, ces enjeux financiers le sont aussi aux risques encourus et aux dommages éventuels liés à une attaque.

Quelques secteurs industriels regrouperont 80% des dépenses (ou revenus selon l'angle de vue) du marché IoT en 2020 (source ATKearney) :

- L'industrie (et notamment l'automatisation)
- L'énergie (avec notamment le développement des Smartgrid)
- Les transports et La logisitique
- Le logement
- La santé

Au vu de cette liste, il est évident que l'enjeu premier pour les années à venir sera lié à la sécurité.

Les risques

Les systèmes embarqués évoluent dans des contextes extrêmement variés et surtout hors du contrôle étroit qu'on peut envisager pour des ordinateurs connectés en réseau, par exemple au sein d'une entreprise. L'objet connecté va être déployé en grandes quantités, par des utilisateurs ignorant généralement les risques techniques, dans le respect plus ou moins approximatif du mode d'emploi, et va communiquer avec une variété de systèmes, la plupart inconnus du concepteur de l'objet. Par ailleurs, leur prolifération augmente de facto la surface d'attaque offerte à des individus ou organisations malveillants. Leurs concepteurs sont focalisés sur les fonctionnalités et l'apport d'innovations de leur produit, et peu se préoccupent des risques liés à la cybersécurité encourus par l'intégration de l'objet dans son environnement futur.
Jusqu'à récemment, et bien qu'ils soient éventuellement en réseau, les systèmes embarqués évoluaient en vase clos, un parfait exemple étant l'automobile : quasiment la totalité des calculateurs à bord du véhicule sont interconnectés entre-eux (via le bus CAN[49] principalement), mais jusqu'à présent la connexion vers l'extérieur du véhicule n'était pas la norme. Hors, connecter un équipement à internet revient à le rendre visible potentiellement du monde entier. Il est donc crucial de non seulement contrôler l'accès au système, mais également d'être à même de détecter des tentatives d'accès non autorisées.

Quelles solutions adopter ?

[49] **CAN (Controller Area Network) :** Protocole de communication série normalisé qui supporte efficacement le contrôle en temps réel de systèmes distribués tels qu'on peut en trouver dans les automobiles ou le milieu industriel (Source : http://www.oberle.org/).

Lors de la conception d'un produit connecté, il ne s'agit pas seulement de faire une analyse de risque par rapport à la criticité d'une attaque et des conséquences sur le produit lui-même (vol de données, arrêt du service, etc), mais également en termes de son utilisation frauduleuse.
Il n'y a pas une solution unique et définitive réglant la problématique de sécurité pour les systèmes embarqués. D'une part, ils sont, par nature, très différents les uns des autres, que ce soit en termes d'architecture matérielles ou logicielles ou de ressources disponibles, les écosystèmes dans lesquels ils évoluent sont divers, les risques inhérents sont variés et enfin les attaques ont de multiples facettes et évoluent en permanence. Il existe pourtant aujourd'hui des méthodes de travail et des solutions techniques permettant de se prémunir dans une grande mesure contre les risque encourus. On peut classer ces méthodes et techniques en 3 grandes catégories :

- La protection du système de développement, liée à une sécurité du système d'information du concepteur (et qui couvre aussi l'équipe de développement elle même)
- Des solutions matérielles intégrées aux processeurs ou périphériques, sujet couvert dans un autre chapitre de ce livre blanc
- Les solutions liées au développement et au déploiement du système embarqué lui même, objet de ce chapitre

Protéger et/ou surveiller

En matière de cybersécurité, on considère souvent 2 options qui s'avèrent complémentaires : protéger et surveiller. La 1ère option consiste à sécuriser le système pour le rendre moins vulnérable, tandis que la seconde a pour but de détecter et déjouer les attaques. On peut difficilement imaginer de se contenter de l'une des options si on veut avoir une sécurité correcte dans le temps. Il est également recommandé de prévoir plusieurs lignes de défense, afin qu'une défense en échec n'expose pas le produit. Comme armer le système d'alarme de sa maison (surveillance) n'empêche pas de verrouiller portes et fenêtres (protection) si on s'absente.

Il existe une grande variété de solutions pour chacune de ces options, et plutôt qu'une tentative de les détailler exhaustivement, nous avons plutôt choisi de mettre en lumière dans ce chapitre quelques possibilités pour chaque option. Une bonne démarche de sécurité combine méthodologie et outils. Elle doit intervenir dès les phases initiales de conception du produit en adoptant une démarche « Secure by Design », et être suivie tout au long du projet. Pour la protection, nous allons notamment nous intéresser à la sécurisation du système, du code et des données, et pour la surveillance à quelques solutions permettant de protéger le système durant toute sa durée de vie.
Pour chaque méthode ou typologie d'outil présentée, nous restons dans ce document sur une description simplifiée, le lecteur pourra trouver auprès des auteurs ou sur internet les compléments d'information pour les sections qui lui sembleront appropriées.

7.5.2 Protéger le système

Nous allons dans cette section mettre surtout l'accent sur 2 points principaux, la gestion et traçabilité des exigences et la maîtrise du code par l'analyse statique.

Exigences et traçabilité

Une première étape, encore trop souvent négligée, est de définir précisément les attentes du système global (fonctionnelles mais aussi de sécurité) de façon à pouvoir les tracer ensuite, en s'assurant que le système final répond à toutes les exigences énoncées, et seulement à celles- ci. Autrement dit, le système fait tout ce qu'il doit faire, mais pas plus ni moins. Cette étape est vivement conseillée, aussi bien pour les démarches de sûreté de fonctionnement que par l'**ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information) dans le cadre de la sécurité (dans son document « La cybersécurité des systèmes industriels »).

Qu'est-ce que la traçabilité des exigences ?

La traçabilité des exigences permet à tout instant de connaître facilement les liens entre les exigences (utilisateurs, spécification, conception…), la réalisation et les tests associés. Elle permet donc de répondre aux questions suivantes :

- Comment a-t-on implémenté cette exigence ?
- A-t-on oublié une demande dans le développement ?
- Quels tests permettent de montrer que cette demande est couverte ?
- Quel impact aurait une modification de cette exigence, sur le reste du cycle de vie produit ?

La traçabilité des exigences permet donc non seulement de ne pas oublier une demande dans la réalisation de son produit, mais aussi et surtout de détecter des incompatibilités entre demandes, normes, contraintes techniques, moyens disponibles… Elle nécessite la mise en place préalable d'une démarche de gestion des exigences, c'est-à-dire de :

- Décrire un système en fragmentant sa complexité en portions de dimensions réduites
- Créer un identifiant unique pour chaque exigence, permettant de les distinguer sans erreur.

Assurer la traçabilité des exigences, c'est lier une exigence avec une autre de plus « haut » niveau, les exigences en « aval » couvrant les exigences en « amont ».
Cette tâche peut être effectuée au travers d'un fichier texte ou d'un tableau Excel®, mais lorsque le nombre d'exigences explose, la matrice de traçabilité devient très volumineuse, complexe à mettre à jour, et le taux d'erreur important. Un outil sera alors recommandé, surtout si l'objectif est d'améliorer la qualité et la sécurité du produit embarqué.

Code	Name	Severity	Occurrence	Detection	RPN (FMEA)	Risk Level (FMEA)
ElecReq_0040 (2)	Hardware detection corrupted CRC packet					
RISK_0010 (1)	Fiber Channel - Digital Communications	6 - Moderate	2	10 - No Design Control	120	Unacceptable Risk
ACTION_0010	Increase cable robustness	7 - High	1	5 - Moderate	35	Acceptable Risk
ElecReq_0050 (3)	Communication wheel					
RISK_0050 (2)	VSS-PSS Fiber Channel - Digital Communications	9 - Hazardous wit...	4	9 - Very Remote	324	Unacceptable Risk
ACTION_0030 (...	Communication wheel	5 - Low	4	4 - Moderately High	80	Investigate Risk
ACTION_0...	Redundant Fiber Channel	5 - Low	2	4 - Moderately High	40	Acceptable Risk
ElecReq_0060 (8)	Hardware FRL					

Illustration 30 : Qualité et sécurité du code source,
Source : ISIT

Outre suivre les liens entre exigences, la traçabilité permet a minima de lier automatiquement les exigences avec les tests effectués (vérification de règles de codage,

de métriques qualité logiciel, couverture de code, tests). La mise en œuvre d'un outil permet de traiter les contraintes cybersécurité du projet comme un métier à part entière.

Maîtriser son code

Un code non maîtrisé, c'est une faille de sécurité potentielle. Une première mesure peut être de mettre en place un Plan d'Assurance Qualité Logiciel (PAQL) qui permettra de :

- Suivre et appliquer les normes sécurité (ISO2700x, EDSA, ISA/IEC62443, …) qui apparaissent et donnent des recommandations (voir imposent pour certaines certification sécurité) utiles pour les logiciels
- Définir des méthodologies de développement, gérer les exigences
- Vérifier/tester le code : couverture structurelle, analyse statique des sources, des binaires, des COTS

Analyse statique du code

Le logiciel occupe une place prépondérante dans le développement des systèmes embarqués. Même si ces développements sont faits de manière très professionnelle, il reste des erreurs, et plusieurs analyses arrivent à la conclusion que le taux moyen d'erreur résiduel dans un développement logiciel est de l'ordre de 1 à 3 erreurs pour 1000 lignes de code (LoC). Comparons cette information aux estimations suivantes : Windows représente 45 millions de lignes, Android 12 millions… et le code total déployé dans une voiture moderne se situe autour de 100 millions de lignes de code !!!
Un programme peut très bien fonctionner de façon nominale, et avoir passé une batterie de tests fonctionnels, sans pour autant être exempt de failles. Dès lors, la détection de vulnérabilités au sein des développements logiciels devient d'une importance capitale, car elles peuvent impacter directement la sûreté et la sécurité. Pour mener à bien cette tâche, plusieurs techniques complémentaires existent, et notamment l'analyse statique avancée.

Qu'est-ce que l'analyse statique avancée ?

Contrairement à l'analyse dynamique, qui teste le comportement d'un code en l'exécutant, l'analyse statique détecte des erreurs logicielles ou des violations de règles par relecture, donc sans exécution et sans générer de cas de tests. Elle déduit les informations sur le comportement du logiciel en se basant sur un « modèle », le but étant d'extraire du code des informations sémantiques (chemins, valeurs possibles de variables, …), et de les utiliser pour découvrir des défauts potentiels.

Un des avantages majeurs de l'analyse statique avancée est sa capacité d'automatisation et d'analyse d'un nombre bien plus important de chemins d'exécutions. Ainsi, certains problèmes logiciels pouvant mener à de sévères défaillances ou failles de sécurité, comme les erreurs « Runtime », les dépassements de mémoire, déréférencements de pointeurs nuls, divisions par zéro, fuites mémoires, injections de code, …, peuvent se détecter bien plus facilement en analyse statique avancée qu'en analyse dynamique.

Principes de modélisation

Pour analyser l'ensemble des chemins d'exécutions possibles au sein d'un code, l'analyse statique avancée crée tout d'abord un graphe d'appels, listant l'ensemble des appels entre fonctions de code au sein d'un projet logiciel. La seconde étape consiste à rentrer dans le détail de chaque fonction de code, au travers d'un graphe de flots de contrôle. Les graphes d'appels et de flots de contrôle facilitent la modélisation des chemins d'exécution, permettant

de remonter un chemin lorsqu'une construction connue comme dangereuse est détectée, comme par exemple une division. Les graphes d'appels et de flots de contrôle n'analysant pas les variables et leurs valeurs, ils sont souvent couplés avec les arbres syntaxiques abstraits (*abstract syntax tree* ou *AST*) afin de détecter des non initialisations, fuites mémoires, …

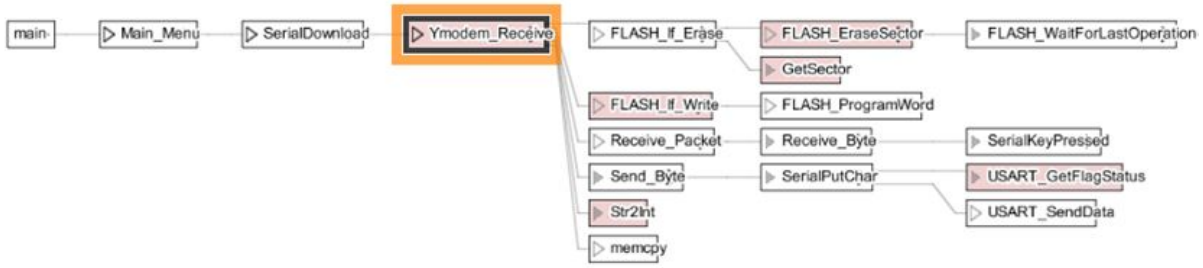


Illustration 31 : Arbre Syntax Tree,
Source : ISIT

À partir de l'analyse des graphes d'appels et de flots de contrôle, ainsi que des arbres syntaxiques abstraits, il est possible de détecter des chemins menant à des erreurs critiques ainsi qu'à des vulnérabilités potentielles.

Un autre avantage de l'analyse statique est qu'elle peut intervenir à n'importe quel moment d'un projet, y compris tout à la fin des développements (même s'il est naturellement préférable de mener l'analyse au fur et à mesure du développement), et qu'elle est très peu intrusive dans le processus de développement lui-même.
Plusieurs outils existent sur le marché, permettant de procéder à des analyses statiques de façon automatisée, sur du code source naturellement, mais aussi pour certains outils sur les librairies et sur même dans certains cas sur des codes binaires tierces.

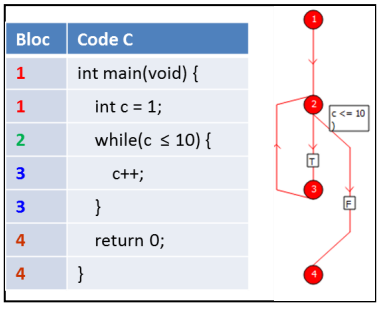


Illustration 32 : Analyse statique,
Source : ISIT

"Cybersécuriser" son Produit

Des mécanismes de protection peuvent également être intégrés dans le produit lors de sa conception et déployés avec le produit. Selon le degré de protection souhaité, la criticité du produit et ses fonctionnalités, les points suivants seront à prendre en compte :

- Protéger les communications, par exemple cryptage
- Sécuriser le cycle de démarrage (secure boot) et les mises à jour (secure update)
- Implémenter un firewall / filtrer les connexions
- Protéger/contrôler l'accès physique à l'équipement (login, mot de passe)

Il existe aujourd'hui différentes solutions (gratuites ou commerciales) permettant d'implémenter ce type de mécanisme. Le choix devra être guidé par la fiabilité de la source et la qualité du développement proposé. Certains composants intègrent même certains de ces mécanismes directement dans le silicium.

7.5.3 Surveiller le système (en fonctionnement)

La seule protection du système par une conception sécurisée ne suffit pas lorsque l'équipement est déployé : l'environnement de fonctionnement est divers et souvent inconnu du concepteur, et les menaces évoluent constamment.
Dans ce contexte, être à même de détecter des tentatives d'intrusions apporte un niveau de sécurisation complémentaire. Comme fonctions de surveillance pertinentes on peut citer :

- Détecter / Signaler les intrusions et tentatives d'intrusions
- Gérer et remonter les alertes (journaux d'événements), intégration aux SIEM (Security Information and Event Management)
- Authentifier/contrôler les accès à distance (certificats, gestion des clés)
- Gérer les données collectées et transmises

Les attaques correspondent souvent à des fonctionnements anormaux ou imprévus. Par exemple, des tentatives insistantes de connexion, des essais de détournement de fonctionnalités, des contacts non authentifiés répétés… Si l'ajout d'un firewall permet de protéger les accès, l'utilisation de fonctions de détection et de signalement des intrusions vont permettre d'alerter l'utilisateur ou le contrôleur afin de lui permettre de réagir avant que l'attaquant ait pu mettre sa menace à l'œuvre. Dans le prolongement, enregistrer les alertes dans des journaux d'évènements, éventuellement intégré à un système de gestion d'évènements et d'information sécuritaires (SIEM), renforce la protection en gardant un historique et permettra le cas échéant de démontrer les mesures prises en réaction aux attaques.

Utiliser des PKI dans l'IoT : L'authentification permet à un équipement de s'assurer que le système avec lequel il communique est légitime et de connaître les opérations qu'il est autorisé à effectuer.
Bon nombre de systèmes IoT actuels utilisent déjà des systèmes d'authentification, mais bien souvent basés sur le simple échange de login et de mot de passe ou de clés de sécurité prédéfinies.
Ces approches sont assez limitées, très vulnérables aux attaques « brutes » par des méthodes d'itération ou le biais de dictionnaires, et elles ne disposent pas de mécanisme pour détecter si les informations ont été volées.

<u>L'authentification Forte pour les équipements IoT</u>

Pour être efficace, tout système d'authentification pour l'IoT doit donc aller au-delà. La solution est de lier ces informations d'authentification à une identité propre à chaque équipement. Non seulement l'équipement doit exiger les bonnes informations (mot de passe et nom d'utilisateur, clé d'authentification, etc.), mais il doit pouvoir vérifier que ces informations sont bien associées à l'appareil les utilisant, tous ces échanges étant faits de manière sécurisée. Ces informations d'authentification ne doivent pas être faciles à voler ou

à cloner, et la distribution, la vérification et la révocation des données d'authentification doivent être automatisées et faciles à gérer.

Utilisation des PKI pour les équipements IoT

Basés sur un mécanisme de certificats numériques, les PKI correspondent à un ensemble de technologies et de services pour la gestion de l'authentification d'un système informatique.

En prouvant l'identité des machines, ils assurent la légitimité et l'intégrité de la transaction des données pouvant être vitales. Le PKI fourni permet l'émission des certificats sur tous les périphériques IoT d'un réseau et leur gestion tout au long du cycle de vie des équipements.

Émis par une autorité de confiance (Autorité de Certification), un certificat numérique, contient des autorisations et permet d'identifier le détenteur du certificat. L'identification repose sur la notion de clés publiques & privées, permettant de vérifier que le détenteur du certificat est bien l'entité spécifiée par le certificat. Le résultat est qu'un appareil peut vérifier, avec certitude, que le détenteur du certificat PKI est réellement celui qu'il prétend être et non un imposteur.

Solutions PKI pour l'IoT

Pour l'IoT, l'authentification mutuelle est obligatoire, les périphériques communiquant doivent se valider les uns avec les autres.

L'authentification mutuelle nécessite que chaque système embarqué possède un certificat qui puisse évoluer en cas d'attaque ou de compromission avérée. De ce fait, et au vu de l'explosion du nombre d'objets, les certificats numériques dans l'IoT doivent pouvoir éliminer toute interaction humaine.

Il existe aujourd'hui sur le marché quelques solutions permettant aux objets de demander automatiquement et en toute sécurité de nouveaux certificats, de les valider et de reconnaître les certificats révoqués. Ces solutions prend également en charge le chaînage de certificats pour s'assurer que l'ensemble des certificats est valide.

De telles solutions doivent aussi permettre la gestion des certificats sur l'ensemble du cycle de vie du système. Cela commence avec l'enregistrement des certificats dans l'appareil pendant la fabrication empêchant ainsi la contrefaçon et le clonage. Vient ensuite le processus de déploiement au cours duquel l'équipement est validé automatiquement, à l'aide du certificat installé lors de la fabrication, et un nouveau certificat est publié pour une utilisation sur le réseau. Ce certificat pourra être révoqué ultérieurement lorsque l'appareil sera mis hors service interdisant toute ré-utilisation frauduleuse.

L'utilisation des certificats est d'autant plus utile que les systèmes sont critiques. En assurant l'authentification mutuelle, les PKI fournissent le socle pour assurer l'intégrité des données utilisées, permettant ainsi de créer de nouveaux modèles économiques, d'augmenter l'efficacité opérationnelle, et au final de réellement tirer profit de l'avènement de l'IoT.

La gestion sécurisée des données

Avec l'augmentation de leur volume et de leur valeur marchande potentielle, les données d'un équipement embarqué sont aujourd'hui devenues cruciales. L'IoT permettant l'émergence de nouveaux services et de nouveaux marchés, intégrer et maîtriser la gestion des données devient un choix stratégique où toute erreur de casting peut avoir de lourdes répercussions, car cette gestion doit répondre à plusieurs exigences : être adaptée au matériel (CPUs) utilisé, permettre éventuellement le traitement des données en local, être évolutive pour répondre à de nouveaux besoins, etc.

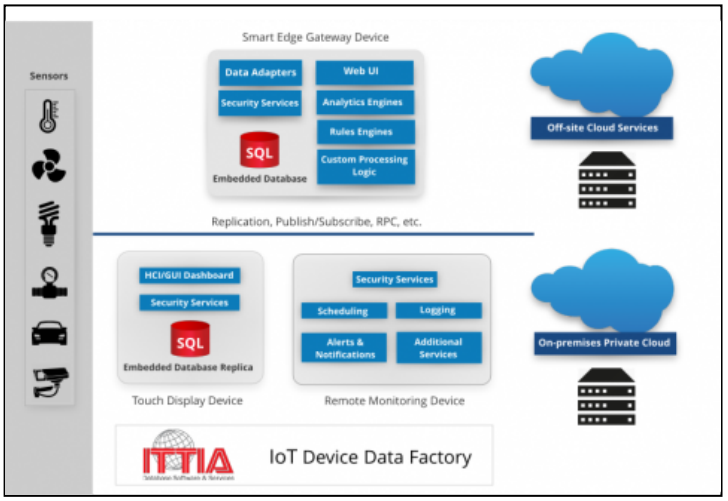


Illustration 33 : ITTIA,
Source : http://www.ittia.com/

Bâtir un tel système de gestion de données nécessite d'intégrer diverses technologies comme, entre autres, le système de gestion des données lui-même (base de données) et les moyens de distribution de ces données vers les autres systèmes. Pour implémenter tout cela, plusieurs approches existent, comme bâtir son propre système de gestion ou utiliser des briques existantes (type Open Source), en prenant en charge l'aspect sécuritaire. Mais il existe aussi des solutions commerciales, apportant les outils et l'expertise, et qui peuvent avoir l'avantage d'intégrer un ensemble de services assurant la distribution des données en toutes sécurité. Comme souvent, il faut évaluer le compromis entre le coût d'une solution commerciale, et le risque de développement de déploiement d'une option « maison ».

"Cybersécuriser" la production :

Une dernière étape devra aussi être analysée, selon le mode de production envisagé. En effet, une fois le nouveau produit connecté totalement fiabilisé, reste à s'assurer que la production ne permettra pas d'introduire des failles ou de contourner les sécurités mises en place à la conception, notamment si la production est sous traitée et a fortiori si la sous-traitance est effectuée à l'étranger, sans contrôle direct du sous-traitant.

Illustration 34 : FlashRunner ATE,
Source : https://www.iss.se/

De nouvelles fonctions sont ainsi intégrées dans les équipements de programmation destinés à la production pour compléter cet arsenal :

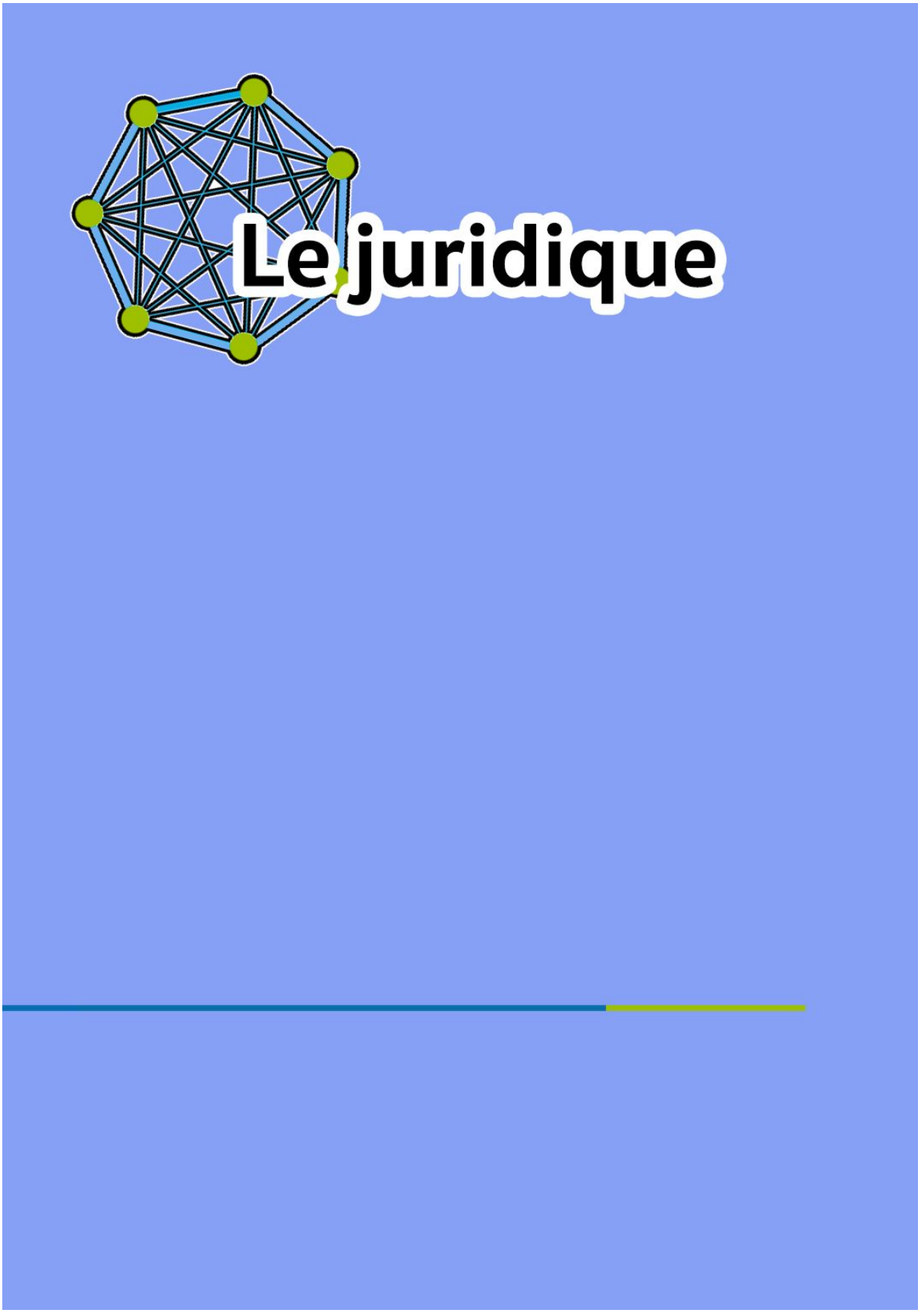
- Contrôle régulier du contenu qui est programmé, évitant des modifications voire de simples altérations lors de transferts de données
- Cryptage/décryptage du contenu, sous le seul contrôle du concepteur
- Décompte précis du nombre d'unités produites pour éviter des productions parallèles
- Contrôle de l'opérateur, et des opérations autorisées à chaque opérateur

7.5.4 Conclusion

Certes la conception de logiciels embarqués sécurisés est complexe et demande de la rigueur, mais elle est une nécessité si une entreprise veut se développer sereinement sur le marché prometteur de l'objet connecté.

Laissons la conclusion à l'étude Gartner citée en début de chapitre : *L'absence de « sécurité par conception »* vient d'un manque de réglementations spécifiques et strictes. À l'avenir, Gartner s'attend à ce que cette tendance change, en particulier dans les industries fortement réglementées telles que la santé et l'automobile.

D'ici 2021, Gartner prédit que la conformité réglementaire deviendra le principal facteur d'adoption de la sécurité de l'IoT. Les industries devant se conformer à la réglementation et aux lignes directrices visant à améliorer la protection des infrastructures critiques et seront obligées de mettre davantage l'accent sur la sécurité du fait que l'Internet des objets imprègne le monde industriel.



8. Juridique

Les objets connectés fascinent le monde des juristes, car leur utilisation laisse présager une multiplication de risques juridiques, et donc de contentieux judiciaires. L'une des problématiques les plus évidentes réside dans la manipulation des données collectées et qui transitent par des ondes, courtes, wifi, ou Bluetooth.

L'autre problématique est la responsabilité en cas de mauvaise utilisation, ou d'une programmation entièrement automatisée qui se réalise de manière incorrecte, ou encore d'une interception frauduleuse.

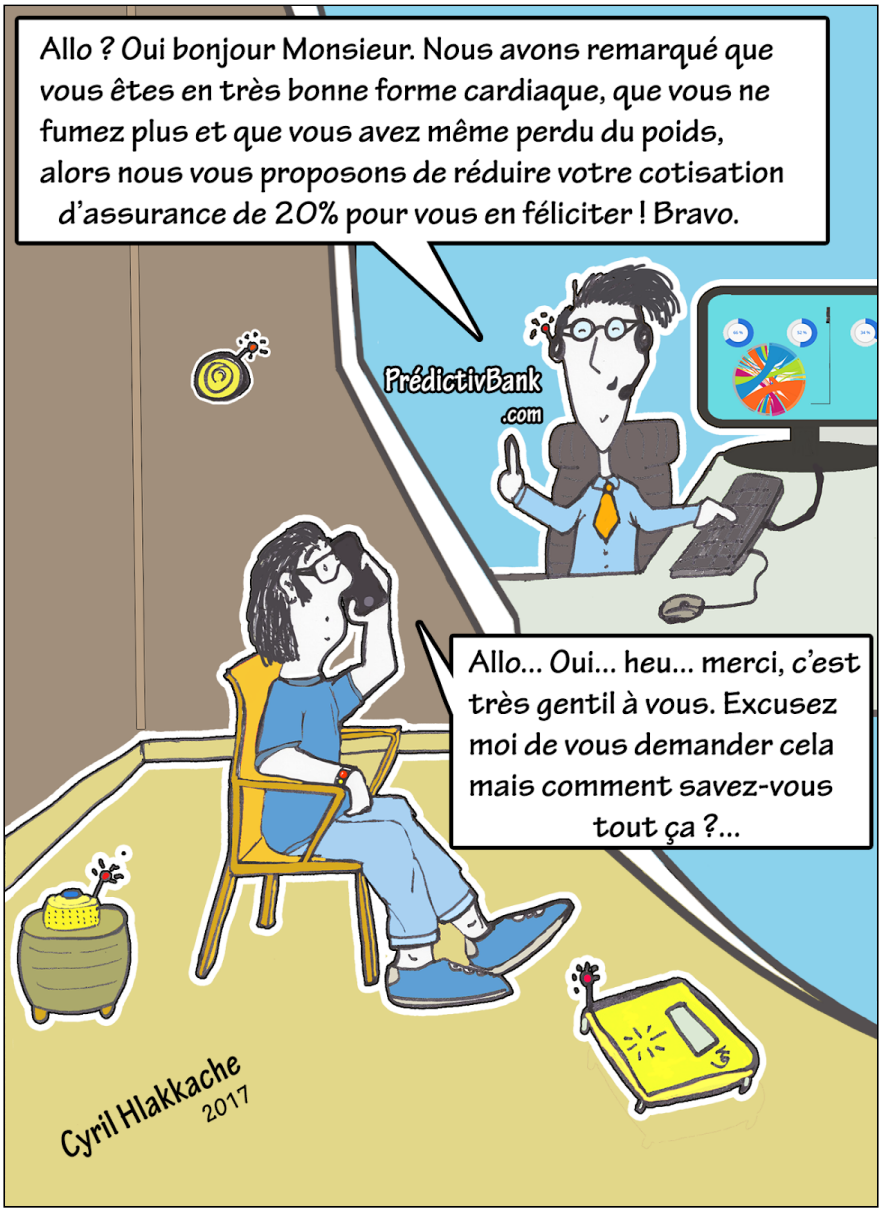


Illustration 35 : "Partage de vie privée" par Cyril Hlakkache - 2017

8.1 La protection juridique relatives aux données

Les objets et applications connectés impliquent dans la grande majorité des cas le traitement de données qui se rapportent à des personnes physiques identifiées ou identifiables.

En tant que tel, ce sont des traitements de données à caractère personnel dont la définition a été étendue par **l'article 2 du Règlement Général sur la Protection des Données** (ou RGPD).

Un objet connecté, suivant l'usage qu'on lui réserve, peut permettre à son utilisateur de se tenir informé de l'évolution de suivre ses progrès sportifs, de bénéficier d'une surveillance à distance, ou plus simplement de bénéficier d'une assistance technique depuis son véhicule. Ce suivi régulier permet la collecte, l'analyse et l'observation des mesures très précises d'une personne : mesures biométriques, mesures relatives à ses habitudes de vie, et consommation, etc…

Ces mesures sont des caractéristiques propres à chaque individu et permettent de le rendre identifiable dans un groupe de personnes.

Ainsi des mesures appropriées de sécurité doivent être prise, mais également la mise en œuvre des principes de *privacy by default.* Il convient donc, dès le départ, de s'enquérir si toutes les données recueillies sont pertinentes et adéquates pour l'objectif poursuivi (article 5).

La diversité des objets connectés, dans leur usage, et dans les données collectées, a conduit la CNIL à se doter de packs de conformité. Deux d'entre eux intéressent plus particulièrement les objets connectés au moment de l'entrée en vigueur du Règlement relatif à la Protection des données (§2 et §3).

8.1.1. Ce qui change avec le RGPD : des notions applicables aux IoT

Le Règlement Général relatif à la Protection des Données est plus qu'une norme à respecter, il devient une philosophie à adopter. Les principes directeurs applicables au droit de la responsabilité sont les principes de « Protection des données dès la conception » ou « Privacy by default » et « Protection des données par défaut » ou « Security by design ».
Ces deux principes imposent une ligne de conduite dans la gestion de projet d'un Traitement, de la conception, à la suppression de ce Traitement. Ces lignes de conduites sont déclinées en droit et obligation tout au long du RGPD.
Cela s'accompagne d'une libéralisation des possibilités de créer ou de gérer un Traitement, sous réserve de respecter les principes fondamentaux des articles 5 et 6.

Plus particulièrement, il conviendra de retenir les principes de :

- licéité, loyauté, transparence du Responsable de Traitement à l'égard de la personne concernée
- adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités des données recueillies
- niveau de sécurité approprié des traitements
- consentement éclairé de la personne concernée, cela implique un dispositif spécifique lorsqu'elle est en situation de faiblesse
- l'obligation d'un fondement légal autorisant ou justifiant l'existence du Traitement : contrat, consentement spécifique, obligation légale, sauvegarde des intérêts vitaux, mission d'intérêt public ou l'intérêt légitime du Responsable du Traitement.

Ces principes sont désormais applicables à des Traitements incluant des données à caractère personnel dont la définition a été considérablement élargie.

L'article 4 nous propose 4 typologies de définitions :

- **«données à caractère personnel»,** toute information se rapportant à une personne physique **identifiée ou identifiable** (ci-après dénommée «personne concernée») ;
    - est réputée être une **«personne physique identifiable»** une personne physique qui peut être identifiée, directement ou indirectement,
    - **notamment par référence à un identifiant,** tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne**, ou à un ou plusieurs éléments spécifiques propres** à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

C'est ainsi que les données personnelles pseudonymisées sont considérées comme des données personnelles à protéger.

- **«données génétiques»,** les données à caractère personnel relatives aux **caractéristiques génétiques héréditaires ou acquises** d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question ;
- **«données biométriques»,** les données à caractère personnel résultant d'un **traitement technique spécifique**, relatives **aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique**, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques ;
- **«données concernant la santé»,** les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne;

Dès lors le champ d'application du RGPD impacte directement les objets connectés, et les « *quantified self »*. Ce sont l'ensemble des applications et objets connectés qui permettent de de mesurer et de comparer avec d'autres personnes des variables relatives à son mode de vie : nutrition, activités physiques, poids, sommeil…

Il impacte également toutes les données issues de dispositifs communiquant ayant pour objet de prélever ou de collecter des informations relatives aux habitudes de vie, tel que les compteurs communicants, et les véhicules connectés.

Plus largement, le RGPD bouscule le niveau le niveau de responsabilité de chacun des acteurs. En effet, le RGPD impose un **principe de responsabilité conjointe (art. 26)** entre tous les responsables de traitement.

« Lorsque deux responsables du traitement ou plus **déterminent conjointement** les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement (…) »

Cela signifie que toutes les personnes qui auront **l'initiative de la collecte** et du traitement des données seront responsables au même degré à l'égard de la personne auprès de laquelle les données seront collectées.

Ce système de responsabilité conjointe s'étend également aux Sous-Traitants issus du principe posé par l'article 35 de la Loi I&L concernant la sous-traitance, principe selon lequel : « **Le responsable de traitement a pour obligation d'assurer la sécurité et la confidentialité des données à caractère personnel de ses clients et prospects et qu'elle ne saurait minimiser sa responsabilité par le recours à plusieurs prestataires.** »

Ce principe est repris dans le RGPD, par l'article 28-1, notamment en ce qu'il énonce que : **« Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée »**

De sorte que les sous-traitants successifs se trouvent co-responsables de la sécurité des Traitements qu'ils gèrent pour le compte du Responsable, au même titre que lui. Cela implique que les sanctions encourues, qui ont été largement alourdies par le RGPD, lui sont directement applicable.

Le fait que la personne puisse actionner elle-même le dispositif, par une action physique, ne signifie pas forcément qu'elle a accepté l'ensemble des finalités et usages que l'objet connecté va opérer sur ses données. Cela ne la rend pas non plus Responsable du traitement.

La difficulté dans la gestion de la collecte sera principalement d'informer correctement la personne concernée des finalités, et de faire le suivi de l'évolution de ces finalités.
En effet, le Règlement impose désormais que le recueil du consentement soit effectué dès que la finalité évolue.

Par ailleurs, le RGPD introduit une nouveauté : à savoir la possibilité de **retirer son consentement à tout moment, ou de geler l'utilisation de ses données.** Dans les deux cas, le Responsable du Traitement doit assurer que les données de l'utilisateur ont été « isolées » du traitement et qu'on leur a appliqué les mesures nécessaires.

Enfin, compte tenu du volume de données collectées, et de leur caractère sensible, il conviendra d'effectuer une **Analyse d'impact relative à la protection des données** (Article 35).

8.1.2. Le Pack Véhicules connectés et Données Personnelles (Ed. Oct. 2017)

Dès l'introduction du Pack, la CNIL précise le périmètre des véhicules connectés soumis à ces lignes directrices : « aux véhicules connectés, c'est-à-dire aux véhicules qui communiquent avec l'extérieur ».

L'objectif de ce pack est de donner un cadre juridique clair de l'ensemble des traitements de données personnelles transmises depuis une voiture connectée.
En effet, l'apport principal de ce pack est la détermination des catégories de données considérées comme des données personnelles et soumises à la Loi.

Pour mémoire, « Constitue une **donnée à caractère personnel** toute information relative à une personne physique identifiée ou identifiable, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. »

Ainsi, les données personnelles concernées **directement identifiantes** sont toutes les données qui, seules ou combinées entre elles, peuvent être rattachées à un usager identifié ou identifiable, notamment *via* le numéro de série du véhicule ou le numéro de la plaque d'immatriculation, que ce soit par le responsable de traitement ou par toute autre personne.

Par ailleurs, les données **indirectement identifiantes** sont des données à caractère personnel les données relatives aux trajets effectués, **à l'état d'usure des pièces**, aux **dates des contrôles techniques**, au nombre de kilomètres, ou au style de conduite, dans la mesure où elles sont susceptibles d'être rattachées à une personne physique, notamment *via* le numéro de série du véhicule et le numéro de la plaque d'immatriculation, par le responsable de traitement ou par toute autre personne. **Les données personnelles ne sont donc pas uniquement les données nominatives (nom et prénom).**

Le deuxième apport de ce pack consiste en l'analyse qui est faite de **la désignation du responsable de traitement d'un véhicule connecté.** En effet, une étude rapide d'un cas pourrait conduire à désigner le constructeur du véhicule comme responsable de traitement. Mais pour la CNIL, le responsable de traitement est « **le fournisseur de services** qui traite les données du véhicule pour adresser au conducteur des messages d'info-trafic, d'éco-conduite ou des alertes sur le fonctionnement du véhicule. »

Le paradigme est donc bien du point de vue des données personnelles, et non du constructeur/ vendeur du véhicule connecté.

Ainsi, le Pack apporte des solutions par l'étude 3 cas.

Scénario n°1 : les données du véhicule ne sont pas transmises au fournisseur de services
A cette occasion la CNIL précise la notion de « **maîtrise par l'usager de ses données** » :

- que les données personnelles ne soient pas transmises au fournisseur de services ;
- la désactivation par défaut, au démarrage du véhicule, de la collecte en local des données de géolocalisation et des données relatives aux infractions, sauf en cas de traitement des données en temps réel ;
- la possibilité de désactiver à tout moment les fonctionnalités concernées, à l'exclusion des fonctionnalités strictement nécessaires au fonctionnement du véhicule
- en l'absence d'un traitement en temps réel, la possibilité d'accéder et de supprimer aisément l'historique de ses données d'usage (*via* par exemple, un bouton à l'intérieur du véhicule et / ou *via* son ordiphone et / ou ordinateur de bord) ;
- l'information de l'usager des données susceptibles d'être conservées en local, des finalités du traitement, ainsi que de la possibilité d'effacer les données.

Ainsi lorsque l'usager maîtrise complètement ses données, et qu'il n'y a aucune transmission de celles-ci au fournisseur de service, par application de l'article 2-2° c/ du Règlement, les traitements mis en œuvre **ne sont pas soumis à la Réglementation.**
Il convient toutefois de s'assurer qu'aucune transmission pour stockage ne soit possible, que l'usager puisse détruire à tout moment ses données, et que la sécurité de ces données soient maximales (chiffrement, etc…).

Scénario n°2 : les données du véhicule sont transmises au fournisseur de services, sans déclencher à distance d'action automatique dans le véhicule
Ce scénario couvre les cas dans lesquels « les données collectées sont transmises au fournisseur de services afin de fournir un service à valeur ajoutée à l'usager ou améliorer les produits ». Il s'agit par exemple d'un service d'assistance.
Pour ce scénario, la CNIL envisage 5 finalités, sans que cela ne soit limitatif : optimisation de modèles, études d'accidentologie, exploitation commerciale des données, e-call d'urgences, lutte contre le vol.
Ce scénario est à rapprocher, sur de nombreux points, du scénario n°3. Pour le détail de la mise en place de la protection des données personnelles en fonction des finalités traitées, nous renvoyons au document complet.

Scénario n°3 : les données sont transmises au fournisseur de services pour déclencher à distance une action automatique dans le véhicule
Ce scénario couvre les cas dans lesquels « les données sont transmises au fournisseur de services pour déclencher à distance une action automatique dans le véhicule »
Pour ce scénario, la CNIL envisage 2 finalités, sans que cela ne soit limitatif : maintenance à distance, amélioration de l'expérience conduite.
Dans ces deux scenarii, la CNIL préconise une information renforcée des usagers concernant les finalités, et les personnes destinataires des données. Elle préconise

également que les données soient traitées dans le véhicule, afin que les données brutes ne soient transmises.

A cette occasion le CNIL rappelle que le **consentement** doit être donné de manière libre et éclairé : « **Dans le cas où le fournisseur de services est le constructeur automobile**, le consentement devra être recueilli lors de la signature du **contrat de prestation, qui devra être distinct du contrat de vente du véhicule.** La vente du véhicule ne saurait être subordonnée à la signature du contrat de prestation et à l'acceptation de la collecte des données du véhicule par le constructeur automobile. »

Par ailleurs, le respect du droit des personnes concernées implique que le **paramétrage des applications** soit :

- par défaut protecteur de la vie privée,
- aisément modifiables, ou activable/ désactivable,
- aisément ajustable d'un point de vue de la granularité des données concernées par rapport au service fourni
- aisément accessible.

Enfin, en terme de sécurité, la CNIL fixe des objectifs claires pour le fournisseur de services, qui « doit mettre en place des mesures permettant de garantir la sécurité et la confidentialité des données qu'il traite et doit prendre toutes les précautions utiles pour en empêcher la prise de contrôle par une personne non autorisée », notamment en :

- chiffrant le canal de communication avec un algorithme à l'état de l'art ;
- mettant en place une gestion des clés de chiffrement propre à chaque véhicule et non à chaque modèle ;
- chiffrant les données en base avec des algorithmes à l'état de l'art ;
- protégeant les clés de chiffrement de toute divulgation accidentelle ;
- authentifiant les appareils destinataires des données ;
- s'assurant de l'intégrité des données (par exemple par calcul d'empreinte) ;
- subordonnant l'accès aux données personnelles à une authentification fiable de l'utilisateur (mot de passe, certificat électronique, etc.) ;
- appliquant les recommandations de la Commission en date du 22 juin 2017, dans le cas d'une authentification par mot de passe (voir délibération n° 2017-190).

Concernant plus spécifiquement les constructeurs automobiles, la CNIL recommande la mise en place des mesures de sécurité suivantes :

- le cloisonnement des fonctions vitales du véhicule par rapport à celles connectées en continu à Internet (« infotainment » par exemple) ;
- la mise en place de mesures techniques permettant de corriger rapidement un défaut de sécurité ;
- pour les fonctions vitales du véhicule, privilégier, autant que possible, le recours à des fréquences sécurisées spécifiquement dédiées aux transports ;
- la mise en place d'un système d'alerte en cas d'attaque et la possibilité d'un fonctionnement en mode dégradé ;
- la conservation d'un historique de logs d'une durée de six mois aux fins de permettre de comprendre l'origine de l'attaque.

Enfin la CNIL rappelle que « les mesures mises en place doivent être adaptées au niveau de sensibilité des données. » Des préconisations renforcées sont faites en cas de collecte de la vitesse instantanée dans le cadre d'études d'accidentologie

Dans ces deux scenarii, la CNIL recommande enfin de réaliser des Analyses d'impact, telles qu'elles sont prévues par l'article 35 du RGPD.

8.1.3. Le Pack Silver Economie et Données personnelles (Ed. Nov. 2017)

Le Pack Silver Economie et Données personnelles a pour objet d'aborder les thématiques des objets connectés, produits ou applications, qui ont pour effet :

- « d'apporter plus de confort et de sécurité aux seniors « actifs » et/ou « fragilisés » et/ou « dépendants » en raison de leur âge, de leur état de santé ou d'un handicap en vue de prévenir leur perte d'autonomie ou de les accompagner dans l'entrée en dépendance ;
- d'intervenir auprès de la personne concernée en cas de besoin. »

Le Pack a pour ambition de permettre une meilleure lisibilité des droits et obligations en matière d'objets connectés recueillant des données sensibles telles que les données de santé, ou les données biométriques. Il est donc possible d'étendre le dispositif de ce Pack à toutes les activités liées au m-santé et quantified self.
Les activités ayant pour base des données de santé ont des obligations renforcées en terme de licéité du traitement, et de formalité à réaliser (registre, Analyse d'impact), mais également en matière de sécurité de l'hébergement des données de santé (article L1111-8 du code de la santé publique, et l'ordonnance n°2017-27 du 12 janvier 2017 relative à l'hébergement des données à caractère personnel).

Comme précédemment, le Pack aborde la thématique par l'étude de 3 cas.

Scénario n°1 :

Dans ce cas, les données sont traitées dans l'espace privé, via des dispositifs restant sous la maîtrise unique de la personne concernée, de ses représentants légaux ou de ses proches n'intervenant pas à titre professionnel. Sont donc exclus toutes les hypothèses où il y aurait un mandataire.

Ce scénario couvre les cas dans lesquels :

- un ou plusieurs produits ou logiciels collectent des données et communiquent éventuellement entre eux sans que les données sortent de l'espace privé ;

- les données sortent de l'espace privé sans être transmises, collectées ni réutilisées par d'autres tiers que les représentants légaux ou les proches de la personne concernée. Dans ce cas d'usage, les données :
    - restent confinées sur des réseaux de communication locaux sécurisés sous la maîtrise unique de l'utilisateur (Wi-Fi, cloud privé ou autre réseau local) ;
    - circulent sur des réseaux de télécommunications ouverts au public (notamment ADSL, fibre optique, GSM, 4G, 3G, EDGE ou GPRS) sans être stockées sur un serveur centralisé ni réutilisées à d'autres fins que la gestion du trafic par les opérateurs de communication électronique.

Par ailleurs les finalités attendues par la CNIL sont « amélioration du confort » et « prévention et renforcement de la sécurité des personnes concernées et de l'espace privé ».
Comme précédemment, l'application de l'article 2-2° c/ du RGP a pour effet d'exclure ce type de traitement de toutes obligations liées au RGPD. Toutefois, la CNIL rappelle que l'exigence **d'absence de transmission** au fournisseur de service doit être effective.
Par ailleurs elle recommande que les personnes concernées puissent définir et modifier elles-mêmes, et à tout moment, la durée de conservation des données ; l'activation, et la désactivation des services. Ces fonctionnalités doivent être adaptées à l'état de santé de la personne concernée.

Scénarii n°2 et 3 :

Dans le cas du scénario n°2, les données sont traitées dans l'espace privé et transmises à l'extérieur et ne font pas de retour. Alors que dans le cas du scénario n°3, les données font un retour vers l'équipement afin de permettre la réalisation d'une action automatique.
La Commission examine des finalités potentielles :

- « la prévention et le renforcement de la sécurité des personnes concernées et de l'espace privé » ; « le renforcement de la prévention dans le domaine de la santé » ; La Commission rappelle, dans ce type de cas, que le consentement de la personne doit être privilégié pour toute mise en place de dispositif. Lorsque le dispositif est mis en place par l'établissement de soins ou d'hébergement pour prévenir un risque tel l'errance, il est possible d'avoir une alternative au recueil du consentement par l'application d'une base légale (prévention d'une mise en danger). Mais les solutions doivent démontrer qu'elles sont les moins intrusives possibles dans la vie des personnes. Enfin, la mise en œuvre de tels dispositifs permettant de localiser les résidents ne doit pas être justifier par le manque de personnels surveillants, et doit être limitée à la surveillance de résidents réellement sujets à des risques d'errance ou de fugue ou par la proximité d'un danger. La pertinence de la mise en œuvre doit faire l'objet d'une analyse au cas par cas.
- « la prospection commerciale » ; enfin « l'optimisation des modèles, l'amélioration des produits ou logiciels, l'élaboration de statistiques ». Dans ces cas, le recueil du consentement de la personne demeure obligatoire.

Dans tous les cas, la Commission rappelle que les personnes concernées devront pouvoir modifier aisément les paramétrages des dispositifs, afin notamment d'activer ou désactiver certains services tels que la géolocalisation (voir ci-dessus).

Ce Pack est l'occasion pour la CNIL de rappeler la nécessité pour les fournisseurs de services **de prévoir des solutions adaptées à l'état des personnes ciblées**, dès la conception des dispositifs, afin que ces dernières puissent en avoir **une maîtrise effective,** par exemple, en permettant à des résidents au sein d'un établissement d'hébergement ou de soin d'être accompagnées par un auxiliaire de vie spécifiquement formé à ces usages. En tout état de cause, lorsqu'un responsable du traitement ou un sous-traitant récupère un dispositif qui n'a pas vocation à être réutilisé par la personne concernée, ces derniers doivent supprimer les données contenues dans ce dispositif, voire détruire le dispositif, par exemple, pour les produits en fin de vie.

Enfin la CNIL estime que la nature sensible des données issues de type de dispositif, quel qu'en soient les finalités, soumettent le Responsable du traitement, et ses sous-traitants, aux obligations les plus dures du RGPD : la tenue d'un registre, la désignation d'un Délégué à la Protection des Données, des Analyses d'impact, un niveau d'information élevé à fournir aux personnes concernées, et enfin à un niveau de sécurité maximale, dont l'anonymisation systématique dès qu'il n'est plus pertinent de conserver une donnée « en clair ».

8.2 La responsabilité du fait des objets connectés

La recherche d'une responsabilité dans le cadre d'un dysfonctionnement d'un objet connecté conduit à s'interroger sur la part de décision que l'objet connecté a pris dans le dysfonctionnement. De la responsabilité à l'éthique, la frontière est mince.

Actuellement en débat, la question du statut juridique du robot dans la chaîne des responsabilités est discutée devant le Parlement Européen.

L'objet connecté est une version simplifiée du robot. Mais la détermination du cadre juridique applicable conduit également à préciser les typologies de cas dans lesquels les objets connectés pourraient être générateur d'une responsabilité.

Scénario n°1 : le traitement des données est réalisé par l'objet connecté, en simultané. La transmission des données au fournisseur de services n'a pas d'effet sur la réalisation du service.

Dans ce cas, les données restent sous la maîtrise seule de l'utilisateur : il a la maîtrise d'actionner ou de désactiver la fonctionnalité. Il s'agit des cas où l'utilisateur a le choix de donner une importance dans sa décision à l'information qui va être fournie. Il s'agit d'une hypothèse très courante, à laquelle chacun se trouve confronté depuis plusieurs décennies.

Pourtant, le développement des algorithmes d'aide à la décision, ou de conduite de véhicule automatisée, ou encore enfin des services fournis sur la base de l'intelligence artificielle, font évoluer le débat.

Dans ce cas, les données brutes sont immédiatement traitées par l'objet connecté, puis sont immédiatement restituées à l'utilisateur.
Il en est ainsi de la montre connectée qui fournit des informations sur le rythme cardiaque, ou d'une application pour retrouver sa voiture. En réalité, le dysfonctionnement dans ce cas ne provient pas des données elles-mêmes, mais du capteur physique d'une part, et de l'algorithme qui les traite d'autre part, soit ensemble, soit séparément.

Juridiquement, l'objet connecté reste sous la garde de celui qui l'utilise, et/ ou qui en est le propriétaire. Cette analyse est confirmée par le fait que les données demeurent en possession de l'utilisateur, et qu'il en est seul Responsable au sens du RGPD. De manière complémentaire, la responsabilité civile régi par l'article 1242 du code civil s'applique : « On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore (…) des choses que l'on a sous sa garde ». En d'autres termes, l'utilisateur serait seul responsable de la défaillance de l'objet connecté, ou d'une mauvaise décision liée à une information erronée fournie par l'objet.

Il convient de préciser que les fabricants sont responsables du fait des produits défectueux (article 1245 du code civil). Mais ce régime de responsabilité ne s'applique pas aux logiciels d'aide à la décision, ni aux logiciels embarqués dans un objet, ni même aux algorithmes. Il ne concerne que l'objet lui-même, incluant les capteurs.

Lorsque la défaillance provient d'une erreur dans l'algorithme ou le code du logiciel traitant les données, en fonction de la typologie des objets, il conviendra d'appliquer les règles classiques de la responsabilité civile. S'il existe un contrat entre l'utilisateur et le fournisseur de services, tel qu'un contrat de fourniture de service, ou de maintenance, la responsabilité contractuelle s'appliquera.

Dans cette hypothèse, l'utilisateur qui serait victime d'une défaillance de l'objet connecté ou de son algorithme, devra rapporter la preuve de la faute du fournisseur de services, et la preuve concomitante que son action n'est pas à l'origine du dysfonctionnement s'il veut obtenir une indemnisation totale.
Cette preuve devra démontrer que l'algorithme n'a pas été correctement conçu dès l'origine. La difficulté dans ce cas réside dans les logiciels d'intelligence artificielle qui apprennent au fur et à mesure qu'ils enregistrent de données, et que des commandes sont actionnées. S'il est relativement concevable d'analyser un code informatique statique, il sera sûrement beaucoup plus difficile d'analyser l'historique d'un code informatique qui évolue seul.

Enfin, si l'algorithme inclus le profilage de l'utilisateur, alors le prestataire de service devra l'en informer en amont.
Sur la base de l'article 4 du RGPD, la doctrine de la Commission Européenne a dégagé des critères pour déterminer l'existence d'un profilage :

- un traitement automatisé ;
- un traitement qui porte sur des données personnelles ;
- un traitement dont l'objectif est d'évaluer les aspects personnels d'une personne physique, notamment pour analyser ou prédire des éléments tel que le comportement, la localisation ou les déplacements de l'utilisateur

Dans ce cas, l'utilisateur a le droit d'être informé de l'existence de ce type d'algorithme, et a le droit de s'y opposer. Le fournisseur de services qui prive l'utilisateur de ce droit s'expose à de lourdes sanctions financières.

C'est ainsi que le paradigme a considérablement évolué. Certains préconisent dès lors que les robots incluant des logiciels d'intelligence artificielle, et donc une certaine autonomie, puisse bénéficier d'un statut juridique distinct. Mais les conséquences de l'adoption d'un tel régime sont encore à l'étude par la Commission Européenne.

Dans le cas où les données sont traitées dans l'espace privé et transmises à l'extérieur, mais ne font pas de retour vers l'objet connecté, alors elles appartiennent au fournisseur de services qui en est Responsable au sens du RGPD.
Ainsi, en cas de perte des données, ou d'une mauvaise utilisation, par le fournisseur de services, seul ce dernier demeure seul responsable, tant à l'égard de l'utilisateur, que de la CNIL, conformément au RGPD.

Scénario n°2 : les données sont transmises au fournisseur de services, puis font un retour vers l'équipement déclenchant à distance une action automatique.

Dans le cas du scénario n°2, les données brutes recueillies par l'objet connecté sont traitées à distance, et reviennent vers l'objet afin de réaliser une action automatique dont la commande a été donnée à distance par le fournisseur de services.
Dans ce cas, la commande de l'objet connecté, ou de l'équipement, s'effectue à distance, sans visibilité ni des lieux, ni des personnes. Les informations fournies par les capteurs ne sont pas vérifiées par une personne physique.

Il est intéressant de comprendre que ce dernier cas est fondé sur l'existence d'une relation contractuelle en cours avec l'utilisateur. Ainsi, la présomption de responsabilité sur le fournisseur de services contractuellement lié à l'utilisateur est de droit. Cette responsabilité ne saurait être écartée, ni d'un point de vue éthique, ni d'un point de vue juridique.
Le fournisseur de services est prestataire, Responsable du Traitement, et est soumis au droit des contrats, et au RGPD.

Pour autant, le fournisseur de services est-il réellement responsable de l'ensemble des défaillances de son algorithme, ou des commandes qui en sont issues ? Au regard des règles du droit des contrats, sa responsabilité demeure entière. Il pourra tenter de s'exonérer en démontrant que l'utilisateur a incorrectement paramétré l'équipement, ou qu'il a eu une action disproportionnée. Mais cela aura peu d'effet car en tant que prestataire de service, il doit fournir à ses utilisateurs un niveau de service attendu avec un référentiel qualité.

L'obligation de résultat assujetti à la prestation fournie est très forte. Les mêmes règles que précédemment régissent la relation contractuelle. A notre sens, le fait que la commande actionnant automatiquement l'équipement s'effectue à distance sans la présence de l'utilisateur, renforce l'obligation de résultat qui pèse sur le fournisseur de service.
Pour l'utilisateur, la preuve à rapporter est donc moins complexe.

Enfin, des études ont révélé l'existence d'importantes failles de sécurité dans les objets connectés, rendant ainsi possible l'utilisation malveillante des données interceptées, le détournement d'une multitude de données personnelles au profit de tiers non autorisés, voire la prise de contrôle de l'objet connecté lui-même. En tant que Responsable du traitement, le fournisseur de services est soumis à une obligation de sécurisation du maniement des données issues de l'objet connecté : lors de la transmission sur les réseaux, au moment du traitement, et du stockage. La jurisprudence de la CNIL a, depuis longtemps, confirmé qu'il s'agissait d'une obligation de résultat, et non de moyen renforcé.

En conclusion, le fournisseur de services associés à un objet connecté a des obligations très lourdes concernant le traitement et la manipulation des données. Il doit être en conformité avec le Règlement européen relatif à la protection des données, et assurer une sécurité maximale des données. Enfin, l'algorithme doit pouvoir, en toute transparence, être expliqué à l'utilisateur final.

9. Véhicule connecté : L'objet connecté ultime

Le marché des objets connectés est d'une diversité sans égale, avec ses wearables, la maison connectée, la réalité virtuelle, les drones ou les nombreuses composantes de la ville intelligente. Dans la pratique, il n'est pas isolé des autres secteurs technologiques tels que les télécoms, les composants ou les services en cloud.
Un objet connecté illustre parfaitement ce principe d'innovations multifacettes : le véhicule autonome. C'est probablement l'objet connecté le plus sophistiqué qui soit et qui est à la croisée de toutes les industries du numérique. Chacun de ces domaines est une opportunité d'innovation qui donne lieu à des batailles industrielles mondiales déjà bien engagées.

Jugeons-en rapidement au travers des différentes facettes de ce marché en ébullition, qui ne devrait cependant être mature que d'ici au minimum une dizaine d'années, illustrant une bataille au long cours.

C'est d'abord un marché pour les **composants**, qu'il s'agisse de capteurs ou de processeurs. Les capteurs des véhicules autonomes comprennent en particulier les caméras comme celles de Mobileye, acquis en 2017 par Intel pour $15B, les détecteurs à ultrasons, les radars et surtout les LiDARs qui permettent de visualiser l'environnement du véhicule en 3D et à 360°. L'innovation bat son plein pour les miniaturiser et en réduire le prix avec des acteurs tels que Velodyne, LeddarTech, Quanergy ou Innoviz. Les équipementiers tels que les Français Valeo et Faurecia ou l'Allemand Bosch conçoivent de tels capteurs et les sous-systèmes associés. Le marché des processeurs embarqués dans les véhicules est dominé par Nvidia avec ses GPU de la série Xavier qui sont intégrés dans ses cartes Drive PX. Il est talonné par Intel et Qualcomm.

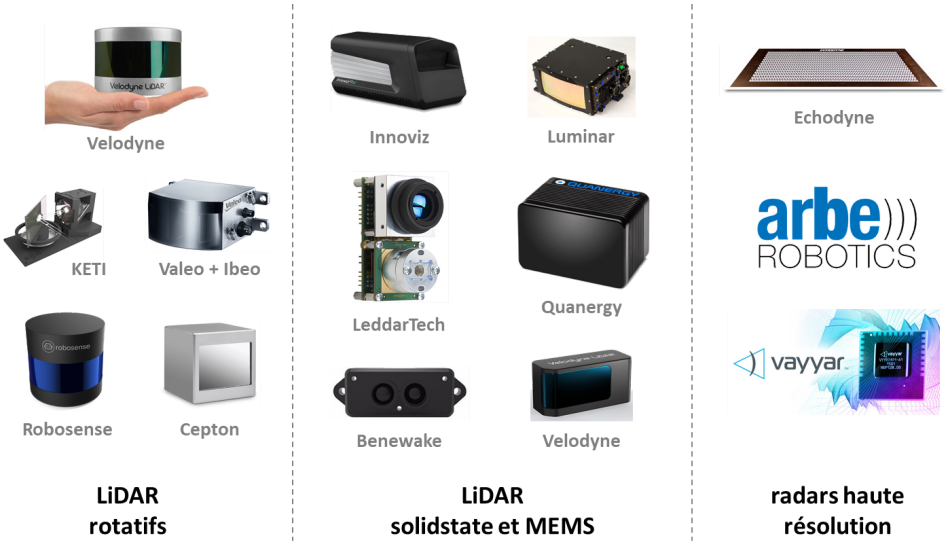


Illustration 36 : LiDARs et radars haute résolution,
Source : Olivier Ezratty

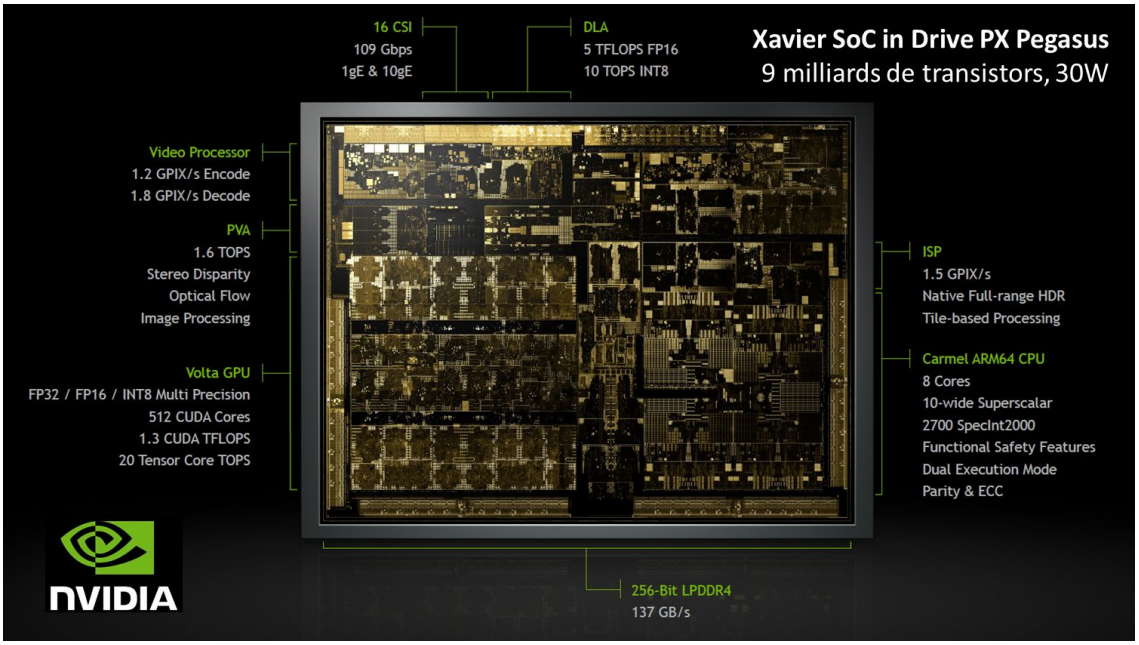


Illustration 37 : Nvidia Xavier,
Source : NVidia

Ces capteurs alimentent des **logiciels** à commencer par ceux de la vision artificielle, puis de la conduite autonome à base de prise de décision, de cartographie et d'optimisation de parcours et aussi de commande vocale. Les systèmes d'exploitation viennent d'acteurs spécialisés tels que **QNX**, filiale de Blackberry. Le leader des moteur de recherche chinois **Baidu** propose de son côté sa plateforme logicielle open source de conduite autonome Apollo 2.0. Elle ajoute des fonctions de sécurisation de la conduite grâce à une meilleure prise en compte des capteurs du véhicule et du planning de la conduite. Le tout s'appuie sur des services en cloud, une plateforme logicielle embarquée et une plateforme matérielle de référence. Apollo 2.0 supporte les chipsets de Nvidia, Intel, NXP et Renesas.
Le **cloud** servira de support aux ressources partagées pour la gestion et l'optimisation des trajets, pour la réservation des véhicules, pour la fourniture de services embarqués dans les véhicules pour les loisirs et le travail, notamment le travail collaboratif. En plus de **Baidu**, il faudra notamment compter avec **Google** et **HERE**.

Au CES 2018, **Ford** annonçait se positionner à terme plus comme un opérateur de plateforme de véhicules et un partenaire d'opérateurs de services qu'en simple constructeur, le tout en se souciant de la bonne intégration des véhicules dans la ville intelligente. Ford entrevoit un monde où les voitures seront de plus en plus mutualisées au niveau de plateformes de services au lieu d'être possédées par les foyers. L'Américain **Uber** anticipe également cette échéance, ayant déjà commandé des milliers de voitures autonomes à **Volvo**. Il en va ainsi de **Lyft** qui expérimentait au CES de Las Vegas des véhicules autonomes BMW réalisés en partenariat avec l'équipementier **Aptiv**, anciennement Delphi.

Les véhicules autonomes s'appuieront donc largement sur les **infrastructures télécoms**, 4G puis 5G avec son très haut débit mobile et un faible temps de latence qui permettra une bonne coordination entre les véhicules et les infrastructures des villes intelligentes. La 5G

servira aussi à alimenter les véhicules en contenus personnalisés, ce d'autant plus qu'ils seront plus fortement mutualisés que les véhicules à essence et diesel actuels.

Enfin, les véhicules autonomes sont quasiment tous électriques. D'où l'importance de disposer de **batteries efficaces**. La recherche s'intensifie pour créer des batteries de nouvelle génération à forte densité énergétique, une charge rapide et des matériaux non polluants et recyclables. En France, SAFT, filiale de Total, est sur les rangs, face à Panasonic et Samsung qui dominent le marché.

Bref, le véhicule autonome ne sera pas un simple objet connecté mobile mais un véritable produit-système, un élément d'un vaste réseau de technologies et de services avec une myriade d'acteurs technologiques et de services. Le tout pour apporter un service sans couture.

Aucun acteur ne semble prêt à maitriser cette chaine de valeur complexe de bout en bout. Elle s'horizontalisera sans doute avec quelques acteurs leaders pour chacune de ces couches techniques, notamment les plus basses et les plus génériques au niveau des composants et des logiciels. A chaque étage, seront associés un mélange de capteurs, de processeurs, de données, de logiciels et de télécommunications.

Certains acteurs portent bien cette vision intégrative du véhicule autonome. C'est notamment le cas de **Byton**, cette startup associant des Chinois, des Américains et des Allemands, ces derniers provenant de BMW. En décembre 2017, la startup annonçait sa berline électrique à conduite assistée puis à terme autonome. Les concepteurs de ce véhicule ont réfléchi à de nombreux aspects et scénarios de son usage et le lien entre véhicule et mobile, le partage du véhicule et sa personnalisation. Doté d'un écran géant de 1,25 m de large, il ressemble à un concept car et pourtant son lancement est prévu d'ici 2019. Byton est une marque de la startup chinoise **Future Mobility** qui a déjà levé $200M pour commencer, notamment auprès de Tencent et Foxconn.

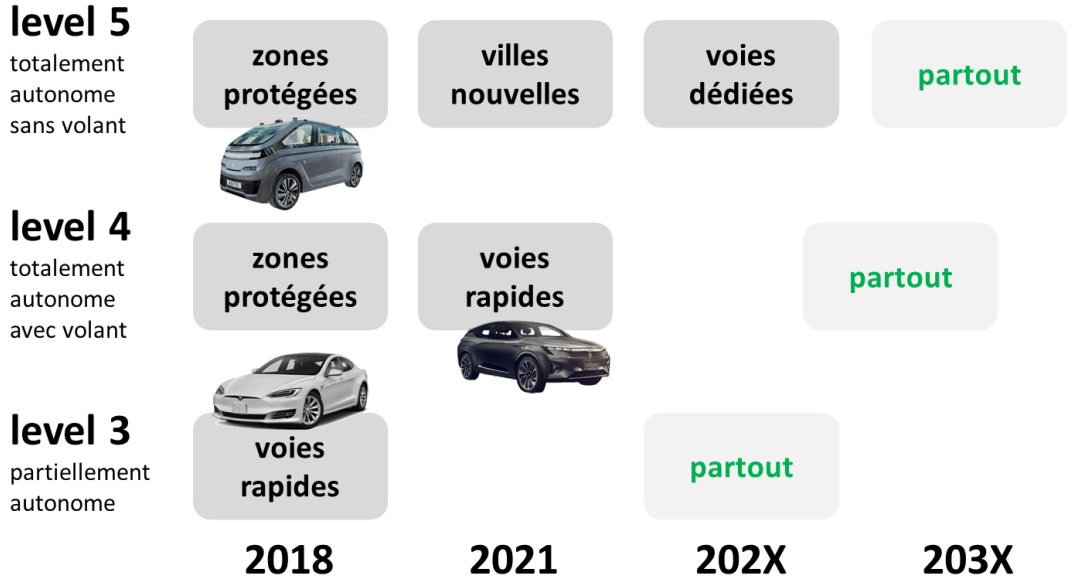
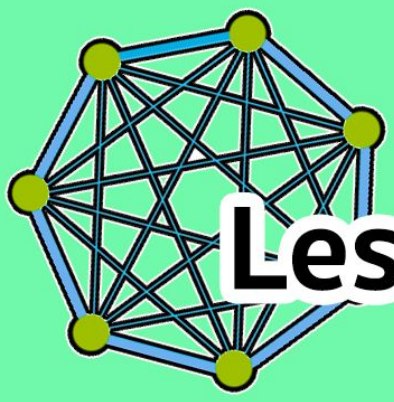


Illustration 38 : Roadmap véhicules autonomes, Source : Olivier Ezratty

L'enjeu technologique le plus complexe à gérer pour les véhicules autonomes est leur interaction avec les véhicules à conducteurs et avec les passants. Ces derniers ne respectent pas toujours les règles et le code de la route. Négocier avec eux est difficile pour les logiciels aussi sophistiqués soient-ils. Les véhicules autonomes pourraient sensiblement réduire l'accidentologie automobile qui est de 1,3 millions de morts par an dans le monde, sans compter les blessés, soit bien plus que toutes les guerres. C'en est à tel point qu'il n'est pas délirant d'imaginer qu'à terme, la conduite manuelle pourra être interdite dans certains endroits, comme dans les villes !

Olivier Ezratty *conseille depuis 2005 les entreprises pour l'élaboration de leurs stratégies d'innovation, en particulier autour des objets connectés et de l'intelligence artificielle. Très actif dans l'écosystème des startups qu'il accompagne comme consultant, advisor, conférencier et auteur, il est apprécié pour les articles fouillés de son blog « Opinions Libres ». Il y publie le « Guide des Startups », le « Rapport du CES de Las Vegas » chaque année depuis 2006 ainsi que l'ebook « Les usages de l'intelligence artificielle » (octobre 2017). Issu de Centrale Paris (1985), Olivier Ezratty a démarré comme ingénieur logiciel et responsable de R&D dans l'informatique éditoriale chez Sogitec, puis fait ses armes dans le marketing chez Microsoft France pour en devenir ensuite le Directeur Marketing et Communication puis le Directeur des Relations Développeurs.*]



Les cas d'usage

10. Cas d'usage

10.1. Supervision d'un parc de tourets de câbles électriques

Cas d'usage : Supervision d'un parc de tourets de câbles électriques

Entreprises : Nexans (gestionnaire) et Enedis (utilisateur)

Besoin : Géolocaliser l'état d'un parc de tourets de câbles destinés aux chantiers de réseaux d'énergie Enedis.
L'objectif est à la fois de tracer la position géographique des tourets, mais également de pouvoir les identifier sur le terrain et de retourner l'état de la longueur de câble disponible.
Ces données sont utilisées à la fois par Nexans et par Enedis

Valeur métier : La solution permet d'optimiser le cycle global d'exploitation des tourets de câbles en anticipant les stocks sur chantier et en réduisant les cycles logistiques (récupération au plus tôt des tourets vides).
La solution permet également de prévenir les pertes d'actifs sur le terrain.

Solution technique :
Balises de géolocalisation **Ffly4u** basées sur les réseaux sans fils Sigfox et LoRa.
plateforme logicielle Ffly4u (en phase de POC) et plateforme Nexans en phase de déploiement industriel

Enseignements :
La taille importante des industriels engagés dans un tel projet nécessite un travail conséquent de coordination et de cadrage amont pour définir le cahier des charges, les rôles et responsabilités et les choix technologiques.
La réalisation d'une preuve de concept (POC) permet de faciliter et d'accélérer l'amorçage et la réalisation d'un tel projet en s'appuyant sur un produit concret et évolutif.

Illustration 39 : Nexans et Ffly4u connectent les tourets de câbles,
Source : http://www.chantiersdefrance.fr/

10.2. Supervision et maintenance d'un parc de cabines de peinture

Cas d'usage : Supervision et maintenance d'un parc de cabines de peinture

Entreprises : Prestataire spécialisé dans la maintenance industrielle

Besoin :
Superviser le fonctionnement d'un parc de cabines de peinture déployées sur de nombreux sites géographiques, en particulier chez des industriels, des équipementiers et des carrossiers.
La société de maintenance souhaite optimiser ses interventions, en mesurant les durées d'utilisation des machines et en détectant des alertes de fonctionnement. Elle s'oriente en outre vers une digitalisation de ses activités et une facturation à l'usage de ses prestations.

Valeur métier :
La solution permet d'optimiser le cycle de maintenance des cabines de peinture en anticipant de façon précise les dates optimales d'intervention.
La plateforme logicielle est en outre accessible aux clients finaux (utilisateurs des cabines de peinture) afin de leur permettre d'accéder aux mesures, aux statuts de maintenance et aux divers rapports d'intervention.

Solution technique :
Modem Industriels Ercogener communicants sur le réseau mobile GPRS/3G
plateforme logicielle Fusion Labs, basée sur Microsoft Azure IoT

Enseignements :
La mise en place d'une première solution opérationnelle a été très rapide. Le déploiement « en volume » a nécessité un travail de fond chez le prestataire de maintenance pour redéfinir son offre, adapter ses processus internes et acquérir de nouvelles compétences.
De nouvelles opportunités sont apparues au fil de l'expérience pour notamment étendre la digitalisation des processus de l'entreprise et enrichir l'offre de services.

Illustration 40 : Cabine de peinture, Source : Fusion Labs

10.3. Dispositif de sécurité pour les femmes pratiquant la course à pieds

Cas d'usage : Dispositif de sécurité pour les femmes pratiquant la course à pieds.

Entreprises : WomenRun - Startup IoT B2B2C

Besoin :
50% des femmes sont réticentes à pratiquer une activité en extérieur en raison d'un sentiment d'insécurité. Elles se rabattent très généralement sur des salles de sport. Elles sont par ailleurs à la recherche de motivations pour maintenir une régularité et progresser dans leur pratique.

Valeur métier :
La solution permet aux coureuses de lancer très simplement des alertes en cas d'agression et de s'entraider grâce au réseau social des utilisateurs.
Le modèle économique WomenRun est basé sur la vente d'objets, de services et d'abonnements en mode B2B2.

Solution technique :
Application mobile et accessoire Bluetooth disposant d'un bouton d'alerte et couplé au smartphone.
Un objet autonome (montre bracelet connecté ayant sa propre connectivité) est à l'étude pour compléter et adresser une population plus large.

Enseignements :
L'utilisation initiale d'un objet fabriqué en Chine a montré des limites sur la qualité du design et la conformité réglementaire. L'investissement sur un objet connecté est assez coûteux et ce secteur est déjà occupé par des acteurs extrêmement importants. Une voie intéressante est la possibilité de nouer des partenariats avec un acteur du secteur (équipementier sportif) ou un acteur B2B désireux de compléter sa digitalisation.

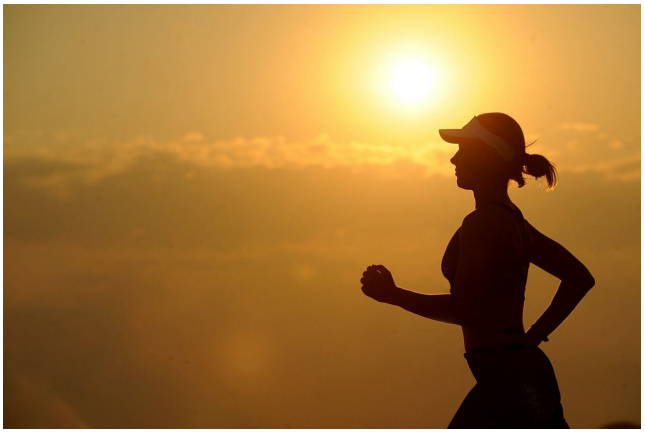


Illustration 41 : WomanRun,
Source : WomanRun

10.4. Ville de Carmaux et transition énergétique

Commune : La ville de Carmaux

Besoin : Profiter des technologies de l'IoT pour contribuer à la tenue d'une des priorités de l'équipe municipale de la Ville de Carmaux à savoir : la transition énergétique qui s'inscrit dans le cadre de la démarche « territoire à énergie positive pour la croissance verte » (TEPCV).

Valeur métier : Pour l'équipe municipale, il est devenu primordial de prêter une attention toute particulière à la consommation d'énergie en commençant par les différentes infrastructures partagées sous leur responsabilité (bâtiment de la Mairie, salle multisports, salle des fêtes, stade…). Les objets connectés apportent des solutions pour connecter les différents lieux composant la ville de manière simple et flexible afin de superviser en temps réel les consommations d'énergie associées à des éléments de contexte ayant de l'influence dessus.

Solution technique : Ils ont choisi d'utiliser les technologies IoT basées sur les réseaux bas débit : LoRa d'Orange et SigFox pour superviser des lieux partagés dont l'optimisation de la consommation énergétique est critique.

Sur base d'objets connectés fixes, Ils supervisent :

- **la production photovoltaïque de plusieurs bâtiments équipés de panneaux solaires** (en s'appuyant la solution du fournisseur Tecsol),
- **la consommation énergétique de leur salle multisports et du bâtiment de la Mairie** à l'aide d'une flotte de différents capteurs permettant de mesurer des paramètres (température, hygrométrie), de relever des compteurs (Gaz et électricité avec Phinect) et aussi détecter des événements de contexte (ouverture de porte et luminosité).

Sur base d'objets connectés mobiles, Ils organisent **des campagnes de mesures temporaires à la demande** sur certains lieux identifiés par les citoyens. Avec une flotte de capteurs mobiles, ils peuvent contrôler la température et l'hygrométrie pendant une période définie, comme dans une école qui se plaindrait de la température de certaines salles.

Enseignements : La ville de Carmaux fait partie des précurseurs dans la mise en oeuvre de solutions connectées pour accompagner leur politique de supervision intelligente de l'énergie. Cependant, ils n'ont au départ pas choisi les outils adaptés en implémentant des solutions M2M, moins flexibles et plus coûteuses. Les **réseaux bas débit** comme LoRa et Sigfox correspondent à ce type de besoin (économique en abonnement et doté d'une pile d'autonomie d'environ 3 à 5 ans).

Aussi, les solutions actuellement proposées par les différents fournisseurs de services, restent encore complexes à utiliser au quotidien en ce sens que chacune d'entre elles

dispose de sa propre plateforme. Les utilisateurs sont donc confrontés à une multitude d'applications. Une amélioration notable réside en la capacité à **fédérer toutes les données utiles à une ville dans un seul et unique portail**. De la même façon, **l'ergonomie** de ces applications doit être simple et accessible pour faciliter leur usage au quotidien.

Actuellement, la Ville de Carmaux se préoccupe de la mesure de la **Qualité de l'air** du fait de la législation d'une part et d'un intérêt croissant pour ce sujet de la part de ses habitants d'autre part.

Pour la commune, les technologies IoT et les applications logicielles associées, représentent un formidable outil pour **améliorer le fonctionnement des villes**. Qui plus est, les objets connectés présentent aussi un côté **ludique** qui peut faciliter leur adoption. Dans cet esprit elle envisage d'utiliser des boutons connectés pour mener des campagnes de mesure de satisfaction de ses administrés dans des lieux stratégiques ou à l'occasion de manifestations qu'elle organise comme le salon des éco-énergies.

Dans le même temps elle songe déjà à l'**Open Data** pour participer à mettre en intelligence les services de la ville et du territoire entre-eux.

Remerciements au Maire de la ville de Carmaux, Mr Alain Espié et son Directeur Général des Services, Mr Henri Ebbo.

Illustration 42 : La ville de Carmaux,
Source : Service de communication Ville de Carmaux

10.5. Services connectés de Smart Care

Cas d'usage : Protéger **les personnes âgées fragilisées vivant seules,** tout en restant en lien avec leurs proches.

Entreprises : Téléassisteur, Entreprise de services à la personne, Résidence Senior, Ehpad, Mutuelles et Assurances, Collectivités

Besoin : 90% des personnes âgées veulent rester à domicile le plus longtemps possible, mais 81% **des chutes** ont lieu à domicile.
La solution majoritairement utilisée pour protéger ces personnes est la **téléassistance** avec médaillon d'appel. Néanmoins, la majorité d'entre elles ne le portent pas sur elles ou ne peuvent pas appuyer sur le bouton lorsqu'elles chutent.

Valeur métier :
La solution **Otono-me** *www.otono-me.com* permet de détecter et d'identifier **des situations d'anomalie** dans l'activité d'une personne âgée à domicile et ainsi générer automatiquement des **alertes** à partir de l'analyse de ses données comportementales.
Elle permet aux professionnels du vieillissement et du soutien à domicile d'accéder à des fonctionnalités poussées, comme des **statistiques prédictives**, de la modélisation comportementale, des moteurs de règles avancés.

Solution technique :
- Capteurs environnement + Plateforme(s) IOT
- **Plateforme intelligente d'analyse de données TELEGRAFIK** + Application mobile et web permettant aux proches de vérifier que tout va bien au domicile de la personne âgée

Enseignements :
Le marché du maintien à domicile est composé d'acteurs historiques proposant le médaillon d'appel depuis de nombreuses années. La réalisation d'une phase de test de la solution est généralement demandée par ces acteurs afin de pouvoir en comprendre les fonctionnalités, la valider et l'intégrer dans leurs gammes de produits. Une fois ces étapes franchies, l'enjeu est pour eux de **réussir à l'expliquer et la diffuser auprès du grand public et des réseaux de prescripteurs,** peu habitués aux innovants dans les domaines des services connectés.

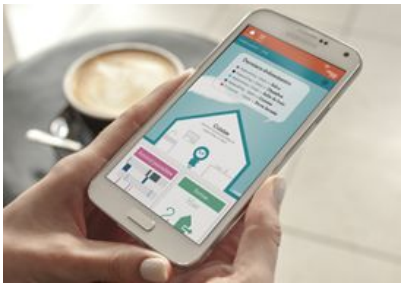


Illustration 43 : Application mobile pour les proches,
Source : www.otono-me.com TELEGRAFIK

11. Formation

Les projets IoT nécessitent des compétences dans plusieurs domaines : électronique, logiciel embarqué, applicatif (web, applications mobiles...), réseau, intégration système, data scientist et sécurité.

L'IoT est, comme tout nouveau domaine, source de métiers et compétences spécifiques qui demandent plus largement de savoir proposer des formations plus spécialisées. Nous anticipons l'émergence de nouveaux types de métiers de plus haut niveau, capables d'avoir une vision complète de la chaîne IoT, métier que l'on pourrait qualifier de : "**IoT chain Manager**".

Depuis 2015, des formations professionnelles et académiques spécialisées voient le jour afin d'accompagner l'émergence de ce nouveau marché. Par exemple, INSA (Toulouse), ICAM (Toulouse), Université de Cergy (Paris)...

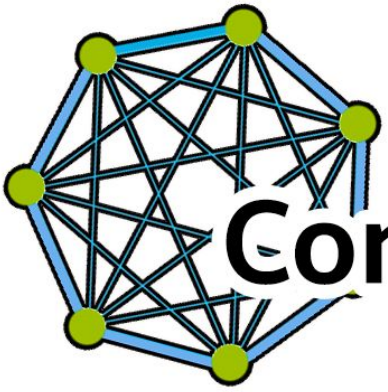
Exemple de formations académiques :

- **IUT Paul Sabatier de Toulouse** : Formation Internet des objets depuis 2016.
- **Université de Cergy-Pontoise** : "comprendre et créer l'Internet des Objets".
- **IUT Paris-Est de Marnes-la-vallée** : Master Systèmes et services pour l'Internet des Objets.
- La prestigieuse école **X-Polytechnique** propose depuis 2016 une formation objets connectés.
- **Télécom Sud Paris :** Certificat d'Études Spécialisées "Internet des objets (IoT), conception de solutions".
- **ISEP :** Parcours Architecte Télécom et Internet des objets.
- **Open Source School :** http://formations.opensourceschool.fr/formations/embarqu%C3%A9-iot

Exemples de formations professionnelles :

- Chez **Human Coders** : Formation Internet des objets.
- Chez **Cap Gemini** : formation de 2 jours "Objets connectés et Internet des objets".
- Chez **Orsys** : Formation Internet des objets, développer des applications en Java.
- ...

L'offre de formation sur le sujet s'est largement étoffé. L'offre de formation chez les généralistes intègre désormais un volet IoT, qui s'enrichit peu à peu vers une gamme de formations IoT.



Conclusion

12. Conclusion

Ainsi, bien que tous les standards ne soient pas encore bien établis et que les freins, comme les inconnues, soient encore nombreux, l'IoT est un marché émergeant qui se voit accéléré par les nouveaux enjeux du numérique, que l'on qualifie de **transformation digitale**. Cette transition, nous menant progressivement dans le monde des services intelligents, draine naturellement le besoin d'intégrer ces objets connectés pour être en mesure de répondre aux différents cas d'usage, comme par exemple, ceux décrits dans les concepts de :

- **Smart Cities** : Concept visant à améliorer la vie en ville au travers de six axes : économie, mobilité, environnement, habitants, mode de vie et administration grâce à l'utilisation des technologies de la communication et de l'information.
- **Smart Building** : Concept de bâtiments connectés, intelligents et évolutifs.
- **Smart Home** : Maison connectée et intelligente.
- **Smart Factory ou industrie 4.0** : Représentant l'usine du futur basée sur de nouveaux modèles de fonctionnement.
- **Smart Grid** : Réseau de distribution d'électricité intelligent.
- **Smart Transport** : Véhicules connectés, les voiries…
- **Smart Tracking :** Géolocalisation des positions et des déplacements d'objets mobiles.

L'expansion de l'IoT dans les années à venir ne fait maintenant plus aucun doute, et cela a d'ailleurs déjà commencé.

Comme vous avez pu le constater en parcourant ce livre blanc "Panorama du monde de l'Internet des Objets", l'IoT est un domaine de compétence à lui seul, puisqu'il fait appel à des technologies (logicielles et matérielles), des méthodologies, et même des métiers qui peuvent être spécifiques à ce domaine. Alors, pour pouvoir bénéficier de ces services à forte valeur ajoutée, il faudra vous décider à rapidement "sauter le pas" pour justement appréhender ces nouvelles briques du monde digital de demain et pouvoir bénéficier de ses promesses au plus tôt. Dans le domaine professionnel, ces objets, parfois qualifiés de capteurs, couplés à vos systèmes Big Data, vous offriront de nouveaux super pouvoirs capables de résoudre certains de vos problèmes auparavant insolubles. Ils vous permettront aussi d'aller plus loin dans l'optimisation de vos processus et d'améliorer significativement la qualité de vos services.

Vous l'aurez compris, bien que le Smartphone puisse être considéré comme le premier objet connecté distribué à grande échelle, le marché grand public reste sans doute le moins prévisible de l'IoT. Les experts s'accordent à dire que le plus dur n'est pas de connecter les objets, mais bien de trouver les usages qui vont avec, ceci afin de sortir de l'effet purement "gadget" que certains objets connectés apportent encore aujourd'hui. L'effort est donc à mettre sur la partie utile du service. C'est actuellement la domotique qui se révèle être la plus implantée dans la durée, mais la plus visible reste les objets « wearable » (ou «

portables ») qui suscitent le plus d'intérêt. L'Apple Watch, par exemple, se vend finalement très bien, avec plus de 3 millions d'exemplaires livrées en 2015 et 5,6 millions rien que sur le dernier trimestre 2016 comptabilisant près de 11,9 millions d'unités dans le Monde, les vêtements connectés fleurissent de toute part avec différentes fonctionnalités et Google a annoncé lancer une nouvelle version de ses lunettes « Google Glass », pendant que Microsoft mise sur ses "Hololens" et Facebook sur son "Oculus VR". La tendance va donc vers le « moi augmenté » et le pilotage sur soi de ses appareils distants, avec une touche de réalité augmentée.

Face à la multitude d'objets connectés existants et à venir, et donc à cette incertitude planant sur les objets star de demain, les enjeux commencent à se porter sur des solutions fédératrices, sur l'exemple de la bataille qui se joue actuellement sur les normes et standards de l'IoT. Ainsi, Apple a présenté des évolutions de son framework « HomeKit » destiné à la domotique, connecté à son compte service iCloud et, bien évidemment, les appareils de sa marque. De leur côté, Toshiba et Microsoft ont signé un partenariat, le premier s'occupant de l'électronique et le second des applications. Concernant Google, le géant propose un système d'exploitation dédié à l'IoT qui se nomme « Brillo » proposé gratuitement en Open Source.

Le défi immédiat consiste donc à créer de nouveaux usages interopérables et reliés entre eux puisqu'aucun standard ne sort encore clairement du lot.

Même si la route promet d'être encore longue pour converger sur un standard précis, l'IoT offre dès à présent un important potentiel commercial du fait des services qu'il est capable de nous rendre en s'intégrant dans le cadre de notre transformation digitale. Alors, cher lecteur, si ce n'est pas déjà fait, pourquoi ne pas décider de prendre part à cette nouvelle aventure ? Celle-ci commence ici et chacun peut contribuer à accélérer son inévitable émergence.

Vous désirez contribuer à la prochaine version de ce document ?
Alors, contactez-nous par mail : livreblanc-iot@digitalplace.fr

Postface

 Nous connaissons les objets connectés d'aujourd'hui : la montre ou la balance connectée, le capteur d'humidité pour nos plantes vertes, ou bien encore la voiture autonome. Des start-up inventent chaque jour des objets parfois utiles, parfois gadgets, parfois délirants : grille-pain connecté, biberons connectés,...

Une seconde catégorie d'objets connectés nous entoure déjà sans que nous ne les percevions : capteurs environnementaux de la ville intelligente, éléments d'infrastructure routière (péage, parking...), suivi des colis dans une chaine d'approvisionnement, capteurs et actionneurs dans nos usines automatisées...

Demain, des composants électroniques autonomes en énergie et à extrêmement faible coût (energy harvesting) intègreront des capteurs de plus en plus diversifiés, des processeurs très basse consommation et une communication radio capable de transmettre à une dizaine de mètres. Grâce à cette véritable poussière intelligente (smart dust), de plus en plus d'objets manufacturés pourront ainsi être rendus (un peu) plus intelligents, être reliés à un système d'information ou à l'Internet, et dialoguer avec des applications métier ou des services.

A terme, on peut imaginer que tous les objets manufacturés pourront ainsi, pour quelques euros, être connectés à l'Internet.

Il y a 3 grands enjeux techniques, pour lesquels les chercheurs travaillent à l'échelle mondiale, et sur lesquels la recherche d'Orange est mobilisée :

• créer une connectivité adaptée aux besoins de l'Internet des objets : bas débit, latences très faibles, basse consommation, coûts réduits et capacité de gérer simultanément des milliards d'objets, à l'échelle de la planète. Les technologies d'aujourd'hui, propriétaires comme LORA, ou normalisées comme LTE-M seront complétées demain par la 5G, qui permettra de mutualiser à très grande échelle les réseaux.

- la capacité à des objets et des services à « se trouver et se comprendre » : comment un service va-t-il découvrir où sont les capteurs de pollution dans une ville ? comment va-t-il savoir qu'une place de parking est disponible dans une certaine rue... Des solutions existent aujourd'hui, mais il n'y a pas de mécanisme universel permettant aux hommes et aux services d'interagir avec des objets, de manière simple et interopérable.

- enfin, les questions de sécurité et de protection de la vie privée : l'Internet des Objets pose de nouvelles questions de sécurité. Comment assurer la sécurité d'une myriade d'objets connectés de nature différente, comment gérer les droits d'accès aux capacités de l'objet? On comprend bien qu'une chaine de production automatisée pose des problèmes de sécurité bien différents que ceux posés par un capteur de d'humidité pour une plante verte.

Les ordinateurs et l'Internet ont engendré la transformation numérique de toutes les activités humaines manipulant des données et des connaissances. Cet Internet cerveau « réside » aujourd'hui très largement dans de gros Data Center. A moyenne échéance, Internet sera doté de nouvelle capacités sensorielles avec des milliards de capteurs mesurant toutes sortes de choses dans le monde physique (données environnementales, biologiques, industrielles, mesures physiques,...). Il sera aussi doté de muscles : les milliards d'actionneurs permettant d'agir sur des processus physiques, au sein de la ville, dans l'industrie, en médecine ou en agriculture. On passera ainsi d'un Internet des objets, limité à la connectivité, à un véritable Web des Objets où les objets pourront interagir entre eux et mener des tâches complexes.

Le Web des Objets sera une révolution aussi importante que l'a été en son temps l'Internet « des pages web » qui a été lancé il y 30 ans. Ce qui est vraiment différent avec le Web des Objets, c'est qu'il transformera des activités économiques se réalisant au sein du monde physique : processus industriels, chaines logistiques, robotique...

Et à terme, l'Internet que nous connaissons sera donc très largement imbriqué dans notre monde physique. Bien au-delà les effets de mode des objets connectés d'aujourd'hui, ce Web des Objets constituera une transformation de la nature même de l'Internet.

Nicolas Demassieux
Senior Vice President, Orange Labs Research

Références

- The IOT Book 2015 : « Créer un objet connecté pour le vendre »
- OneM2M
- Wikipedia
- Article sur le LiFi de Whim
- Réseaux Sans Infrastructure par M. Abderrezak RACHEDI de l'UPEM
- Enterprise IoT
- Livre Blanc Internet des Objets 2015, auteur : EBG
- Livre Blanc 360° de l'Internet des Objets, auteur : CIGREF
- Ignite Eclipse project IoT Methodology, auteurs : La fondation Eclipse associée à des experts
- Meetup IoT organisé sur Toulouse en 2016
- Blog de Stéphane Bortzmeyer
- Web Objetsconnectes.com
- Le fil rouge de la RFID article sur les nouvelles réglementation des objets connectés
- ANSSI : Chapitre 3.3 « Intégration de la cybersécurité dans le cycle de vie du système industriel »
- Gartner report "Forecast: IoT Security, Worldwide, 2018", Mars 2018

Crédits et remerciements

Les noms de produits utilisés dans ce livre sont à des fins de citation seulement. Toutes les marques commerciales et marques déposées sont la propriété de leurs propriétaires respectifs.

- Illustrations 1, 2, 3, 7, 8, 9, 28, 40 : courtoisie de **Fusion Labs**
- Illustration 4 : source **Flickr savoirenactes.fr PhilCaz**, Licence CC BY-SA 2.0
- Illustration 5 : site web Open Data de la **SNCF**
- Illustrations 6, 29 et 35 : courtoisie de **Cyril Hlakkache**
- Illustrations 10 : courtoisie de **Sierra Wireless**
- Illustrations 11, 12, 16, 20, 21, 22 : Courtoisie de **ST Microelectronics**
- Illustration 13 : Source *https://www.telensa.com/*
- Illustration 14 : Source *http://www.healthcardionexion.com/*
- Illustration 15 : Source *https://wireless.murata.com/*
- Illustration 17 : **ARM**, Source *https://www.arm.com/*
- Illustration 18 : **MBed**, Source *https://www.mbed.com/*
- Illustration 19 : **Amazon**, Source *https://aws.amazon.com/*
- Illustrations 23, 24, 25, 26, 27 : Source http://enterprise-iot.org/
- Illustration 30, 31, 32 : Courtoisie de **ISIT**
- Illustration 33 : Source http://www.ittia.com/
- Illustration 34 : Source https://www.iss.se/

- Illustration 36, 38 : Courtoisie de **Olivier Ezratty**
- Illustration 37 : **Nvidia**, Source http://www.nvidia.fr/
- Illustration 39 : Source http://www.chantiersdefrance.fr/
- Illustration 41 : Société **Womenrun**, Source : https://www.womenrun.net/
- Illustration 42 : Service de communication de la **ville de Carmaux**
- Illustration 43 : Source **TELEGRAFIK** www.telegrafik.eu

Licence

DigitalPlace, le cluster du numérique

DigitalPlace est le cluster d'entreprises numériques d'Occitanie. Il est constitué d'entreprises de toutes tailles, de la startup à l'entreprise de taille intermédiaire (ETI) représentatives de tous les métiers des Technologies de l'Information et de la Communication. Il a le statut d'association loi 1901 et a été initié et labellisé en 2011 par l'Etat et la Région Occitanie. Il regroupe près de 200 entités adhérentes : startups, TPME, ETI, grands comptes, laboratoires de recherche, institutionnels et partenaires économique.

DigitalPlace propose notamment différentes commissions thématiques (Internationale, Financement, Innovation, Cybersécurité, Big Data). Ce document s'inscrit dans le cadre de la Commission Innovation.

- Missions principales :
    - **Accompagner, fédérer et animer** toute la filière du numérique en région Midi- Pyrénées

    - **Aider les entreprises** à se saisir de l'ensemble des leviers de croissance, et à franchir des caps en matière de chiffre d'affaires et d'accès à de nouveaux marchés.

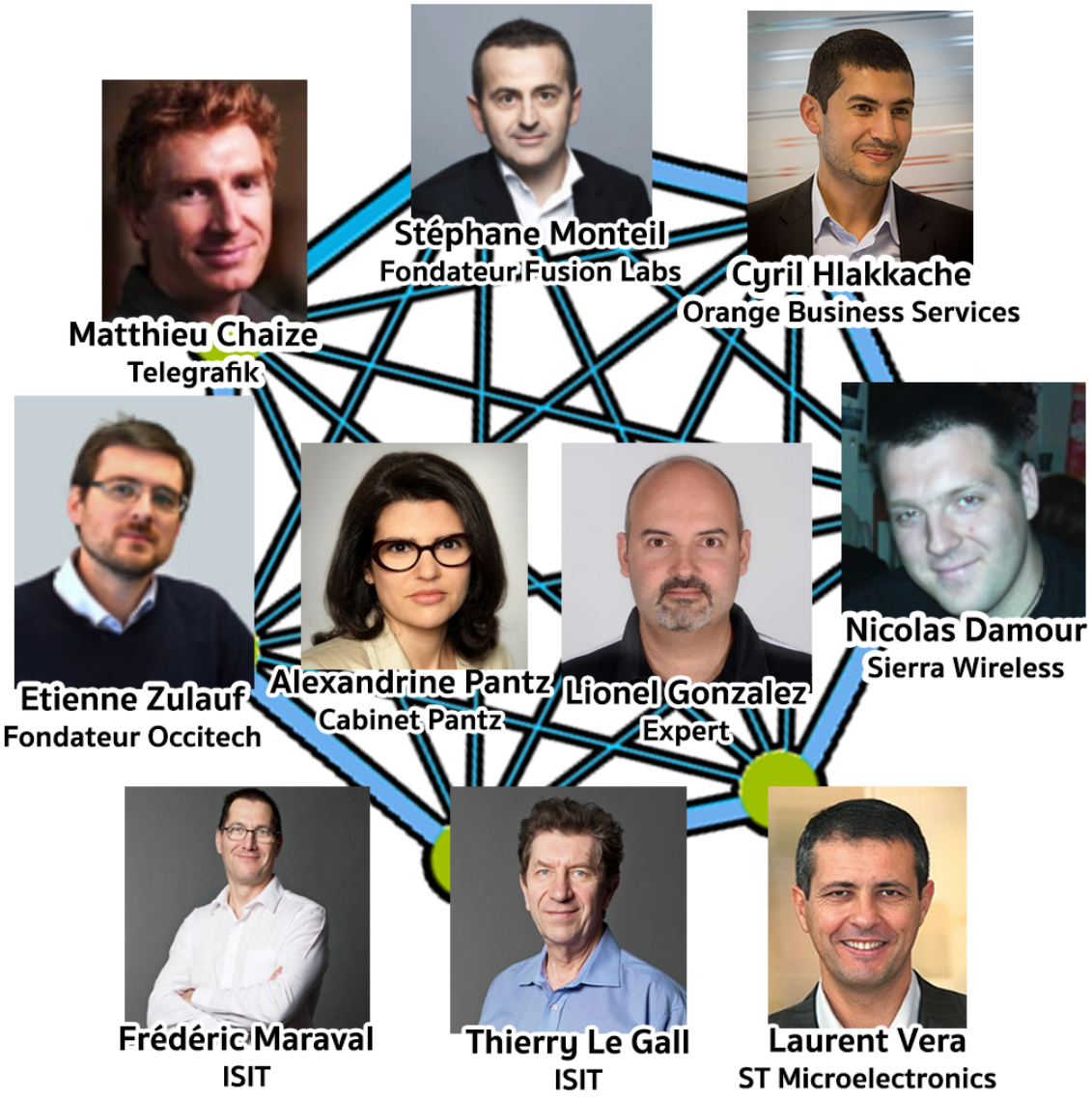
- DigitalPlace a une stratégie d'appui aux entreprises sur 4 axes :
    - **Le développement de l'innovation** sous toutes ses formes
    - **Le développement international**
    - **Le financement** de la croissance
    - **La mutualisation** des services

- Pourquoi adhérer au cluster ?
    - **Participer à la dynamique collective** des entreprises du cluster en participant à des groupes de travail et de réflexion
    - **Bénéficier d'un accompagnement** dans son développement et sa croissance
    - **Rencontrer les acteurs nationaux et régionaux** de l'écosystème numérique: startups, PME, ETI et grands comptes innovants, mais aussi laboratoires, écoles, universités et financeurs
    - **Accéder à des services** et de moyens mutualisés
    - S'inscrire fortement dans **l'écosystème régional** du numérique

DigitalPlace organise également l'**Innovation IT Day**, l'événement qui réunit le même jour en un même lieu toute la chaîne de l'innovation numérique : laboratoires de recherche, start-ups, PME innovantes et les grands comptes industriels. Son objectif est de créer des passerelles entre des mondes qui se côtoient peu, à savoir ceux de la recherche, des TPME innovantes et des grands comptes, pour donner naissance à des synergies et des partenariats entre eux.

C'est lors de l'édition 2015 et sur l'initiative de membres de la Commission Innovation de DigitalPlace (**Orange**, **Fusion Labs**, **Telegrafik**, **Occitech** et **Sierra Wireless**), que s'est tenu un atelier ayant pour vocation de dresser le panorama de l'Internet des Objets. Ce livre blanc est le résultat d'un travail collectif de représentants de ces entreprises. DigitalPlace remercie l'ensemble des contributeurs pour leur mobilisation et la richesse de ce document.

www.digitalplace.fr - contact@digitalplace.fr
PORTES SUD, BAT 3
12 rue Louis Courtois de Viçose
31100 TOULOUSE
Téléphone : +33 5 34 31 41 95
Suivez-nous sur Twitter : @DigitalPlaceICT



Merci d'avoir pris le temps de parcourir la version 3 du livre blanc : «Panorama de l'Internet de Objets» !

