



Panorama de l'Internet des Objets



DigitalPlace

FUSION LABS

Internet des objets et services Cloud



SIERRA
WIRELESS™



TELEGRAFIK

Services connectés intergénérationnels

OCCITECH
// INGENIERIE WEB



Auteurs :

2017

Cyril Hlakkache - Orange,
Stéphane Monteil - Fusion Labs,
Matthieu Chaize - Telegrafik,
Etienne Zulauf - Occitech,
Nicolas Damour - Sierra Wireless,
Lionel Gonzalez - Symantec,
Alexandrine Pantz - Cabinet Pantz.

Préface de :

Thierry Sachot

Président de la Cité de l'objet connecté

Postface de :

Nicolas Demassieux

Senior Vice President, Orange Labs Research



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'**Innovation IT Day** (IITD) est la rencontre annuelle des acteurs de l'innovation. Y échantent les laboratoires de recherche, les jeunes pousses et les industriels. Dans le cadre de l'IITD 2016, sur l'initiative de membres de la Commission Innovation de DigitalPlace et d'une collaboration étendue (**Orange, Fusion Labs, Telegrafik, Occitech, Sierra Wireless, Symantec** et le **cabinet d'avocats Pantz**), s'est tenu un **atelier pour dresser le panorama de l'Internet des Objets** (Internet of Things ou IoT) tant en termes économiques que techniques.

Ce document reflète ces échanges et débats. En particulier, il est apparu au cours de cet atelier que la version 2016 ne traitait que superficiellement des problématiques au combien essentielles que sont la sécurité et la place de la confidentialité des données personnelles. Ainsi cette nouvelle version 2017 du Livre Blanc sur l'IoT complète le document avec les résultats des travaux des experts sur les aspects Sécurité et Juridique. Sur cette base, l'[IITD 2017](#) proposera un atelier ouvert à tous afin de le compléter dans une démarche collaborative qui sied bien à notre cluster, lieu permanent d'échanges de l'écosystème numérique en Occitanie.

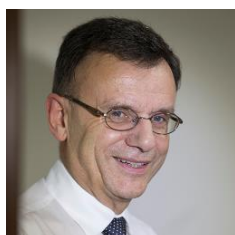
Nous exprimons toute notre gratitude à **Cyril Hlakkache** pour avoir proposé et initié ce projet lors d'une Commission Innovation du cluster et à **Stéphane Monteil, Matthieu Chaize, Etienne Zulauf, Nicolas Damour, Lionel Gonzalez** et **Alexandrine Pantz** pour l'animation de l'atelier et la rédaction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

Fabien Gaidon (Gaidon 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'appêtent 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 2 ? Le succès rencontré par la première version du document (publié en mai 2016) nous a motivé à publier une nouvelle version proposant un contenu actualisé, dans un domaine riche en actualités, mais aussi et surtout développant deux nouvelles parties dédiées aux aspects **sécurité** et **juridique**. Pour développer ces nouvelles parties nous avons accueilli deux nouveaux contributeurs disposant d'une expertise dans ces domaines très spécifiques.

Issu de la rencontre de plusieurs individus en lien avec l'IoT dans le cadre de l'[Innovation IT Day](#), événement organisé par le cluster numérique [Digital Place](#), ce livre blanc a permis à chacun-e d'approfondir ses connaissances grâce aux contributions des autres et a été pour nous une formidable expérience.

Nous vous souhaitons une bonne lecture de cette nouvelle édition 2017 !

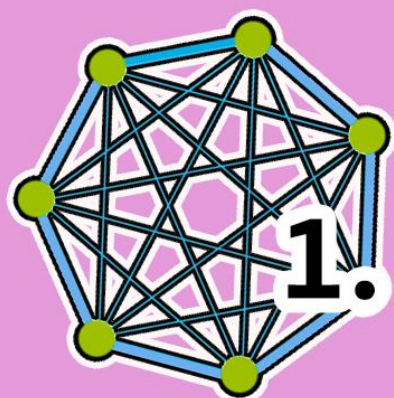


Sommaire :

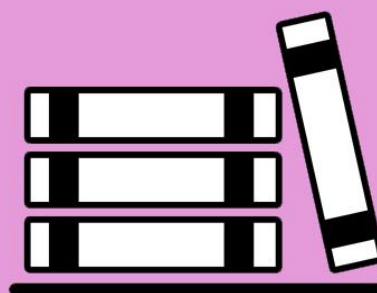
1. Glossaire.....	8
2. Le marché et sa dynamique	11
2.1. Introduction.....	11
2.3. Chaîne de valeur	13
2.5. Modèle de maturité et d'adoption.....	14
2.6. Les moteurs du marché.....	15
2.6.1. Pour le grand public	15
2.6.2. Pour les entreprises	16
2.6.3. Les facteurs favorables	16
2.6.4 Introduction de l'IoT sur le marché des professionnels	17
2.7. Le ROI.....	17
3. Les freins	20
3.1. Manque de maturité des standards techniques.....	20
3.2. Manque de maturité des usages.....	20
3.3. Difficulté de gestion d'équipements matériels	21
3.4. Acceptation difficile des nouveaux business models.....	21
3.5. ROI difficile à démontrer	21
3.6. Besoin de concepts innovants pour la gestion de l'énergie	22
3.7. Enjeux sécurité et cybersécurité	22
3.8. Manque de cadre juridique solide	23
3.9 Manque de données et plateformes partagées	24
3.10 Confiance des acheteurs en la pérennité de la solution	24
4. Les technologies	29
4.1. Architectures M2M / IoT.....	29
4.1.1. Les objets ou équipements (devices)	30
4.1.2. Passerelle (gateway) ou modem	30
4.1.3. Réseau de communication	30
4.1.4. Infrastructure de services	31
4.1.5. Application métier.....	31
4.2. Les technologies.....	33
4.2.1. La connectivité WAN	33



4.2.2. La connectivité LAN	34
4.2.3. Compatibilité des équipements et standardisation.....	36
4.2.4. Une réponse multi-technologique.....	38
4.2.5. Plates-formes de services M2M/IoT	38
4.3. La gestion de l'énergie des objets connectés	40
4.3.1. Usages.....	40
4.3.2. Technologies.....	40
4.4. Quelles perspectives sur le long terme ?	41
5. Méthodologie projet.....	43
5.1. Stratégie d'entreprise : à quoi peut ressembler la feuille de route de transformation digitale de votre entreprise ?	43
5.2. Au niveau opérationnel, à quoi peut ressembler une démarche projet IoT ?	45
5.3. Questions / Réponses	48
6. Stratégie de collecte et de traitement des données	52
6.1 Les données.....	52
6.2. Quelles données faut-il récupérer des objets ?	52
6.3. Pour en faire quoi ?	53
6.4. Synthèse	54
7. La sécurité des objets connectés	56
7.1 Un état des lieux préoccupant	56
7.2 Une maturité à construire	57
7.3 La nécessité d'une sécurité de bout en bout.....	59
7.3.1 Sécurité intrinsèque	59
7.3.2 Protection des dispositifs.....	60
7.3.3 Protection des communications et authentification	62
7.3.4 Supervision du service	64
7.4 Des pistes pour l'avenir de la sécurité des objets	64
7.4.1 Détection d'anomalies	64
7.4.2 Éducation des utilisateurs	65
7.4.3 Déclaratif des objets.....	65
8. Juridique	67
8.1 La protection juridique relatives aux données	68
8.2 La responsabilité du fait des objets connectés.....	69
9. Formation.....	72
10. Conclusion	74
Postface.....	76



1. Glossaire





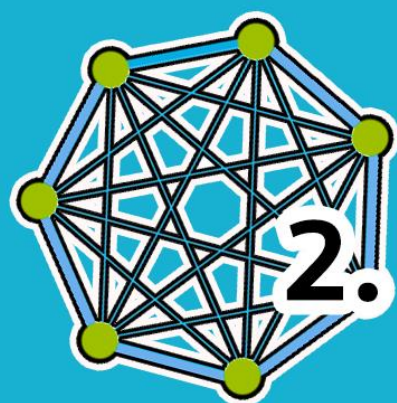
1. Glossaire

Certaines de ces définitions exploitent des extraits issus de Wikipédia qui ont été ensuite adaptées par les auteurs.

1. **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.
2. **M2M (Machine-to-Machine)** : Technologies permettant des échanges entre machines, sans intervention humaine (par opposition aux Interfaces Hommes-Machines).
3. **ETSI (European Telecommunication Standardization Institute)** : Organisme de normalisation européen du domaine des télécommunications.
4. **Agile** : Méthode reposant sur une approche itérative et incrémentale, menée dans un esprit collaboratif avec juste ce qu'il faut de formalisme (selon Véronique Messenger Rota, dans Gestion de projet : Vers les méthodes agiles). L'objectif est de faciliter la mise en œuvre de produits de haute qualité, tout en prenant en compte l'évolution des besoins métiers.
5. **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.
6. **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.
7. **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".
8. **B2B (Business to Business)** : Ensemble des activités d'une entreprise visant une clientèle d'entreprises.
9. **B2C (Business to Consumer)** : Ensemble des activités d'une entreprise visant une clientèle de consommateurs.
10. **Open Data** : Donnée numérique de nature privée ou publique, diffusée de manière structurée et ouverte à tous sans restriction technique, juridique ou financière.
11. **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.
12. **NFC (Near Field Communication)** : Technologie de communication sans fil en champ proche, à courte portée et utilisant des hautes fréquences.
13. **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.
14. **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.
15. **PaaS (Platform as a Service)** : Plate-forme cloud mettant à disposition un environnement d'exécution rapidement disponible et opéré avec un niveau de service défini.
16. **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.



17. **IETF (The Internet Engineering Task Force)** : organisme de normalisation international dédié à l'élaboration des standards Internet.
18. **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.
19. **CDMA (Code Division Multiple Access)** : Système de codage des transmissions, utilisant la technique d'étalement de spectre permettant à plusieurs liaisons numériques d'utiliser simultanément la même fréquence porteuse.
20. **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).
21. **RFC (Requests For Comments)** : Série numérotée de documents officiels publiés par l'IETF décrivant les normes élaborées par l'IETF pour Internet.
22. **DTLS (Datagram Transport Layer Security)** : Protocole fournissant une sécurisation des échanges basée sur des protocoles en mode datagramme comme l'UDP.
23. **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/>).
24. **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.
25. **LiFi (Light Fidelity)** : Technologie de communication sans fil basée sur l'utilisation de la lumière visible (optique) du spectre électromagnétique.
26. **LTE (Long Term Evolution)** : Terme générique pour la 4G.
27. **LTE-M (Long Term Evolution for Machines)** : évolution de la 4G adaptée aux usages IoT.
28. **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.
29. **LPWA (Low Power Wide Area)** : Réseau sans fils basse consommation et longue portée, optimisé pour l'Internet des objets.
30. **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.
31. **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.
32. **ISO (International Standardization Organization)** : Organisation Internationale de Normalisation, composée des différentes organisations nationales de normalisation de chaque pays comme l'AFNOR en France.
33. **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.
34. **Web of Things (Web des objets)** : désigne l'intégration de tout appareil interrogeable ou contrôlable à distance, dans le monde du World Wide Web.
35. **MQTT (MQ Telemetry Transport)** : Protocole de messagerie publish-subscribe basé sur le protocole TCP/IP.
36. **AMQP (pour Advanced Message Queuing Protocol)** : Protocole ouvert pour les systèmes de messagerie standardisant les échanges entre serveurs de messages.



2. Le marché





2. Le marché et sa dynamique

2.1. Introduction

L'Internet des objets, également appelé en anglais **Web of Things** ou **IoT**¹, **M2M**² 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.

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 », 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.

Energie	Transports	Industrie	Grand public	e-Santé	Bâtiment
• Compteurs intelligents • Télémétrie • Panneaux solaires • Eoliennes	• Géolocalisation • Supervision • Sécurité • Transports publics	• Industrie 4.0 • Supervision et automatisation • Maintenance prédictive • Chaîne d'approvisionnement	• Maison intelligentes • Surveillance et alarmes surveillance • Technologies portables & capteurs textiles	• Télémédecine • Appareils médicaux mobiles • Maintien à domicile	• Chauffage, ventilation, climatisation • Eclairage • Sécurité des accès • Alarmes incendie

Figure 1 : les segments de marché de l'IoT (source Fusion labs)

Les autres secteurs B2B[®] et B2C[®] 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.



Figure 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 :

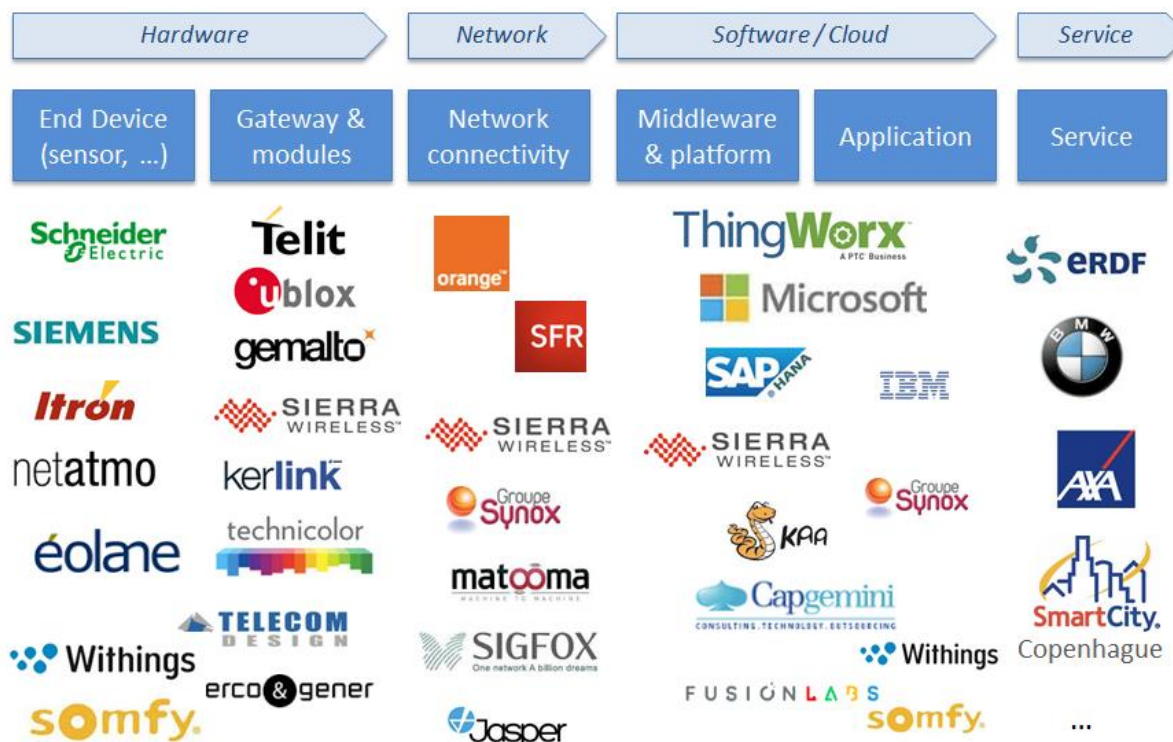


Figure 3 : Quelques acteurs de l'IoT sur la chaîne de valeur (source Fusion Labs)

Les **écosystèmes de startups** et les **PME innovantes** sont des acteurs importants, car nombreux et porteurs de nombreuses innovations ou approches disruptives, en réalité 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 essentielles. 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.

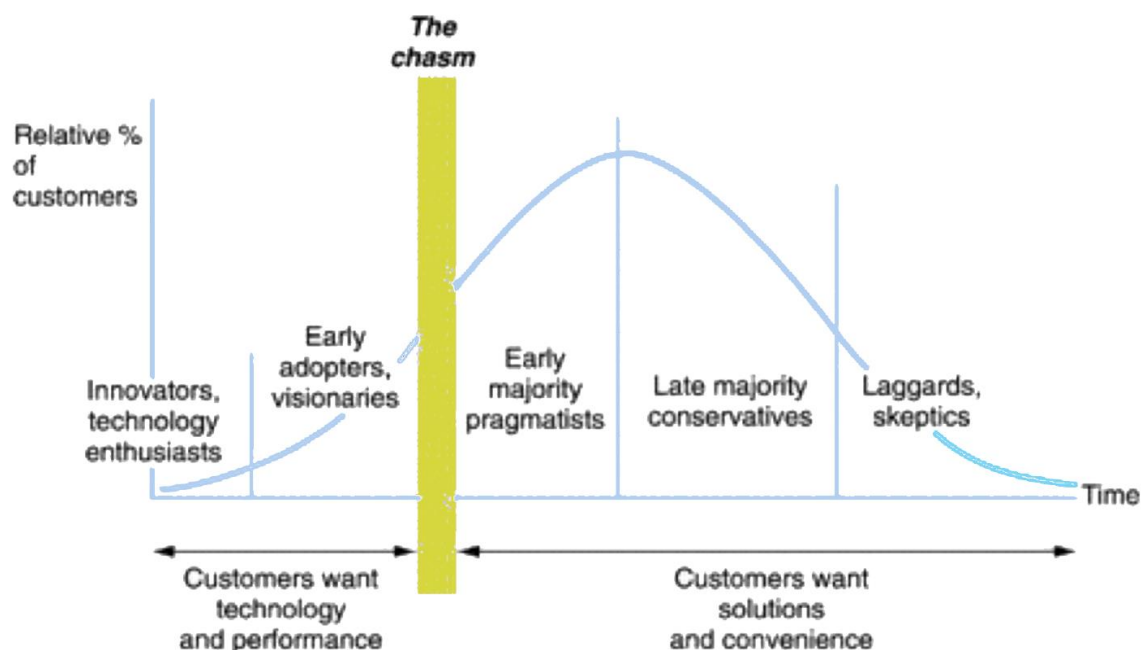


Figure 4 : Courbe de Moore, source Flickr savoirrenactes

Concrètement, le Gartner Group analyse chaque année au travers du « Hype Cycle » (voir Hype Cycle 2016 version <http://www.gartner.com/newsroom/id/3412017> - Source Gartner group), 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 5 à 10 a

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 data¹⁰.

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 orientée 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 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 clients.
- **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 justement 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/>.

Cet exercice 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 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** (Chief Digital Officer) d'une entreprise qui permettra de garantir une mobilisation totale sur le projet.



3. Les freins





3. Les freins

L'IoT est un marché 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. Cette complexité réside dans le fait qu'un objet connecté est matériel, 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 minimum d'expérience afin de mieux agir et de 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 gourmand en énergie, mais échange 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-middle¹⁴ 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 malware¹ Mirai** ou encore **le botnet² 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.

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 BLE¹¹, le NFC¹², le LiFi²⁵ 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.

¹ **Malware** : Logiciel malveillant développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté.

² **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.



3.9 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 transivité 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 standardisées. 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.

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.

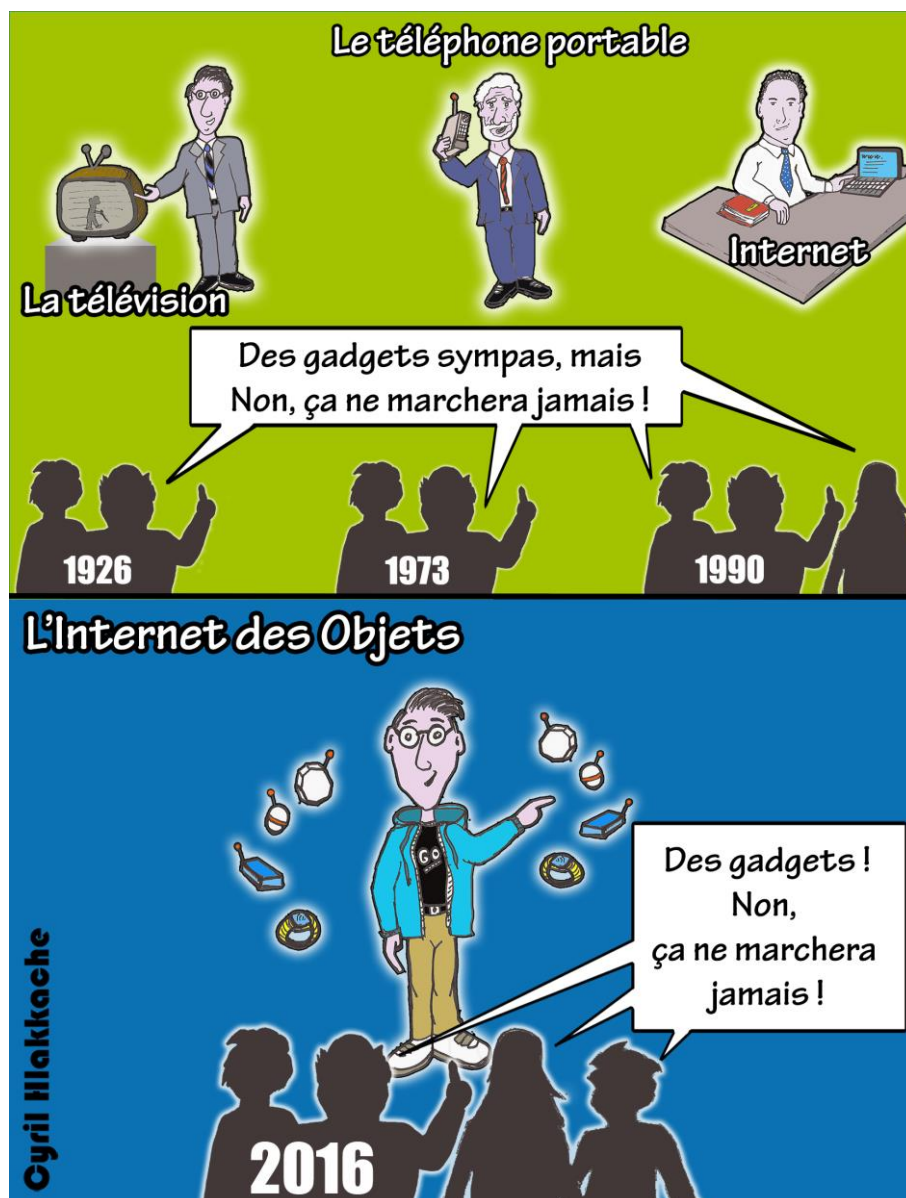
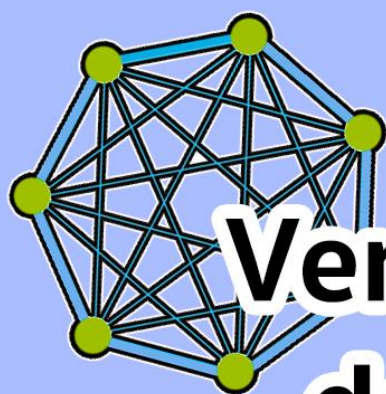
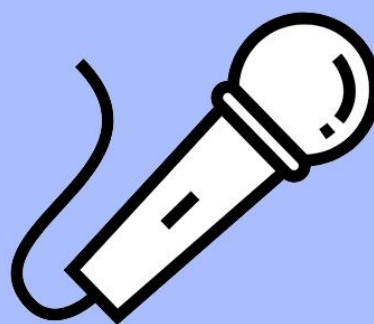


Figure 5 : « Innovation et pessimisme » par Cyril Hlakkache - 2016



Verbatims des acteurs de l'IoT





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 expérience).

*Comme l’illustre [cet enfant de 11 ans](http://mashable.france24.com/) (<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 sécurisée.*

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 ?”*

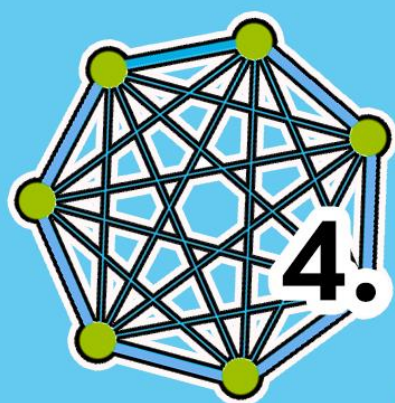


Emmanuel Mouton, CEO et Directeur Général de [Synox](#) (Montpellier, Occitanie) nous dit :

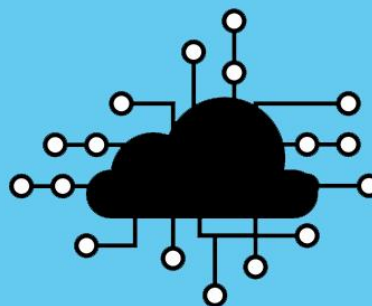
“Les projets d’objets connectés sont désormais passés dans une étape plus mature. Les industriels ont dépassé cette année le cap du Proof of Concept et entament leur transformation numérique grâce à l’IoT.

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’acquies 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. 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'ETSI³. 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'ETSI³ 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'ISO³² au sein de son "Joint Technical Committee 1", dédié aux technologies de l'information en général, ou encore au niveau européen dans l'AIOTI³³, 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'ETSI³ :

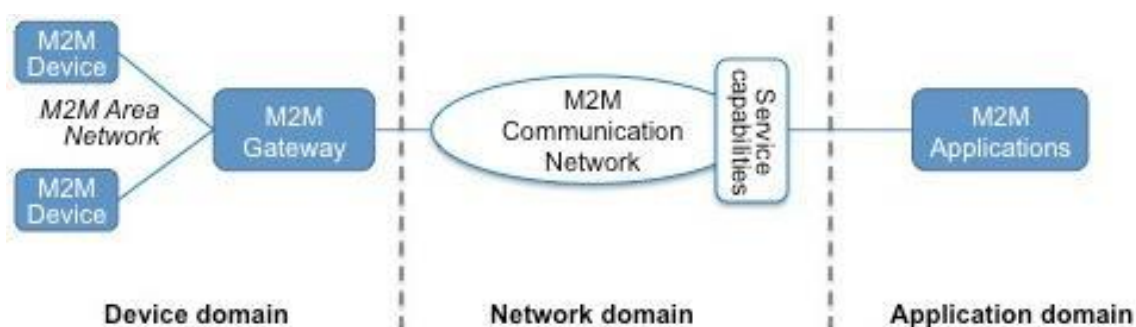


Figure 6 : Modèle d'architecture M2M de l'ETSI

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 Datavue, ...) proposent des plates-formes destinées à l'IoT à travers des solutions spécialisées (PaaS¹⁵). 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.

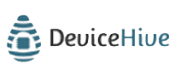
IT Services				
Open source				
Software & cloud				  
Telecom				
Hardware & network				

Figure 7 : Panorama du marché des plateformes IoT (non exhaustif)

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.). Elles peuvent être développées dans une multitude de langages de développement, qui sera choisi en fonction de l'environnement cible (ordinateur, mobile, tablette, montre connectée...), mais



doivent 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" (Android, 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.

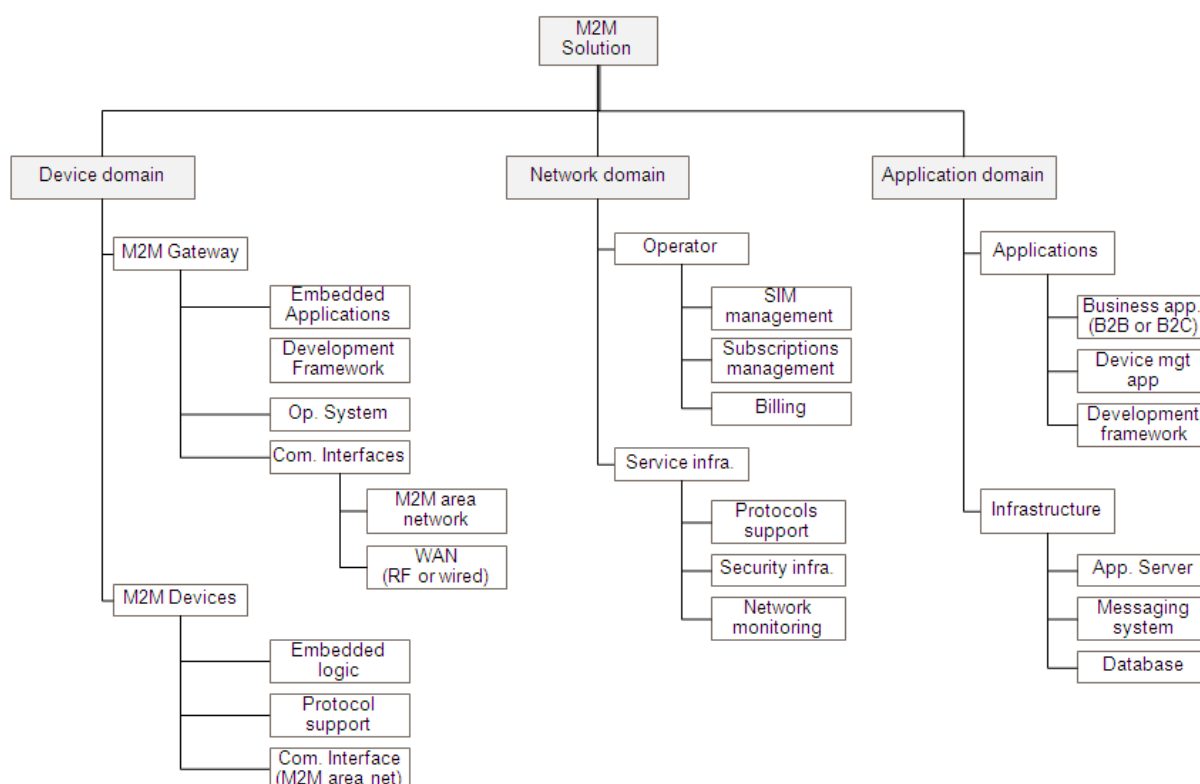


Figure 8 : Organigramme des composants techniques des solutions M2M (source Fusion Labs)



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 (Low Power Wide Area) : EC-GSM-IoT (2G), LTE-M²⁷ (4G LTE catégorie M1), et NB-IoT²⁸ (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 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.



Figure 9 : Passerelle M2M Sierra Wireless GX450 (connectivité 4G, Ethernet, Wifi)

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'actuateurs¹³ 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 :**
 - 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) 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 (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**¹⁷ 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**²⁴ (courants porteur en ligne) utilisés notamment par le désormais célèbre compteur électrique intelligent Linky.

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 CDMA¹⁹, 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 RFCs²¹, 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 CoAP²⁰ ou DTLS²². 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** ou **AMQP** 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 BYOD¹⁶, 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 coexistants dans ces systèmes doivent se mettre d'accord sur 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 (référéncée 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'ultrason, 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 SDK¹⁸ mis à disposition par le constructeur d'une plate-forme 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 (Datavenue), Deutsche Telecom, ...
- **Les plates-formes d'éditeurs ou de sociétés de services** : PTC/ThingWorx, Capgemini-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 plate-formes, 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** (abrégié 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.



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”³**, ou l'émergence du “low tech”.

³ 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. Quelles perspectives sur le long terme ?

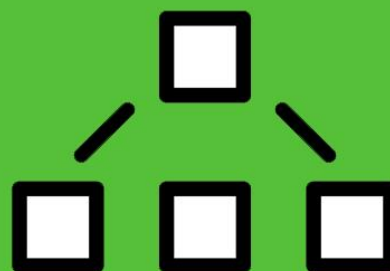
Après avoir assisté à une multiplication des tentatives, nous assisterons à une sélection naturelle autour de quelques normes qui auront fait leurs preuves par le terrain et qui auront su fédérer les énergies nécessaires pour être standardisées.

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





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 favorisé 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. Stratégie 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 **plate-forme 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 autour 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 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 la valoriser. De plus, le fait d'organiser l'ensemble des projets de transformation digital 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 :



Figure 10 : 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 dans 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 que le nombre d'acteurs sont trop importants, 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, 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 fameuses 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 :

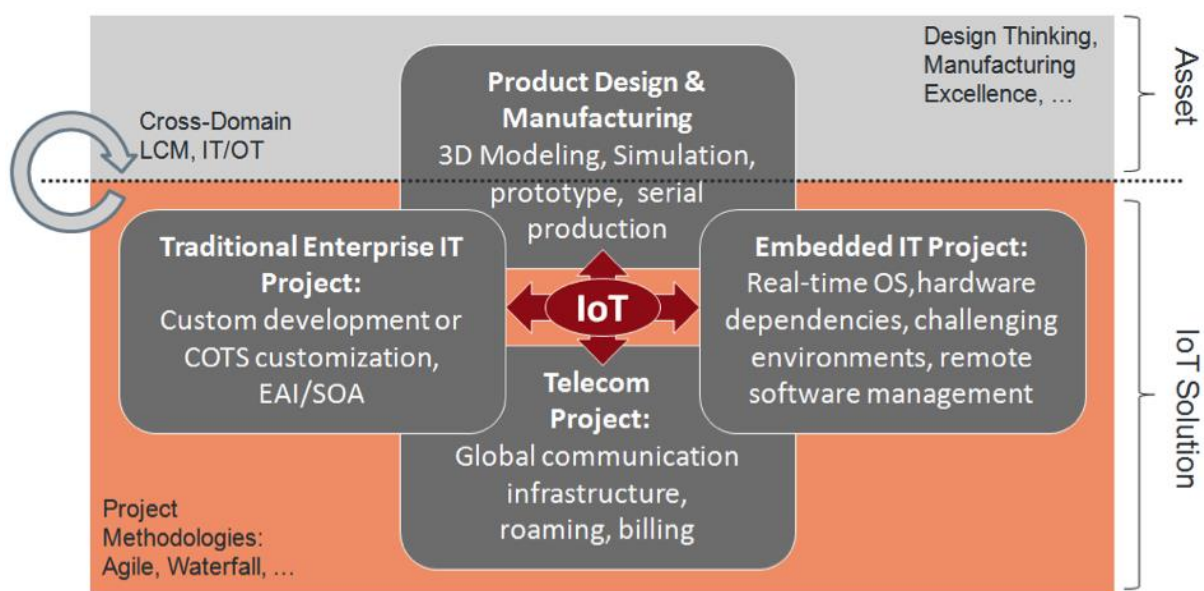


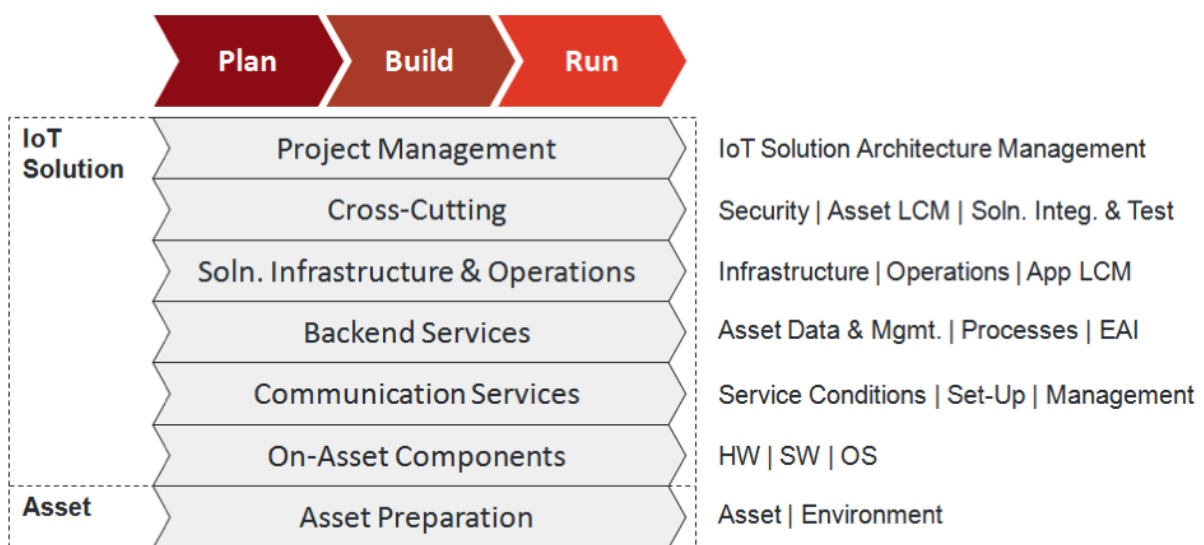
Figure 11 : Multi dimensions of IoT project Management, Source : www.enterprise-iot.org



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

- La conception du **produit** ou du **service**,
- Le conception des **objets matériel** (Hardware, boîtier...)
- 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 :



Source: www.enterprise-iot.org

Figure 12 : IoT Project workstreams, Source : www.enterprise-iot.org

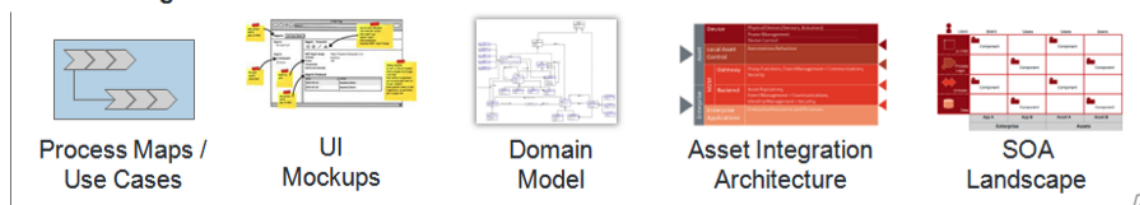
La phase de lancement donne lieu à une conception initiale, suivant 3 axes, décrits dans l'illustration suivante :



Analysis, Projections, Planning ▶



Functional Design ▶



Technical Design ▶



Source: www.enterprise-iot.org

Figure 13 : Ignite Initial Solution Design, Source : www.enterprise-iot.org

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.



Project Dimensions

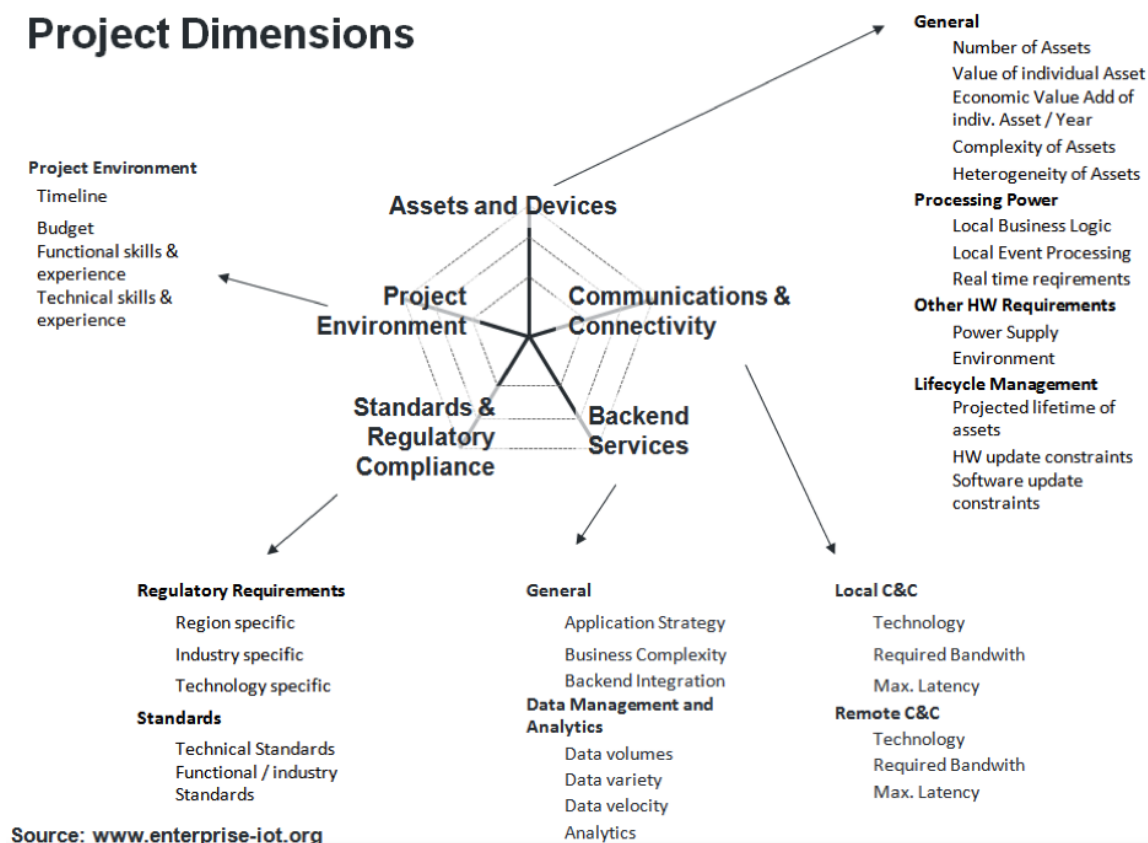


Figure 14 : Schéma de mesure de dimension d'un projet, Source : www.enterprise-iot.org

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 boîtier). 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 (Agile⁴) ou plutôt une conservation des pratiques de l'organisation ?** Dans un marché émergent, difficile de savoir exactement quels seront les attentes des futurs utilisateurs. Il convient donc d'appliquer une démarche "Lean Startup⁵" 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 une 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 formaliser de manière à donner une base solide au projet qui pourra ensuite être 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 organisé autour 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.

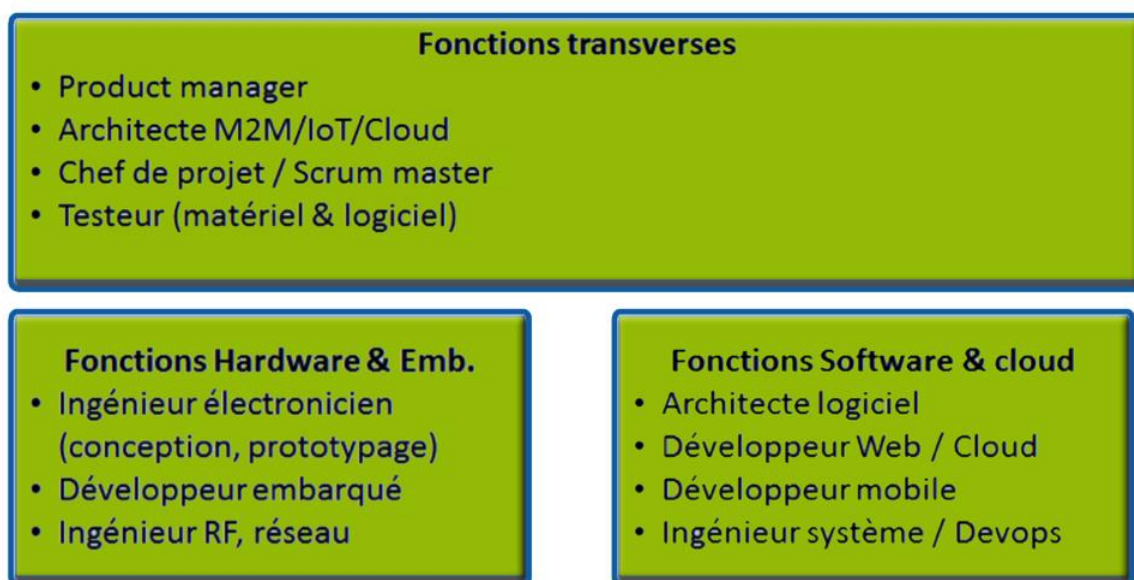
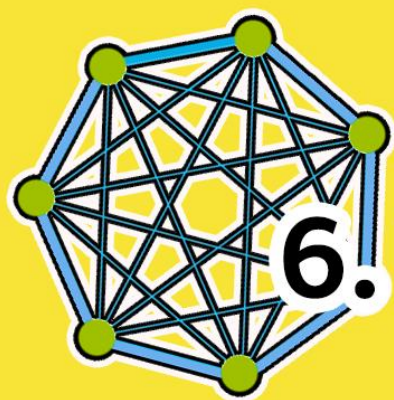


Figure 15 : Panorama des compétences projet.

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** visant à l'alignement de l'ensemble des équipes sur un objectif commun. Cette méthode est née de la volonté à 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 dont la richesse de composant et

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.



6. La collecte des données





6. Stratégie de collecte et de 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 constructeurs variés, de ce fait, pour agréger, utiliser ou comparer les ces données, une phase de **normalisation de la donnée** peut devenir nécessaire avant de les intégrer.

Pour que cette normalisation soit rendu 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 données** 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, car 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.



7. 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 jouant 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, écouteurs-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 vncroulette⁴, 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 temps⁵.
- 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 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.

⁴ Sur vncroulette, voir cet [article](#) pour un résumé

⁵ Sur ce sujet, une illustration très pertinente est [la démonstration du hack de téléviseurs connectés](#) via les canaux de diffusions numérique, permettant la mise en place d'un malware résidant dont la suppression coûte plus cher que le remplacement du dispositif sur 90% des téléviseurs récents.



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 (GDPR⁶)** 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. 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 :

⁶ **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 notions 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.



- **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**, 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 où les ressources sont souvent limitées de par la nature des devices IoT qui n'ont souvent pas la puissance nécessaire pour supporter les solutions de sécurité 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 confiance⁷, 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.

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

⁷ 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'une meilleure intégration logicielle et matérielle



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 qu'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**⁸ (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,
- **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

⁸ **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.



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 SCEP⁹, ou OCSP¹⁰ permettant une gestion OTA des certificats. Ces protocoles d'authentification mis en place dans le cadre de communication TLS¹¹ ou DTLS¹² 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

⁹ **SCEP (Simple Certificate Enrollment Protocol)** : Protocole simple d'enregistrement de certificat développé par Cisco Systems.

¹⁰ **OCSP (Online Certificate Status Protocol)** : Protocole Internet utilisé pour valider un certificat numérique X.509 et qui est standardisé par l'IETF.

¹¹ **TLS (Transport Layer Security)** : Protocoles de sécurisation des échanges sur Internet.

¹² **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.



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,
- **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 précédent¹³ 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 être considérée 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 modifiés que difficilement pour rentrer dans un cadre de sécurité intrinsèque.

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

Malgré les mesures décrites précédemment, les environnements IoT demandent d'explorer de nouvelles voies pour offrir de meilleures garanties de sécurité, 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

¹³ 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 ?



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

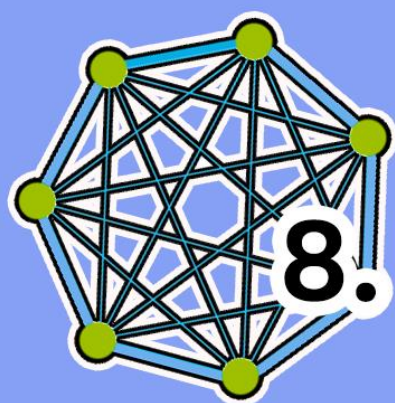
Au niveau des consommateurs, le rétablissement de la confiance passe par une meilleure éducation et une meilleure information. L'éducation doit se faire sur les précautions d'usage à prendre dans la mise en place d'objet connecté et peut se faire lors de l'activation du service en imposant des précautions 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 émergeant 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.

[3] La révocation d'anciens droits est souvent sous-estimée : beaucoup de serrures connectée 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 ?



8. Le juridique





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 16 : "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 et qui répondent à la qualification de « **données personnelles** » au sens de **l'article 2 de la Loi Informatique et libertés du 6 janvier 1978**.

Les données personnelles sont envoyées aux entreprises qui peuvent ainsi mieux connaître leurs clients. Le corps humain va devenir connecté via l'utilisation de capteurs corporels connectés (bracelets, podomètres, balances, tensiomètres) et [d'applications mobiles](#). Conformément à la **Loi Informatique et Libertés**, un traitement ne peut porter que sur des données personnelles qui sont collectées et traitées de manière loyale et licite, pour des finalités déterminées, explicites et légitimes. Cela suppose **l'absence de collecte de données à l'insu des utilisateurs et l'interdiction de procéder à des traitements pour d'autres buts que ceux annoncés**.

Les données collectées doivent être pertinentes et proportionnées à la finalité du traitement et conservées pour une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées. De sorte que le concepteur devra développer une réflexion en amont sur le type de données qui lui seront réellement nécessaires et la durée de conservation de celles-ci.

Le paradoxe des objets connectés réside dans le fait que ce sont les usagers eux-mêmes qui décident quel type de donnée sera collectée, et qui vont ensuite les gérer grâce à une plateforme, ou à un équipement qui va leur permettre soit de prendre une décision, soit de pré-programmer un équipement électronique qui sera actionné en fonction de la valeur qui sera transmise. De sorte que l'usage devient co-responsable de l'utilisation qui est faite des données. Il conviendra donc pour l'opérateur de mettre en place un cadre juridique strict à l'égard des usagers, et de les informer sur ces obligations.

Le **Règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données du 27 avril 2016**, impose un **principe de coresponsabilité**.

Le traitement des données personnelles est d'autant plus important qu'il peut concerner des données sensibles de santé. L'ampleur des « **quantified self** », objets qui mesurent la température du corps ou du rythme cardiaque, repose selon la **CNIL** sur la collecte et le traitement de données dites « sensibles » qui, à cet égard, doivent faire l'objet d'une protection renforcée. Le caractère sensible de ces données tient à leur communication à des tiers, tels que les assureurs.

D'autres données, comme les données de géolocalisation des individus, ne sont certes pas classées « sensibles », mais doivent faire l'objet d'une vive attention. Si ces données viennent à être détournées, elles pourraient être très utiles aux [cybercriminels](#). La géolocalisation fait l'objet de toutes les craintes, craintes alimentées par **la loi relative à la géolocalisation du 28 mars 2014**.



Cette loi prévoit que dans le cadre d'une enquête et sous l'autorité d'un juge, les enquêteurs peuvent avoir recours à « tout moyen technique destiné à la localisation en temps réel » d'une personne, « d'un véhicule ou de tout autre objet ». Pour garantir le développement du marché des objets connectés, il devient nécessaire d'assurer aux individus le respect de leurs droits et ainsi de rassurer le consommateur. Les industriels ne doivent donc pas faire l'impasse sur la sécurité du produit dès la conception.

Les manquements aux obligations édictées par la **Loi Informatique et Libertés** et le **Règlement européen** sont pénalement sanctionnés. S'agissant des amendes administratives, elles peuvent s'élever, selon la catégorie de l'infraction, de 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, de 2% jusqu'à 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

8.2 La responsabilité du fait des objets connectés

Les objets connectés sont des dispositifs permettant de collecter, stocker, transmettre et traiter des données issues du monde physique. Ce sont des sources de données, identifiés et identifiables de façon unique et ayant un lien direct ou indirect avec Internet.

Des millions de capteurs connectés ont désormais intégré les objets du quotidien. Via une application mobile ils sont amenés à collecter, analyser, stocker et restituer une multitude de données en rapport avec un individu, son environnement, sa consommation, ses habitudes, son hygiène de vie ou encore sa santé. Ces nouveaux usages impliquent la mise en œuvre de la responsabilité des utilisateurs, des connectiques et des opérateurs d'une manière nouvelle. La question de la responsabilité des objets connectés recouvre donc plusieurs facettes et impliquent plusieurs acteurs. Les principes fondamentaux de la responsabilité sont exposés dans les **articles 1240 et suivants du Code civil**. « Tout fait d'une personne qui cause à autrui un dommage oblige le responsable à réparer le préjudice de la victime. » Selon l'**article 1242 du Code civil** « On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde ».

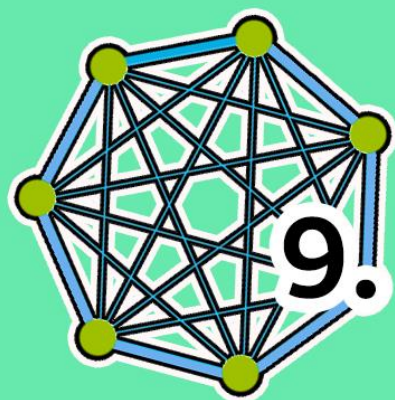
Ainsi on peut être déclaré responsable des objets connectés que l'on a sous sa garde, notamment ceux que l'on utilise ou sur lesquels on a un contrôle exclusif. Mais la responsabilité de l'auteur du dommage peut remonter à un tiers quand la personne ou la chose est sous sa surveillance, comme le prévoit les **alinéas 4, 5 et 6 de l'article 1242 du Code civil**.

Par rapport à l'éventualité des objets connectés de conclure un contrat en leur nom propre, selon l'**article 1101 du Code civil**, un contrat est passé uniquement entre des personnes. Ainsi les objets connectés, même ceux dotés d'une intelligence artificielle ne pourront en principe rentrer dans cette catégorie. De même, seule une personne peut être titulaire d'un mandat et conclure au nom et pour le compte d'une autre personne.



Ainsi, concernant la responsabilité des objets connectés il convient de rester sur le principe de base : **la responsabilité s'applique pour tout objet que l'on a sous sa garde**. Que l'objet soit connecté ou non ne permet pas de traiter la responsabilité de manière différente. La notion de garde pourrait être étendue à celui qui surveille à distance des équipements électroniques par tous moyens.

Or des études ont révélé 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. Les interceptions frauduleuses, mais aussi l'intrusion frauduleuse dans un système d'information sont des infractions pénales. De sorte que des chaînes de responsabilités civiles et pénales pourraient être mises en œuvre en cas d'attaque.



9. La formation





9. 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 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)...

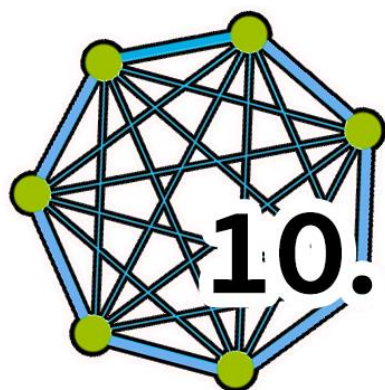
Exemple de formations académiques :

- **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](#).

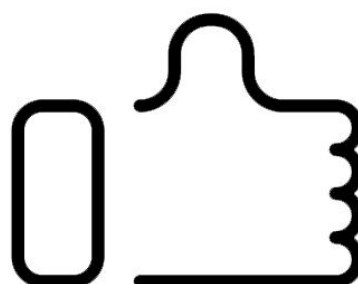
Exemples de formations professionnelles :

- 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 formation IOT.



10. Conclusion





10. Conclusion

Ainsi, bien que tous les standards ne soient pas encore bien établis et que les freins, comme les inconnus, soient encore nombreux, l'IoT est un marché émergent 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...

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'unité 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 chaîne d'approvisionnement, capteurs et actionneurs dans nos usines automatisées...

Demain, des composants électroniques autonomes en énergie et à extrêmement faible coût (*energy harvesting*) intégreront 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 le capteur 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 chaîne 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, chaînes 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
- [The noun project](#)

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.

- Figures 1, 2, 3, 6, 7, 15 : courtoisie de **Fusion Labs**
- Figure 4 : source **Flickr PhilCaz**, Licence CC BY-SA 2.0
- Illustration 5 et 16 : courtoisie de **Cyril Hlakkache**
- Figure 9 : courtoisie de **Sierra Wireless**
- Figures 10, 11, 12, 13, 14 : source **enterprise-iot.org**, Licence CC BY 3.0

Licence

Cet ouvrage est distribué en licence **Creative Commons BY 3.0**





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

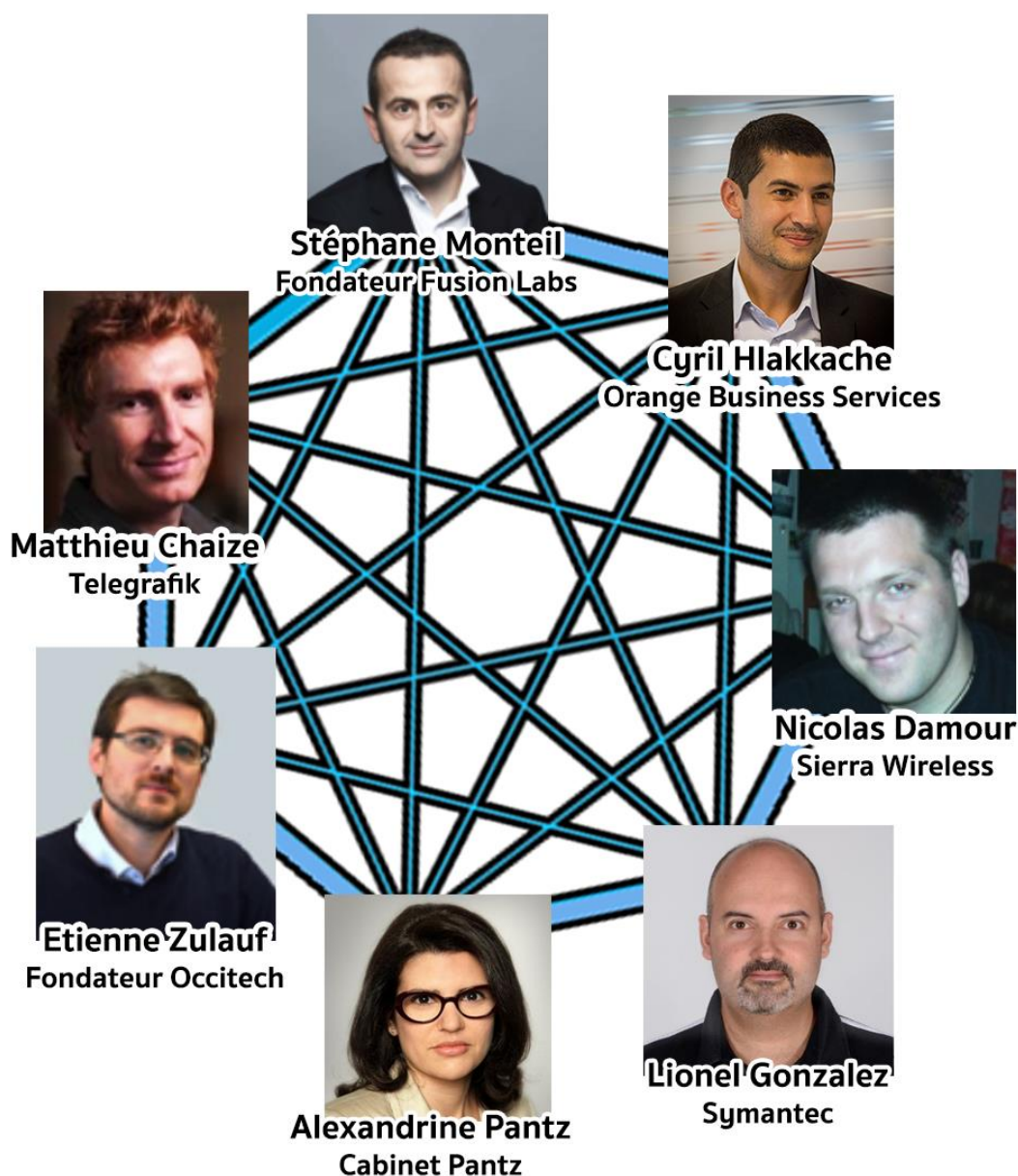
PORTES SUD, BAT 3

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 2** du livre blanc :
«**Panorama de l'Internet de Objets**» !**