

2019 | 2022

IOT INTERNET DES OBJETS



POLESCS

MISES A JOUR 2021

AXE STRATEGIQUE PHASE 4.0

TABLE DES MATIERES



La mise à jour 2021 est stipulée par un filet vertical vert sur le côté des "paragraphes du texte concerné."

est stipulée par un filet vertical vert sur le "texte" et de l'annotation MAJ* dans le titre

LE MOT DU PRESIDENT	3
SYNTHESE DES MISES A JOUR (SUITE COVID-19)	4
1. Description et périmètre de l'IoT	6
1.1 Présentation de l'IoT et des enjeux génériques	6
1.2 Périmètre de l'IoT au sein du Pôle SCS	9
1.3 Enjeux génériques pour l'IoT	9
2. Références/Liens/Position avec les stratégies régionales et nationales	11
2.1 Des initiatives engagées au niveau régional, national et européen	11
2.2 Synergies entre l'IoT et les autres axes stratégiques du Pôle	13
3. Chaîne de valeur et cartographie des acteurs	13
4. Marchés et usages cibles	16
4.1 Marchés prioritaires	16
4.2 Dimensionnement des marchés cibles	17
4.3 Opportunités marché liées aux évolutions réglementaires et sociétales	24
5. Verrous et enjeux technologiques	25
5.1 Etat des lieux	25
5.2 Les verrous prioritaires	25
5.3 Projets en cours	27
6. Enjeux de formation	27
6.1 Etat des lieux	27
6.2 Enjeux autour de formation	28
7. Soutien & croissance des Startups & PME	29
7.1 Etat des lieux	29
7.2 Enjeux	30
8. Visibilité & attractivité & communication	32
8.1 Etat des lieux	32
8.2 Enjeux	32
9. Plan d'actions	33
10. Annexes	35



LE MOT DU PRESIDENT

Chers membres, chers partenaires,

LA PHASE 4.0 des pôles de compétitivité a démarré pour la période 2019 à 2022. SCS a été sélectionné pour cette PHASE 4.0 et a choisi un positionnement dans la continuité avec quatre axes stratégiques dont l'Internet des Objets (IoT) avec une feuille de route à construire pour les 4 prochaines années.

Expert du domaine de l'IoT et des objets connectés, SCS accompagne les projets innovants, soutient les startups et PME du domaine et structure l'écosystème via l'animation d'un groupe thématique « IoT » depuis 2015.

Les membres SCS conçoivent et développent des solutions IoT éprouvées pour de nombreux domaines d'application depuis les mesures et le suivi dans le secteur industriel et logistique, en passant par les capteurs intégrés dans les « smartcities » jusqu'à la gestion multi capteurs toujours plus performants et provenant de sources hétérogènes dans un véhicule autonome.

Dans le contexte des événements sanitaires exceptionnels de l'année 2020 et 2021, SCS a souhaité mettre à jour cette feuille de route avec l'appui d'experts du domaine et dans une démarche collective.

Cette contribution « collective » à la mise à jour de la feuille de route est essentielle pour l'ensemble des acteurs de l'écosystème SCS mais aussi pour les financeurs de SCS. Elle permettra de construire un positionnement robuste et visible au niveau européen, et aussi d'orienter les actions (notamment les animations) pour l'écosystème IoT & objets connectés.

Moussa Belkhiter,

*Président de SCS
& Site Manager de NXP Semiconductor
Sophia Antipolis*

"Nous remercions les personnes suivantes pour leur contribution à la mise à jour de la feuille de route en 2021"

*Paul Vincent BONZOM
Directeur laboratoire
CEA Tech*

*Romain PALMADE
CEO
CENTILOC*

*Philippe PANNIER
Directeur laboratoire
IM2NP/AMU*

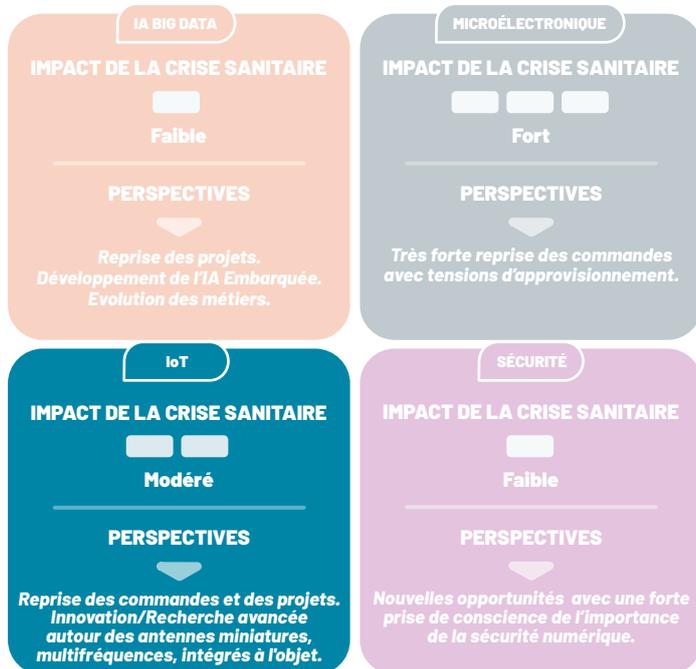
LA PRESENTE FEUILLE DE ROUTE A POUR VOCATION

De décrire le marché
et son périmètre

D'identifier les enjeux,
les acteurs, les opportunités
liés à l'IoT

De préciser des objectifs
et les actions principales
sur la période

SYNTHESE DES MISES A JOUR (SUITE COVID-19)



Cette pandémie nous a fait prendre conscience qu'on ne peut tout prévoir et **souligné l'importance accrue d'avoir une stratégie proactive pour le futur**. Les technologies, les solutions et/ou produits devront être agiles et protégés efficacement avec des systèmes de sécurité très élaborés.

Les vulnérabilités aux attaques cyber, l'hyperconnectivité, les déluges de données, la diffusion de technologies de rupture comme le quantique, l'IA, l'émergence de nouveaux usages, l'accélération de certains marchés imposent de **repenser l'innovation et de miser encore plus qu'avant sur les écosystèmes et les compétences**.

Il y a une **volonté politique forte, française et européenne de soutenir la filière numérique** et les aides gouvernementales ont été exceptionnelles.

Cette crise a aussi révélé **l'agilité de nos entreprises et montré la pertinence des coopérations entre start-ups, grands comptes et organismes de recherche**.

Les membres SCS ont saisi ces opportunités avec des premiers résultats très encourageants sur l'innovation générée, les perspectives de développement de certaines entreprises et les futurs investissements locaux contribuant à la souveraineté technologique, recherchée par les pouvoirs publics.

La région Provence-Alpes Côte d'Azur a des atouts indéniables dans le domaine du numérique, et cette pandémie nous démontre la pertinence de la coopération entre le monde académique et les industriels, qui va contribuer au rayonnement international de ces acteurs.

Dans le domaine de l'IoT, la pandémie a eu un impact sur certains marchés. **La tension sur les composants électroniques a créé des tensions dans la réalisation d'objets et de produits connectés**. Des filières ont arrêté ou décalé des projets d'IoT. A l'inverse, des secteurs qui faisaient grise mine en 2019 à l'image du Smart Retail ou e-commerce ou AgriTech, reprennent des couleurs en cette année 2021.

Marchés, tendances et chaîne de valeur

Des opportunités sur 3 marchés sont apparues depuis 2019

➤ **L'Agriculture connectée et « intelligente »** émerge avec de nouvelles applications « éco responsables » pour optimiser les engrais, les irrigations, surveiller des maladies, ... Des besoins en capteurs plus petits plus performants... apparaissent et de nouveaux réseaux d'objets connectés (LoRa, ...) sont installés. Enfin, on constate une utilisation importante de l'IA pour analyser les données (météo..).

➤ **Les Villes « intelligentes »** (smart, safe and green cities) utilisent aujourd'hui massivement les biens de consommation courante (véhicules connectés, compteurs connectés, caméras de surveillance « intelligentes » ...). Les réseaux de type 5G commencent à être opérés. Là encore, l'implémentation d'IA est accélérée (Cloud, Edge) pour différents types de données : météo, environnementales, trafic, ...

➤ **L'Industrie du futur** à travers la digitalisation des usines s'est accélérée pendant la pandémie avec de nouveaux services, nouvelles fonctionnalités au sein des sites de production. Une utilisation massive sur des réseaux type 5G est à prévoir ainsi qu'un usage intensif de l'IA pour automatiser les process, prédire les pannes...

Verrous technologiques

Les verrous technologiques de la Feuille de route en 2019 **sont toujours d'actualité** mais **de nouveaux apparaissent ou prennent de l'importance**.

Les laboratoires de recherche font face à une demande accrue de **miniaturisation & intégration d'antennes** (*multi fréquences*), mais aussi de **sécurité des objets** (*au niveau composant, système ou communication*). Enfin, la **gestion de l'énergie** et la récupération de l'énergie (*issue de tout type de sources possibles dans l'environnement de l'objet*) **devient un verrou technologique majeur**.

Le déploiement de la 5G va aussi entraîner des modifications technologiques sur les architectures IoT notamment celles qui n'intégraient pas des fonctionnalités cellulaires. Si les **réseaux « ad-hoc »** sur des fréquences libres tels que **LORA** et **Sigfox** vont pouvoir continuer à être positionnés sur des applications spécifiques, les investissements et les moyens mis en œuvre par les opérateurs et fournisseurs de technologies 5G vont entraîner certains bouleversements des approches technologiques de l'IoT. *Par exemple, Ericsson a récemment annoncé la disponibilité de solutions 5G privée pour les industries.*

Nouveaux Usages

Un Impact majeur sur les usages de 2 marchés qui ont « explosé » pendant la pandémie :



Dans le domaine Santé à domicile, le contexte sanitaire et les restrictions de sorties a permis une généralisation de la **téléconsultation** avec des **télémesures**. A l'hôpital, la surcharge des hôpitaux et la prise en charge du patient se sont accélérées: une optimisation de la prise en charge a été nécessaire. Enfin, le **Track and trace pour les vaccins**, les médicaments et les respirateurs est devenu stratégique pendant la pandémie.



Dans le Commerce, au niveau des magasins (*Smart Retail*), le Click and Collect s'est démocratisé et **la vue en temps réel des stocks des magasins** (*afin de faciliter le Click and Collect*) s'est révélée fondamentale. Zara et Décathlon étaient déjà organisés avec un déploiement massif du RFID. D'autres magasins équipés de **Smart shelves** grâce à la **technologie NFC** ont pu voir en temps réel leurs stocks. Certains fournisseurs de solutions IoT ont accéléré leur développement grâce à ces technologies innovantes (*Ex : Centiloc*)... Grâce aux caméras, la vérification du bon respect des gestes barrières, comme la distanciation sociale des clients et personnels dans un commerce a été facilitée.



Formations

Des formations sont apparues depuis 2019 mais ont surtout évolué grâce à l'implication d'industriels dans l'élaboration du contenu des programmes de formation.

Une grande tendance constatée depuis la pandémie est une **très forte demande en apprentissage** qui est aussi une volonté gouvernementale. Suite à une demande forte des industriels de la région, Polytech Marseille prépare par exemple un nouveau diplôme d'ingénieur par apprentissage : ingénieur IoT (*rentrée 2022*).

Le nouveau **projet PIA Innovation-micro et le campus des métiers** répondent bien aux enjeux de formation exprimés en 2019 : sensibiliser les jeunes aux métiers de l'électronique, former des ingénieurs aux enjeux à venir (*IoT, IA, industrie 4.0...*) et reformer les ingénieurs en poste à ces nouveaux métiers.

Les formations d'ingénieurs évoluent avec l'ajout de nouvelles options ou parcours de formations à partir de la 4^{ème} ou 5^{ème} année. En Provence-Alpes-Côte d'Azur, **10 Masters proposent des formations IoT** (*Master informatique / télécommunication ou microélectronique avec des parcours IoT*).

Un nouveau Master « Réseaux et télécommunications - parcours IoT » co-habilité entre AMU et l'École des Mines de Saint-Étienne à Gardanne est prévu pour septembre 2021. Ce master a pour objectif de former par alternance des futurs ingénieurs aux problématiques de la chaîne IoT de développement et plus spécifiquement autour des objets connectés sécurisés.

Enfin une révolution, la **transformation des DUT en BUT** (*Bachelor*) BAC+3 est en marche avec des programmes en cours et qui seront finalisés fin 2021.

1. Description et périmètre de l'loT

1.1 Présentation de l'loT et des enjeux génériques

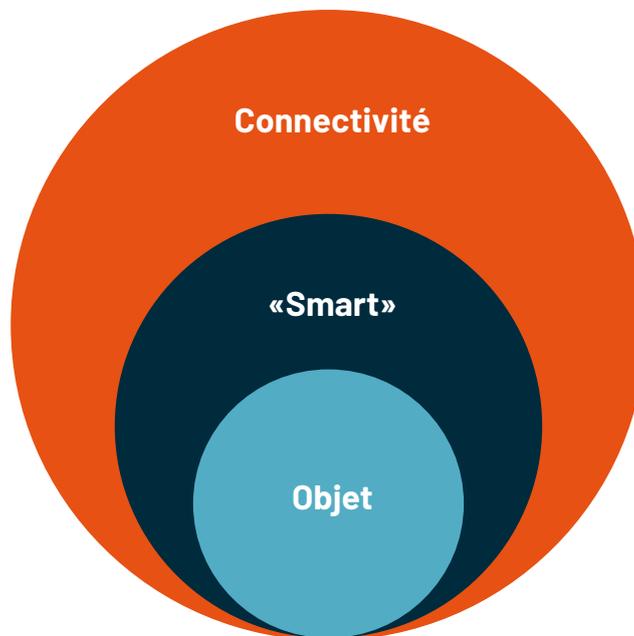
L'**Internet des objets** (*Internet of Things*) souvent appelé **loT** est un écosystème mondial, réseau de réseaux, il permet de disposer de services évolués en mettant en réseau des objets connectés grâce à des technologies de l'information (*réseau, M2M, cloud...*). C'est un domaine très large et pluri technologique qui sollicite un ensemble de briques technologiques clés comme les composants et capteurs, les machines intelligentes, la connectivité et les réseaux, la collection et l'analyse des données (*edge et cloud computing*), l'automatisation des décisions.

Au cœur de cet écosystème, les **objets connectés** sont des types d'objets dont la vocation première n'est pas d'être des périphériques informatiques ni des interfaces d'accès au web (*e.g. brosse à dent, machine industrielle...*), **mais auxquels l'ajout d'une connexion Internet a permis d'apporter une valeur supplémentaire en termes de fonctionnalité, d'information, d'interaction avec l'environnement ou d'usage.**

Ils comportent :

- les **composants physiques** incluant les **parties mécaniques et électriques du produit...**
- les **composants** dits « **Smart** » incluant les capteurs, les microprocesseurs, le stockage de données, les commandes, les logiciels et généralement **un système d'exploitation.**
- les **composants connectés** comprennent les ports (*USB...*), antennes et protocoles **permettant une connexion avec ou sans fils avec le produit.**

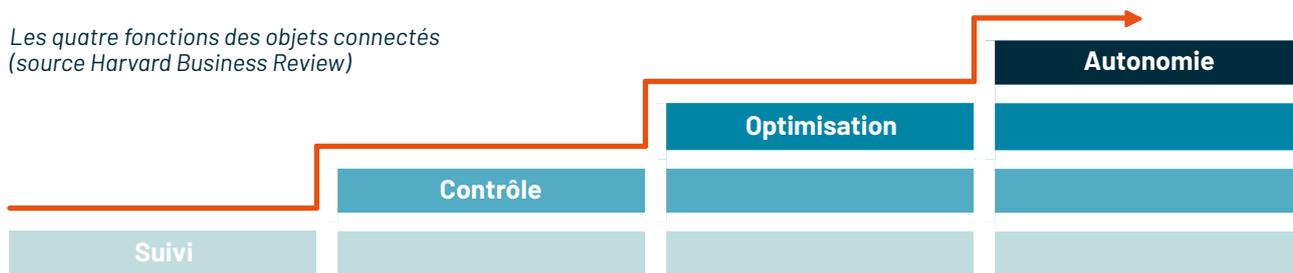
3 composants d'un objet connecté :



Sources : Harvard Business Review

Les objets connectés remplissent 4 grands types de fonction : **suivi, contrôle, optimisation et autonomie.**

Les quatre fonctions des objets connectés
(source Harvard Business Review)



1

2

3

4

Les capteurs et les sources de données externes permettent un suivi attentif :

- Des conditions du produit
- De l'environnement externe
- Des usages du produit

Ce suivi permet de notifier et d'alerter sur les changements.

Les logiciels embarqués dans la mémoire du produit permettent :

- Un contrôle des fonctionnalités du produit
- Une personnalisation de l'expérience utilisateur
- Une prise en compte des commandes extérieures (*renvoi d'informations vers l'objet/actuation*)

Les capacités de suivi et de contrôle permettent la création d'algorithmes qui optimisent le fonctionnement et l'utilisation du produit dans le but de :

- Améliorer les performances du produit
- Permettre de prédire des diagnostics, des services et des réparations

Combiner le suivi, le contrôle et l'optimisation permet :

- Un fonctionnement autonome du produit
- Le fonctionnement auto-coordonné avec d'autres produits et systèmes
- Une personnalisation et amélioration autonome
- Un auto-diagnostic

Le marché de l'Internet des Objets a :

dépassé le
MILLIARD D'€
en France
en 2017¹

en 2020
prévision mondiale entre
30 et 80
MILLIARDS D'IOT
(source DGE)²

CROISSANCE
11%
du marché mondial
du numérique
en 2023
(source McKinsey)

Tous les secteurs de l'économie sont touchés. Les applications de l'IoT concernent les individus et les entreprises avec de nombreux cas d'usages.

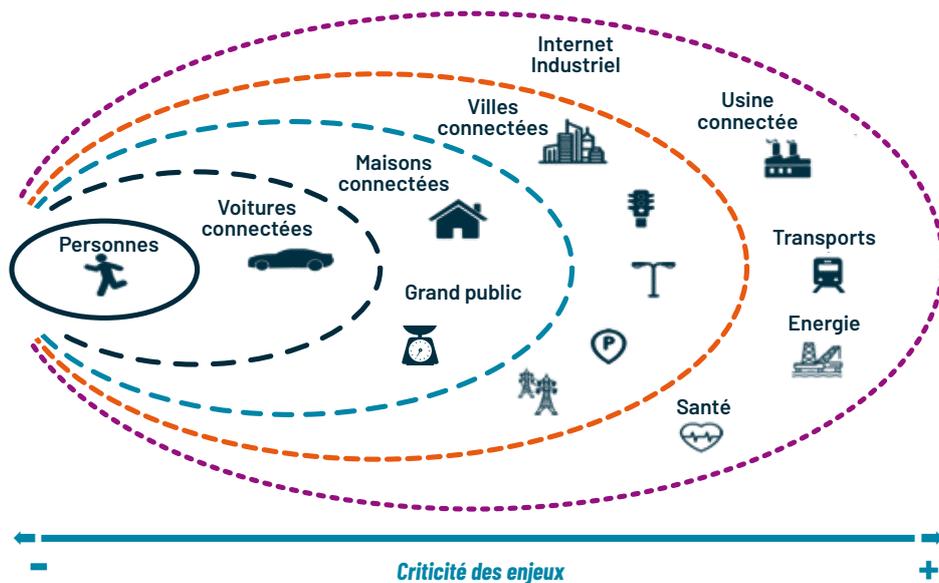
Si les objets connectés grands publics sont déjà largement répandus (*mesures de ses données physiologiques, quantified self...*), on assiste maintenant à la montée en puissance des applications industrielles et le développement des applications prédictives (*maintenance prédictive...*).

Selon Gartner, les marchés professionnels devraient représenter entre :

40 et 50%
des applications en 2020 et une majorité du marché en valeur (*estimation Gartner*).

¹ <https://www.gfk.com/fr/insights/press-release/objets-connectes-le-cap-du-milliard-deuros-franchi/>

² <https://www.entreprises.gouv.fr/etudes-et-statistiques/marches-des-objets-connectes-a-destination-du-grand-public>



Verticaux d'adoption prioritaires (Sources : KPMG Knowledge & Research, Goldman Sachs analysis)

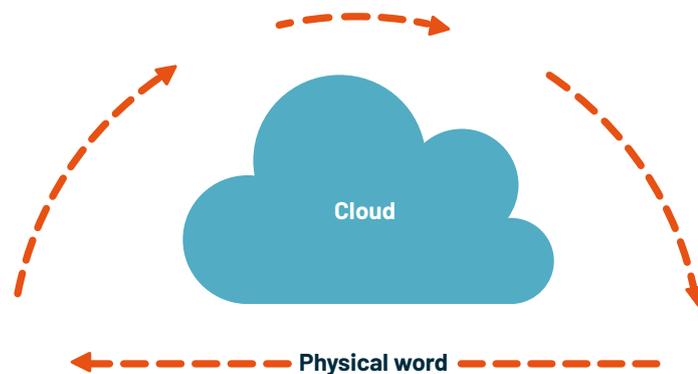
Perspectives

Longtemps limité à des cas d'usages à base de données simples, l'IoT est en train d'évoluer vers la prise en compte de données de plus en plus complexes (e.g. vidéo) pour des services de plus en plus performants.

La conjonction de l'IoT et de l'intelligence artificielle permet le déploiement de nouveaux cas d'usage per-

mettant de passer de la collecte d'information et du monitoring à l'action et à la prédiction (*maintenance prédictive, commande automatique d'actuateurs..*).

La disponibilité, le traitement, l'analyse et la sécurité des données deviendront des enjeux majeurs de l'IoT dans les prochaines années.



	Sensors	Data aggregation	Analytics	Decisions and automation
High-value video analytics	Cameras or vision sensors with video capability	Complex visual-data feeds	Advanced pattern recognition	Multidimensional decisions and multiple variables
Low-value typical IoT	Low-complexity sensors	Binary data	Linear algorithms	Single-variable and linear decision models

Data challenge for new services - Source McKinsey³

³ <https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/the-internet-of-things-how-to-capture-the-value-of-iiot>

1.2 Périmètre de l' IoT au sein du Pôle SCS

Dans le **secteur de l'internet des Objets**, le Pôle SCS rassemble un écosystème très dynamique en croissance composé d'acteurs industriels (*PME et grands groupes*) et académiques positionnés sur les différents éléments de la chaîne de valeur du hardware aux applications.

Les expertises fortes en Microélectronique, BigData & IA, Sécurité Numérique, et, plus particulièrement sécurité de l'Internet des Objets, enjeu majeur de ce secteur sont un des atouts clés.

On peut citer particulièrement :

- **Les objets connectés et sécurisés** pour des marchés B2B sur technologies de communication faible consommation (*Low Power :RFID, BLE, SIGFOX, LORA, ...*) et 5G.
- **Les technologies d'antennes** et de report d'antennes sur différents supports.
- **L'intégration hétérogène de puces** électroniques dans de petits systèmes autonomes et sur des supports souples.
- **L'utilisation de technologies d'energy harvesting** (*récupération d'énergie*) et l'intégration de capteurs innovants.
- **Le développement d'applications** mobiles et d'application métiers en liaison avec les objets.
- **La Sécurité de l'Internet des objets** avec à la fois une expertise très pointue sur les composants et les protocoles associée à une expertise reconnue sur les différents maillons de la chaîne (*logiciel, cloud*) permettant d'aborder la sécurité de bout en bout.

Ce périmètre n'est pas figé et évolue en fonction du renforcement de certaines expertises ou secteurs technologiques.

En complément, l'écosystème est riche des entreprises des pôles sectoriels présents en région (*Eurobiomed, Optitec, Pôle Mer, Pôle Safe, Cap Energies...*) **qui commencent à intégrer l' IoT dans leur évolution** : connexion de leurs produits, utilisation de l' IoT pour l'efficacité opérationnelle de leur entreprise (*logistique, relation client...*).

Le Pôle SCS a déjà lancé plusieurs initiatives et place l' IoT au cœur de sa feuille de route 2019-2022.

1.3 Enjeux génériques pour l' IoT

1.3.1 Enjeux pour le développement du marché de l' IoT

Même si la croissance du marché de l' IoT est importante et que la diffusion des objets connectés grand public est significative, le marché est encore en phase de démarrage avec les applications industrielles.

Les enjeux principaux pour le développement de l' IoT sont les suivants :

Interopérabilité et connectivité : Multiplicité des modes de connectivité actuels et en développement

Connectivité

- Low Power Wide Area Networks/LPWAN (*Lora WAN, NB-IoT, Sigfox, Ingenu etc.*) en phase de déploiement.
- Réseaux IoT opérés (*Ingenu, Orange, Objenious, Sigfox...*) ou non opérés.
- Réseaux cellulaires 5G, 4G/LTE avec un déploiement en cours.
- Solutions courte portée sans licence mais avec limitations (*WIFI, Bluetooth, Zigbee, Thread etc.*).

Interopérabilité

Nombreuses plateformes pour des applications sectorielles ou maîtrisées par des gros acteurs de l'internet (*Amazon, Microsoft Azure, PTC, Carplay, Android auto, Healthkit, Plateforme Somfy...*) mais à ce jour le marché est fragmenté permettant difficilement de connecter des objets de différents fournisseurs ou éco-systèmes.

Sécurité

Avec 20 ou 30 milliards d'objets connectés anticipés en 2020 (*source McKinsey*) la prise de conscience en matière de sécurité est maintenant réelle, cependant cela ne se traduit pas encore dans les cahiers des charges des donneurs d'ordre et la prise en compte effective de la sécurité de l' IoT par les organisations n'est pas encore suffisante.

Les récentes avancées dans le domaine de la certification sécuritaire de l' IoT vont permettre de donner un cadre de référence normalisé. La sécurité des composants et des protocoles sont des maillons indispensables pour une sécurité de bout en bout.

La sécurité des données privées est également un enjeu majeur (*quantified self, médecine connectée en particulier*). La prise en compte d'approches de type décentralisée comme la Blockchain va aussi concerner l' IoT.

En outre, la problématique de sécurité se complexifie de manière significative : les ressources CPU nécessaires au bon fonctionnement des technologies sont trop faibles et la surface d'attaque augmente considérablement avec la multiplicité des connexions d'objets et de systèmes vers des infrastructures critiques (*ICS, SCADA...*).

Autonomie et maîtrise de l'énergie

L'autonomie des capteurs et des objets est un enjeu majeur pour le déploiement de multiples applications nécessitant souvent des durées de vie jusqu'à 10 ans.

► Miniaturisation

La miniaturisation des objets, leur intégration optimisée et l'intégration des antennes, dans une optique d'augmenter les performances, réduire la consommation et les coûts sont très complexe.

► Disponibilité et capacité de traitement des données IoT

McKinsey estime que les données de l'IoT représenteront 10% des données mondiales dès 2020.

La capacité d'accéder et de traiter des données fiables est un enjeu majeur pour le développement de services avancés. La valorisation de ces données et la répartition de la valeur est un enjeu majeur du développement de l'IoT.

► Accompagnement de l'« IoTisation » des entreprises

Dans leur démarche de digitalisation et d'augmentation de l'efficacité opérationnelle.

Une étude menée auprès d'acteurs du marché conforte ces éléments :

Six points de blocage à lever par les écosystèmes IoT

(France 2015, échantillon de 50 acteurs du marché)



Sources : Etude Markess - 2015 (source KPMG)

1.3.2 Enjeux pour les acteurs de l'IoT

- **Maîtriser** les technologies nécessaires (*existantes et en évolution*).
- Contrôler les technologies spécifiques aux marchés en termes d'**IPs** et de **standardisation** de nouvelles technologies.
- Se maintenir à l'état de l'art et innover pour répondre aux défis de la **miniaturisation**, de l'intégration et de la **sécurité numérique**.
- Investir la **chaîne de valeur** et éviter la présence monopolistique des poids lourds de l'Internet au niveau des plateformes en nuage avec un risque de captation de la valeur générée par les données au détriment des objets et des composants.
- Limiter la « **commoditisation** » des objets et des composants (*avec peu de valeur ajoutée*) avec une différenciation forte (*contrôle de l'énergie, interopérabilité, miniaturisation, sécurité...*) tout en ayant la compétitivité nécessaire pour être présent sur un marché de volume.
- S'intégrer dans les différents **écosystèmes sectoriels** ou de plateformes qui vont structurer le marché à terme après une phase de consolidation.
- Maîtriser la chaîne des **données** (*disponibilité, sécurité, analytics, IA...*) pour être à la pointe des **services à valeur ajoutée** de demain.

2.

Références/Liens/Position avec les stratégies régionales et nationales

2.1 Des initiatives engagées au niveau régional, national et européen

Le Pôle SCS contribue aux stratégies européennes, nationales et régionales sur les filières impliquant l'IoT afin de mettre en avant **les atouts et spécificités de son écosystème**.

Conscient de l'opportunité représentée par l'IoT et des enjeux associés, le Pôle s'est très vite impliqué sur l'IoT.

Un groupe de travail très actif a été créé dès 2016 regroupant plus de 130 membres sur l'ensemble de la chaîne de valeur.

Ce groupe thématique a pour objectif la réflexion sur les enjeux & verrous technologiques, et l'émergence de projets. Il inclut des acteurs majeurs de l'écosystème grands groupes, PME et startups, académiques.

La filière IoT s'inscrit dans plusieurs stratégies et actions aux niveaux Europe, France et Région :

NIVEAU EUROPEEN

Le Pôle SCS suit attentivement les initiatives développées au niveau européen pour se positionner, contribuer ou pour être à même de conseiller les membres de l'écosystème.

Participation au Réseau EE Silicon Europe⁴ qui se positionne comme le point d'entrée pour les solutions innovantes, base d'innovation dans les composants et logiciels.

Il est à noter que les composants pour l'IoT sont un enjeu majeur de compétitivité (*gestion de l'énergie, sécurité...*).

NIVEAU NATIONAL

Le Pôle est en particulier impliqué dans les initiatives suivantes.

Conseil National de l'Industrie⁵ regroupant les filières industrielles avec notamment le Comité Stratégique Filière Electronique⁶ et l'Alliance pour l'Industrie du Futur, avec le soutien actif de l'État (*Ministère de l'Économie et des finances et Secrétariat d'État auprès du Premier ministre, chargé du numérique*). L'objectif est de définir un plan d'action stratégique pour accompagner les filières industrielles dans leur transformation, en particulier au moyen du numérique.

Plan nano2022⁷

NIVEAU REGIONAL

Les actions et la feuille de route du Pôle s'articulent avec les priorités régionales et le Pôle est actif dans des initiatives phares.

OIR (*Opérations d'intérêt régional*) Smartech et Industrie du futur⁸. L'IoT représente un enjeu fort tant pour les offreurs de solution que pour les industriels.

Plateformes mutualisées CIMPACA : les 3 plateformes de recherche coopératives (*conception, caractérisation, micro-packaging et sécurité*) ont pour objet de favoriser innovation et l'industrialisation des objets communicants sécurisés.

⁴ <http://www.silicon-europe.eu>

⁵ <https://www.entreprises.gouv.fr/conseil-national-industrie/cni-numerique>

⁶ <https://www.entreprises.gouv.fr/conseil-national-industrie/la-filiere-industries-electroniques>

⁷ Page 25 du document https://www.gouvernement.fr/sites/default/files/document/document/2018/05/dossier_de_presse_-_conseil_national_de_lindustrie.pdf

⁸ <https://www.maregionsud.fr/economie-emploi/innover-plus-pour-doper-la-croissance-et-la-competitivite/8-operations-dinteret-regional.html>

D'autre part, SCS est actif sur différents projets en cours :

POSITIONNEMENT SUR DES PROJETS H2020

- Nouveau projet H2020 «Smart Anything Everywhere » en cours de dépôt.
- Chef de file du projet « IoT4Industry »⁹ qui vise à co-financer¹⁰ et mettre en œuvre des centaines de démonstrateurs grandeur nature intégrant l'IoT, le Big Data, l'Intelligence Artificielle et la Cybersécurité dans les outils et moyens de production d'entreprises industrielles européennes souhaitant numériser leurs processus.
- Support et labellisation de projets IoT (cf. exemples de projets en annexe).

CRÉATION DE L'IOT CENTER (IPCEI RÉGION SUD)

- Centre de ressources et de prototypage pour l'IoT porté notamment par STMicroelectronics dans le cadre d'un projet Européen collaboratif pour le financement de l'industrie microélectronique (Projet Nano2022).
- Présence et visibilité en tant que Digital Innovation Hub (DIH) sur la plateforme Smart Specialisation¹¹. C'est un moyen de donner de la visibilité à l'écosystème avec une possibilité de « one stop shop » pour les fournisseurs de technologie.

PARTENARIAT AVEC LES AUTRES PÔLES DE COMPÉTITIVITÉ RÉGIONAUX

- En partenariat avec la Région, Cap Energie et le Pôle SCS ont sollicité leurs écosystèmes respectifs pour monter des expérimentations dans le cadre du projet Flexgrid de gestion innovante de l'énergie.
Avec le Pôle Mer, le Pôle SCS a monté des journées autour de l'industrie du futur appliquée à la filière navale et défense permettant d'augmenter les relations entre les utilisateurs de technologies et les offreurs de solutions (*meilleure compréhension des besoins des utilisateurs et des problématiques métiers par les offreurs de solutions et du potentiel des technologies et sensibilisation des donneurs d'ordre du naval et de la défense des opportunités offertes par ces technologies innovantes sur leur use case*).
- D'autres collaborations avec les pôles « locaux » comme SAFE & Eurobiomed seront initiées pour apporter une complémentarité de nos écosystèmes respectifs sur la filière (*Sécurité & Défense avec Safe, Medical avec Eurobiomed*).

⁹ <https://www.iot4industry.eu/>

¹⁰ Financement de PME jusqu'à 60 000 euros pour la faisabilité, le prototypage ou la démonstration de projets visant l'intégration de technologies dans des cas d'usages industriels

¹¹ <http://s3platform.jrc.ec.europa.eu/digital-innovation-hubs>

2.2 Synergies entre l'IIoT et les autres axes stratégiques du Pôle

Le Pôle SCS met également en place des feuilles de route sur ses trois autres axes stratégiques, la microélectronique, la Sécurité et l'IIA/BIG Data.

Les différents domaines s'enrichissent mutuellement :

Microélectronique :

- L'accès à des composants performants est un élément clé pour le développement de l'IIoT (*maîtrise de l'énergie, intégration des protocoles, sécurité*) et la compétitivité de ses acteurs.
- Les circuits intégrés complexes miniaturisés, peu consommateurs d'énergie permettent d'aboutir à des objets, portés sur soi par exemple, autonomes, ultra performants en environnement contraint, pas intrusifs et discrets.
- L'intégration hétérogène, les supports souples et la miniaturisation de l'électronique.

Sécurité numérique :

- La sécurité des composants et systèmes électroniques ainsi qu'une sécurité de bout en bout sont nécessaires. La protection des données personnelles est également un enjeu clé.

La certification sécuritaire des objets et solution IIoT va entrer dans les règlements et législation européenne dès 2019.

IIA/ Big Data :

- Le traitement des données remontées par les nombreux capteurs et objets connectés, couplé à de l'intelligence artificielle est un enjeu majeur pour passer de l'observation à l'action et mettre en place des approches prédictives et des services à forte valeur ajoutée.

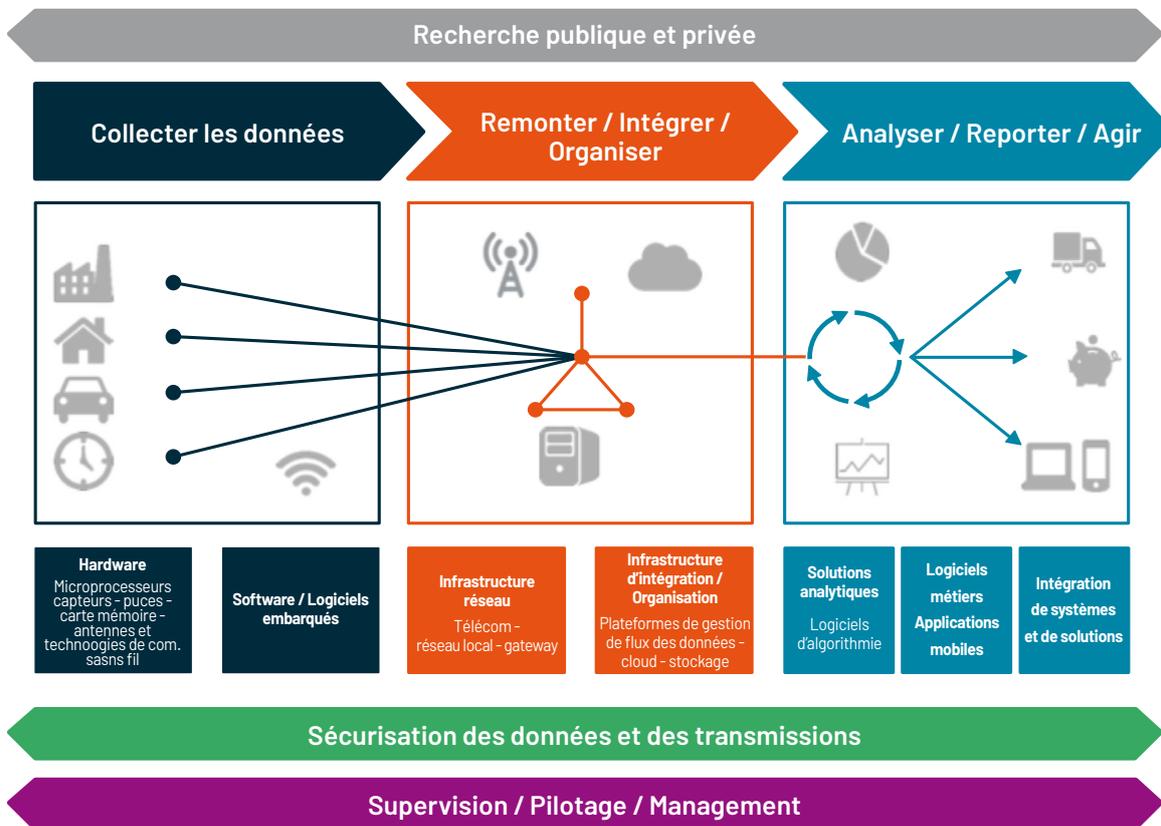
En outre, l'évolution des outils de calcul (*supercalculateur*) et du Hardware nécessaires au développement de l'IIA sera maîtrisé avec le développement de nouveaux capteurs et du EDGE computing :

ces nouveaux capteurs permettront de traiter les données en local (« *edge* » ou *périphérie de réseau*), directement dans l'objet ou au niveau de la passerelle (*donc sans accès au cloud*) et de garantir ainsi les performances de calcul nécessaires aux modèles d'apprentissage.

3.

Chaîne de valeur et cartographie des acteurs

La chaîne de valeur technologique permet d'identifier et de positionner les différentes briques technologiques contribuant à la construction d'un produit ou service IIoT. Elle permet de visualiser graphiquement les éléments clés et les acteurs du domaine.



Sources : Etude Olivier Wyman ; KPMG analysis

Sur cette chaîne de valeur, en plus des acteurs de sécurisation et de supervision qui sont présents sur les différents segments de la chaîne de valeur, on distingue :

Collecter les données /
Fabricants d'objets

- Les fabricants d'objets traditionnels et qui vont connecter des objets historiquement non connectés (e.g. Legrand)
- Les nouveaux entrants qui ne fournissent que des objets connectés (e.g. Withings...)

Remonter/Intégrer /
Organiser

- **Fournisseurs de connectivité** : en général l'opérateur de télécommunication fournissant la connectivité jusqu'au cloud soit par une liaison dédiée (*réseau cellulaire ou LPWAN*) soit par une liaison gratuite type WIFI/ Bluetooth jusqu'à une passerelle. L'alternative est un mix entre un réseau privé LPWAN et le cloud.
- **Les fournisseurs de plateforme** : cet acteur fournit des serveurs, des outils et des interfaces permettant de recueillir des données pour développer des applications et des services basés sur l'objet via des interfaces de programmation de type API. Les grands acteurs du numérique (*GAFA*) sont présents sur ce maillon de la chaîne de même que de nombreuses initiatives sur des marchés verticaux ou sur des niches. La répartition de la valeur entre les objets, le logiciel et les services et les plateformes dans le futur est un enjeu majeur d'autant plus que l'IoT évolue de la prise en compte de données binaires simples vers le traitement de données de plus en plus riches et complexes (*vidéo...*).

Analyser / Reporter / Agir

- **Fournisseurs d'applications simples** : cet acteur fournit les fonctionnalités de base liées à la connectivité des objets (suivi des données, contrôle/commande à distance, etc.). Cet acteur est souvent lié au fournisseur de la plateforme recueillant les données. Il fournit également l'application sur le smartphone et/ou la tablette.
- **Fournisseurs de services avancés** : cet acteur fournit les services à valeur ajoutée tirant parti des données générées par les objets, voire issues de la combinaison de différents objets.

Autres types d'acteurs

- **Distributeurs** : il s'agit de l'acteur qui vend l'objet directement au client final. Il peut être évidemment physique (*une enseigne de magasins, spécialisée ou non*) ou virtuel via par exemple des plateformes de commerce en ligne. Les nouveaux acteurs s'orientent par ailleurs de plus en plus vers de la vente directe, sur leur propre site internet.
- **Acteurs transverses** : certains acteurs, comme les géants de l'Internet peuvent être présents sur différents segments de la chaîne de valeur (*rachat du thermostat Nest par Google, Android Auto, Carplay, Playstore...*).

Pour compléter la chaîne de valeur, il est important de préciser les principaux **types de clients et utilisateurs** :

- **Particuliers** pour les applications BtoC (*domotique, bien être/quantified self, assistant personnel...*). Les objets connectés se sont largement diffusés et sont intégrés dans le quotidien (*compteurs électriques, alarmes ...*)
- **Entreprises**
 - Pour améliorer leur efficacité opérationnelle « **IoTisation** » dans le cadre de la numérisation (*digitalisation*) en cours et l'évolution vers l'entreprise 4.0. La logistique, et la maintenance industrielle sont des exemples de processus fortement impactés par l'IoT.
 - Pour enrichir leur offre produit ou service.



4. Marchés et usages cibles

4.1 Marchés prioritaires

Les marchés de l'IoT sont multiples tant pour les particuliers (*smarthome, quantified self, e-santé...*) que pour les professionnels (*maintenance, logistique...*).

Le Pôle SCS se positionne sur cinq marchés prioritaires pour cette phase 2019-2022. Ils ont été choisis pour leur forte croissance et parce qu'ils impliquent une part importante de l'écosystème SCS. Ils permettent également d'adresser les applications BtoB et les applications BtoC.

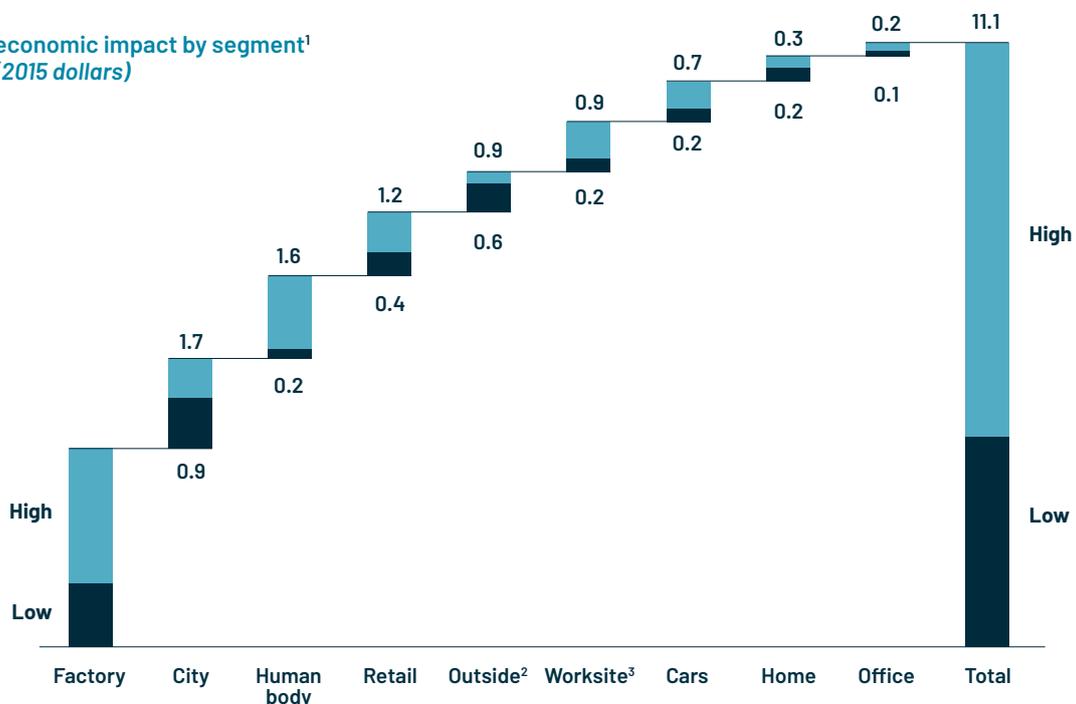
Les marchés prioritaires pour l'IoT sont similaires à ceux prioritaires de façon transverse pour le Pôle. Il s'agit des marchés suivants :

1. Santé
2. Smart Cities
3. Industrie 4.0
4. Transport & Mobilité
5. Smart Vehicle (exploratoire)

Le marché **Smart Vehicle** est lancé en mode exploratoire en 2019 et sera traité uniquement si des opportunités et des actions concrètes sont identifiées.

Selon McKinsey Global Institute (2017), le potentiel de l'IoT se répartit entre les marchés d'ici 2025 de la façon suivante :

Potential economic impact by segment¹
\$ Billions (2015 dollars)



1. For sized applications only. Numbers do not sum to total because of rounding.
2. Outside settings include outdoor environments, excluding those in urban settings.
3. Worksites are delivered as custom production environments.

Sources : McKinsey Global Institute analysis

4.2 Dimensionnement des marchés cibles MAJ*

De nombreux marchés verticaux applicatifs vont pouvoir bénéficier des avancées technologiques de la filière IoT
Ci-dessous quelques chiffres de taille de marché et de croissance de marché qui vont en bénéficier :

PRINCIPAUX CHIFFRES	
 <p>INDUSTRIE 4.0 (incluant l'agriculture)</p>	<p>504 M d'objets connectés en 2025 dont 80% pour les opérations de supply chain et de logistique – croissance de 20% / an (Idate).</p> <p>Marché « Smart Logistics », CAGR 2016-2021 32,7% , vers 41,30 Mds\$¹² (MarketsandMarkets)</p>
 <p>SMART CITIES (incluant SmartBuildings & Retail, Smart Metering Energy, SmartHome)</p>	<p>Smart Cities : Marché estimé à plus de 150Mds€ en 2025 (Market Research) – croissance de 23%/an</p> <p>SmartBuildings & Retail : 1,5Mds€ en 2025 – croissance de 17%/an (Frost&Sullivan)</p> <p>Smart Metering/Energy : 1 Mds de compteurs communicants dans le monde en 2020 (ABI)</p> <p>SmartHome : 224Mu de maisons équipées à court terme pour environ 35Mds€ (Strategy Analytics)</p>
 <p>SANTE & BIEN-ETRE</p>	<p>Santé & Bien être : Plus de 160Mds€ en 2022, croissance de 20%/an (Technavio, Research & Market)</p> <p>Wearables (incluant les dispositifs portés sur soi comme les « quantified self ») : 471Mu en 2021 – croissance de 100% sur la période 2016/2021 (Strategy Analytics)</p>
 <p>TRANSPORT & MOBILITE (incluant transport intelligent et véhicule autonome)</p>	<p>176,5Mds\$ en 2021 pour les solutions de smart transport¹³ (Transparency Market Research),</p> <p>126Mds€ en 2027 pour le marché des véhicules autonomes – croissance de 40%/an (Market research)</p>



¹² <https://www.marketsandmarkets.com/Market-Reports/connected-logistics-market-81941108.html>

¹³ <https://globenewswire.com/news-release/2016/06/24/851178/0/en/Global-Smart-Transportation-Market-Boosted-by-Growing-Need-for-Smart-Services-to-reach-US-176-5-bn-by-2021-TMR.html>

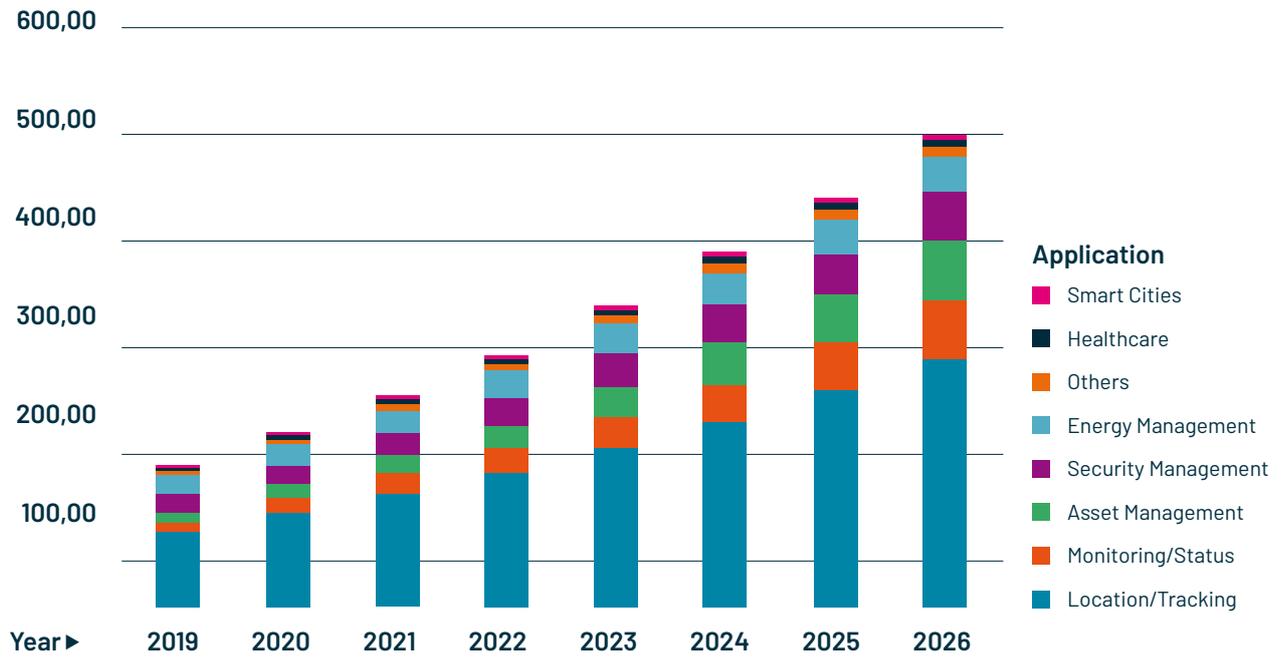
Classification fine par applications & usages :

L'loT fait l'objet de nombreuses études de marché. L'étude ABI Research du 23 octobre 2018 « **IoT Market Tracker – Worldwide** » classifie les marchés loT par types d'applications et usage, suivant les définitions insérées en annexe.

Avec une telle classification, ci-dessous les prévisions de ABI Research sur les années à venir, en millions de dollars américains :

Revenu prévisionnel en Millions de dollars par secteurs applicatifs
Sources : ABI Research

Sum of Value ▼





4.2.1 Santé

Ce marché inclus à la fois l'usage d'objets connectés pour de la prévention et du suivi médical, c'est le marché de la e-santé et des applications de bien-être à base d'objets connectés souvent classées dans le marché du « quantified self ».

Dans un contexte de vieillissement de la population, de diminution des dépenses publiques, de concentration territoriale et de saturation des infrastructures de soins, la prise en charge des patients à domicile est clé.



Les segments suivants sont des domaines d'application prioritaires où les acteurs SCS ont un fort domaine d'expertise et se positionnent¹⁴:

1. Santé à domicile (*Integrated Care, e-consultation, télémonitoring*) :

dans ce contexte les outils qui permettent de suivre des individus à domicile dans le cadre d'une action de prévention ou de soin. De la simple gestion d'alerte à l'analyse prédictive et l'anticipation des événements, le télémonitoring fait cependant face à des enjeux technologiques tels que la fiabilité, l'analyse et le partage des données. La télé-consultation à domicile est maintenant très développée suite au confinement. Elle vient en complément du télémonitoring.

2. Les objets connectés de traitement médical :

ces objets permettent un suivi régulier à distance de patients atteints de maladies chroniques (*en pleine explosion : asthme, diabète...*). La diffusion d'objets et de solutions connectées nécessite la réalisation de solutions ergonomiques, implantables ou non intrusives et autonomes. L'impact économique et sociétal lié à un meilleur traitement des maladies chroniques est énorme.

3. Les applications bien-être :

ces outils grand public sont utilisés sans contrôle médical et permettent aux individus de gérer directement leur santé ou bien-être et faire de la prévention. Le développement de mesures portées pour le sport et bien-être nécessite la réalisation de solutions ergonomiques et autonomes (*montre connectée...*).



Notons que les approches du marché, les attentes techniques et financières de ces outils « Wellness » ou « Bien-être sportif » (*montres connectées...*) sont différents des objets connectés dits « à application médicale ».

4. Les outils de sécurisation, la chirurgie à distance et l'optimisation de la prise en charge en milieu hospitalier :

ces outils visent à améliorer le fonctionnement interne des établissements de santé et la qualité de service rendu aux patients (*identification des personnes et matériels médicaux*). **La téléprésence** se développe fortement dans les Ephad avec les robots et également les objets de **détection de chute**.

Les produits médicaux connectés à usage unique tels que composants implantables, cathéters connectés, pansements équipés de capteurs, containers médicaux connectés (*pipettes...*) sont inclus dans cette catégorie – tout comme les matériels et équipement de tests médicamenteux cliniques (*tests in-vivo ou pas, tests sur ou dans les animaux cobayes, ...*) **Le Track and trace** des équipements critiques de réanimation tels que les respirateurs est devenue clé. La traçabilité des vaccins (*connaissance du stock et géolocalisation "indoor" précise*) qui sont en nombre très limité est également un enjeu important.

En milieu hospitalier, **la 5G** va permettre le déploiement d'opérations à distance avec un chirurgien expert basé à Paris et un patient à Marseille par exemple.

Le marché de la santé a des enjeux spécifiques :

- **Fiabilité** : les enjeux en cas de non fonctionnement sont critiques.
- **Autonomie** : les contraintes de consommation et de miniaturisation sont fortes sur les capteurs et les unités locales de traitement permettant la remontée d'informations ou la remontée d'alertes. La conception **d'architectures** et produits pour en augmenter l'autonomie ainsi que les solutions

¹⁴ Cf Livre blanc esanté publié par SCS

locales **de collecte, de stockage et de gestion de l'énergie** sont des axes d'innovation primordiaux. La réalisation de **nouveaux supports pour l'électronique** et les capteurs sont nécessaires dans le cas d'applications de mesure portées sur soi (*électronique imprimée, support souple, textiles intelligents, ...*).

- **Sécurité et confidentialité des données** : la sécurité et la confidentialité des informations est une préoccupation générale à tous ces segments, tant pour les patients, les organismes hospitaliers ou de santé, que les personnels médicaux. **La confidentialité des données et la sécurité des systèmes doit être assurée pour protéger les données médicales personnelles** pouvant faire l'objet d'utilisation frauduleuse. Les enjeux de sécurité des données sont des enjeux transverses à plusieurs marchés et seront traités dans la feuille de route Sécurité de SCS. L'aspect **Hacking/sécurité** des infrastructures industrielles qui peuvent être reconnues comme des objets connectés - ex : l'IRM, connecté au réseau peut être victime d'une cyber attaque. Ces outils sont pilotés par des automates programmables qui sont sujets à de nombreuses attaques. (cf CHU Nice, Schneider à Carros)



4.2.2 Smart Cities

La gestion et le monitoring intelligent des grandes infrastructures urbaines et des villes passera par le déploiement d'infrastructures à base d'objets connectés intelligents. Les applications sont nombreuses.

la ville intelligente sera « durable » et passe par la gestion intelligente :

- **Commerces & Grands Magasins** : les magasins ont besoin d'être connectés et devront offrir dorénavant le "Click&collect" (*comme le paiement sans contact, la visioconférence...sont des usages qui existaient mais ont été boostés avec la crise Covid-19*).
- **de l'eau, de l'électricité, des déchets, de l'éclairage** : la maîtrise de la demande en énergie, comme une plus grande flexibilité de consommation (*d'eau, d'électricité, de service de ramassage...*) sera atteinte avec les objets connectés implémentés dans les infrastructures de la ville.
- **Transport des biens et des personnes dans la ville** : favoriser et simplifier la mobilité des citoyens, mais aussi décongestionner la ville tout en diminuant l'empreinte écologique des déplacements sera possible avec les objets connectés.

- **Des cameras intelligentes ("safe city") :**

la ville intelligente comporte: smartgrid, smart transport, smart retail ET safe city. Les "cameras connectées" ont un rôle important pour détecter des actes de malveillance, des flux de personnes... (*comme à Nice après l'attentat*).

- **Des E-services et e-administration :**

une organisation intelligente permettra de faire adhérer les citoyens aux initiatives des politiques locales.

- **Des lieux de spectacles, des stades etc...**



Les enjeux spécifiques à l'IoT pour un déploiement des usages sont nombreux :

- **Capteurs intelligents** : les objets sont dotés de capacité de calculs et d'intelligence suffisante pour pouvoir effectuer des traitements directement au niveau des objets ou des gateways (*Edge Computing*). Une électronique de puissance sera nécessaire pour agir sur les systèmes physiques.
- **Sécurité des données** : protéger les données personnelles des citoyens est clé pour garantir la confiance de ceux-ci envers les nouveaux usages offerts par la ville. Sans sécurité et « privacy » des données collectées (*consommation d'eau, d'électricité...*), le déploiement des e-services sera freiné.
- **Autonomie & consommation** : des compteurs d'énergie, de niveau des cuves ou des capteurs liés à l'environnement ou à la supervision de sites publics, doivent avoir une durée de vie souvent supérieure à dix ans. Les capteurs doivent mesurer des paramètres environnementaux de manière permanente, et donc doivent être maintenus sous tension ou « réveillables » à distance.

Ces objets pouvant être autonomes doivent être, le plus souvent, alimentés par une batterie. Devant ces contraintes, une attention toute particulière est prêté à la consommation du capteur. Les développeurs de capteurs conçoivent leur produit en fonction de ces contraintes et choisissent tous les composants en fonction de leur faible consommation.

- **Compromis Sécurité, puissance & consommation :** la capacité de calcul est également un paramètre lié à la consommation. Aujourd'hui, les objets sont conçus avec des processeurs de faible puissance, de manière à limiter la consommation électrique. Ce fait peut rendre plus complexe l'adoption de mécanismes de sécurité à base de calculs cryptographiques.

- **Connectivité :**

Les capteurs intégrés dans les lampadaires d'éclairage par exemple nécessite des réseaux longues distances performants. La remontée de données passives environnementales issues de capteurs intégrés dans les lampadaires d'éclairage par exemple nécessite des réseaux longues distances (*dizaine de km*) et/ou maillés pour interconnecter les zones urbaines et rurales. Les réseaux radiofréquence bas débit et basse consommation comme SigFox ou LoRa jouent un rôle majeur.



4.2.3 Industrie 4.0

Dans l'entreprise et dans l'usine, la gestion de chaînes de valeur et des processus complexes inter et intra-entreprises est en constant ajustement : comment gagner en productivité, en flexibilité ?

Pour qui travaille telle machine et comment organise-t-elle sa chaîne d'approvisionnement ? Où se trouve tel outil ? Comment prédire la dérive de telle mesure ?

Les technologies de l'IoT vont permettre une mutation l'industrie vers une industrie connectée, optimisée et créative. Par exemple, l'analyse de perturbations sur un équipement, pourra se faire directement au cœur de l'équipement surveillé (*avec une dépense énergétique minimale et sans envoyer de données vers un cloud*) grâce à l'intelligence embarquée dans les capteurs.

Les solutions technologiques innovantes suivantes vont permettre la modernisation attendue sur les machines, les robots, les procédés industriels :

- des **capteurs plus petits, résistants, plus précis** (MEMS, température, pression, caméras...).

- des **circuits intégrés** dédiés, plus petits, moins consommateurs en énergie pour être en adéquation avec les exigences du monde industriel.
- une connectivité optimisée avec des systèmes sans contact, des **gateways, 5G** et des réseaux bas débit permettant les échanges entre les objets.
- des **infrastructures Cloud** facilitant l'accès aux données industrielles de n'importe où et permettant la synchronisation de sites de production distants.
- les technologies **IA & Big Data** pour prendre des décisions clés, comme la **maintenance prédictive** ainsi que le Deep Learning et l'IA pour automatiser la prise de décision.
- les robots mobiles de plus en plus petits¹⁵.

L'industrie 4.0 s'illustre dans les usines mais aussi dans les chantiers extérieurs et dans l'agriculture¹⁶.

Agriculture connectée : l'agriculture commence sa démarche de modernisation, en intégrant les systèmes de pilotage d'équipements assistés (*machines agricoles autonomes à positionnement par GPS, robots de désherbage évitant l'emploi de pesticides, gestion des intrants et des cheptels, optimisation des paramètres de croissance des végétaux éventuellement en atmosphère contrôlée, ...*).

L'IoT et l'IA vont accélérer leur entrée dans le secteur de l'agriculture connectée. Capteurs d'humidité, drones de surveillance, capteurs de pression, ombrières intelligentes, vannes connectées, débimètres... sont autant d'objets qui aideront demain les agriculteurs dans la gestion intelligente et optimisée de leur exploitation. Avec des retombées économiques et sociétales importantes (*réduction des coûts liés à la perte de production ou à l'utilisation d'intrants, réduction de l'impact environnemental*).



¹⁵ Il faut noter la robotisation massive de l'industrie avec en particulier des robots mobiles de plus en plus petits (Capteurs et Connectivité Robot to Robot, Capteurs et Connectivité Robot mobile vers monde extérieur, le transfert d'une partie de l'intelligence système du système informatique central vers chacun des robots). Les robots collaboratifs (Cobots) sont aussi de plus en plus présents dans de nombreux secteurs industriels, où ils interviennent en support des opérateurs humains pour des tâches lourdes ou dangereuses.

¹⁶ <https://www.dailymotion.com/video/x58pi5q>



4.2.4 Transport & mobilité

Le transport des personnes et des marchandises sera plus soucieux de l'environnement et plus compétitif. La mobilité « intelligente » doit être moins chère, plus libre, plus respectueuse de l'environnement et plus sûre au quotidien.

Plus compactes, plus fiables, plus robustes ou performantes sont les solutions électroniques embarquées dans les moyens de transports.

Des nouveaux capteurs complexes et ultra miniaturisés vont être intégrés dans les moyens de transport ou solution de mobilité intelligente ou infrastructures urbaines pour décrire l'environnement en temps réel et communiquer avec les usagers.

- **Transport personnes :**

les services liés à la mobilité sont clés pour les collectivités (*itinéraires en temps réel, transports à la demande*). Grâce à l'IoT, l'information du conducteur du bus ou du tramway sera enrichie, et exposera en projection sur le pare-brise les panneaux indicateurs, les services à proximité, et permettra de réagir rapidement en cas d'incident etc...L'empreinte écologique des déplacements sera nettement améliorée.

- **Transport marchandises :**

le suivi indispensable en temps réel de certaines marchandises sera facilité, avec par exemple la connaissance, sur un simple smartphone, du parcours de produits à très haute valeur ajoutée.

La livraison du dernier km (*logistique urbaine*) est un enjeu important dans la thématique de la mobilité. L'IA (*associée aux capteurs*) va permettre d'optimiser les tournées de livraison (*aussi appelée "logistique urbaine"*).

Certains capteurs sont déjà capables de fournir en temps réel des données sur la géolocalisation de la marchandise et l'état de son environnement : température, taux d'humidité, présence de gaz ou encore luminosité.

Ils peuvent également intégrer des senseurs spécifiques, par exemple pour contrôler l'intensité de freinage d'un wagon ou les accélérations subies par un container, et contiennent toutes les informations relatives à son statut administratif et douanier. Cela permet de doter le fret de l'intelligence nécessaire pour améliorer la productivité et la sécurité logistique.

Les enjeux à relever pour l'IoT pour les solutions de mobilité et transport sont :

- **Capteurs :** miniaturisation, Complexité, Sécurisation, fiabilité.
- **Optimisation consommation avec une meilleure performance.**
- **Connectivité temps réel pour réagir rapidement.**



4.2.5 Smart Vehicle

L'automobile de demain sera plus sûre et autonome. Equipée d'une multitude de capteurs miniaturisés :

- elle communiquera avec les autres véhicules (V2V) et avec les infrastructures routières (V2I) pour réduire le nombre d'accidents.
- elle sera équipée de systèmes innovants pour améliorer la vision à différentes distances (*capteurs ultrasons, optique, radars...*) et pour détecter les obstacles encore invisibles (*mais approchant derrière les bâtiments ou d'autres véhicules à l'angle du carrefour*).
- il y a un élan important sur le véhicule "propre". Beaucoup de constructeurs en profitent aussi pour monter le niveau d'autonomie (*en terme de conduite*) de leur véhicules (*ex : TESLA, VOLVO, RENAULT, ...*).
Même si les programmes de développement et de mise sur le marché de véhicules autonomes seront certainement plus longs que prévus, la tendance va dans ce sens. On note par ailleurs une forte accélération des projets autour des navettes (*transports collectifs*) autonomes ou semi autonomes.

Parmi les enjeux majeurs pour le déploiement d'usages intégrant l'IoT pour le véhicule connecté et autonome, on peut citer :

- la **baisse des coûts de ces capteurs.**
- leur **autonomie** (*optimisation de la consommation d'énergie*).
- leur **complexification** pour qu'ils soient plus **performants**.
 - Cette complexification permettra aux constructeurs automobiles d'intégrer des fonctions telles que l'injection directe, la suralimentation et la gestion complète des systèmes de transmission dans un seul Capteur.

- Pouvoir traiter et stocker, en **temps réel**, la **grande quantité de données** engendrées par les multiples capteurs du véhicule.
- L'intégration de **l'Intelligence Artificielle dans les objets connectés** et les capteurs.
 - Après la reconnaissance d'images, et donc d'objets détectés, de nouvelles fonctionnalités apparaissent grâce à la reconnaissance vocale, la compréhension du langage naturel.
 - Edge computation & very edge computing apparaissent comme des axes forts en terme de R&D ; les évolutions en terme de marché sont très importantes.
- La **sécurité de la connectivité sans fil** toujours plus complexe au sein de l'habitacle.
 - De gros problèmes de sécurité physique et des risques de piratage devront être impérativement traités.
- **L'arrivée de la 5G** va permettre d'ouvrir (*grâce à ses caractéristiques de faible latence, haut débit ...*) la porte à de nouvelles applications et accélérer le développement autour du véhicule autonome.

Une fois ces défis relevés, **l'expérience utilisateur sera simple et personnalisée** aux utilisateurs de véhicules connectés.



4.3 Opportunités marché liées aux évolutions réglementaires et sociétales MAJ*

Trois enjeux semblent importants pour les activités de la filière et peuvent constituer des atouts pour les acteurs qui sauront s'en emparer :

TROIS ENJEUX

LA PROTECTION DES DONNEES PERSONNELLES

De nouvelles réglementations et en particulier le Règlement Général pour la Protection des Données (RGPD) et la directive ePrivacy ont donné un cadre très clair et structurant pour les entités utilisant, traitant et stockant des données personnelles.

Cette réglementation nécessite l'utilisation de solutions numériques sécurisées pour garantir la protection des données personnelles.

CERTIFICATION SECURITAIRE DES OBJETS IOT

de nombreuses attaques récentes ont montré notamment l'étendue de la menace et les dangers d'un IoT sans sécurité. La Commission Européenne, appuyée notamment par les travaux de l'ECSSO, d'Eurosmart, de l'AIOTI, l'ANSSI en France, a proposé récemment un nouveau règlement concernant la sécurité numérique, le Cyber Security Act.

Celui-ci vise à proposer des processus et méthodes pour évaluer le niveau de sécurité de produits, et notamment ceux de l'IoT, en s'inspirant des méthodes qui ont fait le succès de l'industrie de la carte à puce.

Les composants électroniques et notamment les microcontrôleurs utilisés dans les objets et Gateway IoT devront offrir les bons niveaux de sécurité pour que les objets et produits IoT les utilisant puissent obtenir les certifications nécessaires.

TRANSITION ECOLOGIQUE ET ENVIRONNEMENTALE

La mesure de la qualité de l'air intérieur (*bâtiments*) et extérieur (*centres urbains, surveillance côtière, détection des incendies*) requiert le développement de nouveaux capteurs/multi-capteurs de gaz (*CO, CO2, ozone, COV, SO2*) à faible consommation et la mise au point de systèmes de capteurs intelligents.

Il est ensuite nécessaire de développer les infrastructures nécessaires pour l'exploitation et la valorisation des données et la définition des actions et politiques publiques en conséquence.

La qualité de l'air est mesurée partout aujourd'hui, par contre la mobilité intelligente, douce (*autopartage..*) est au coeur des enjeux de demain.

5.

Verrous et enjeux technologiques

5.1 Etat des lieux MAJ*

Pour déployer les applications mentionnées dans le chapitre précédent et donner un avantage concurrentiel aux entreprises de l'écosystème, les enjeux et verrous technologiques suivants ont été identifiés par les acteurs SCS :

1 Standardisation et Réglementation

2 Intégration des objets connectés dans leur environnement

- Miniaturisation & Intégration antennes
- Supports souples pour les dispositifs portés sur des personnes.

3 Harmonisation de l'infrastructure

- Antennes multifréquences
- Intégration et agrégation multi-protocoles

4 Autonomie et maîtrise de l'énergie

- Low power et Energy Harvesting

5 IA dans les objets et les passerelles avec maîtrise de l'énergie

- Apprentissage dans les objets
- Détections vidéo au niveau des passerelles (*verrou spécifique à un Use Case*)

6 Accessibilité des données

7 Sécurité

- Les enjeux et verrous technologiques liés à la sécurité sont détaillés dans la feuille de route sécurité.

5.2 Les verrous prioritaires

1 Standardisation et Réglementation

- Dans les applications de l'IoT, la majorité des objets communiquent par radiofréquences dans l'une des bandes libres ISM (*Industriel, Scientifique, Médical*). La bande 2.4 GHz a l'avantage d'être disponible mondialement mais souffre de la concurrence d'une multitude de protocoles pas nécessairement liés à l'IoT (*Wifi, Bluetooth etc...*).

Les bandes sub-GHz (868, 433, 169 MHz) dédiées aux applications M2M ont une portée radio et un pouvoir pénétrant supérieurs mais n'offrent pas une couverture mondiale. De plus, du fait de son étroitesse, l'accès au medium radio dans la bande 868 MHz est restreint (*duty cycling*) et le risque de saturation de la bande à moyen terme est patent.

- Les problèmes d'interopérabilité entre objets n'ont toujours pas été levés malgré des efforts certains de standardisation. Mais il manque toujours à l'appel un protocole unifié qui serait accepté par tous, sur le modèle des profils USB par exemple. La faute à la multitude de protocoles radio, de consortiums, de solutions propriétaires etc...

- Du point de vue de la sécurité, les protocoles standards de l'Internet s'avèrent peu adaptés au monde de l'IoT et de nouveaux algorithmes et protocoles cryptographiques spécifiques à l'IoT ont vu le jour. Cependant, un gros travail de recherche reste à accomplir, en particulier pour l'intégration native des objets dans la blockchain.

2 Antennes multifréquences

- La miniaturisation et l'intégration de ou des antennes dans un système nécessite la prise en compte de nombreuses contraintes. Un compromis est à trouver de la part du concepteur.

Ce compromis est imposé par les dimensions de ou des antennes, les performances recherchées en termes de gain, de rayonnement, d'adaptation, mais également en fonction du facteur de forme compatible avec l'application visée. Il est bien connu en électromagnétisme que plus l'antenne est petite, plus les performances sont dégradées.

Le principale critère de performance d'une antenne est son efficacité. L'intégration de l'antenne sur ou dans l'objet dépend fortement du substrat et de ses caractéristiques, ce qui jouent un rôle majeur dans la miniaturisation. Le concepteur d'antenne doit être capable de prendre en compte l'ensemble de ses contraintes dès le début de la conception. L'antenne générique et universelle n'existe pas.

- L'intégration d'antennes sur support souple suppose d'avoir des encres conductrices présentant des caractéristiques électriques proches de celle des métaux habituellement utilisées. Des techniques de dépôt doivent être mieux maîtrisées (*épaisseur, accroche, résolution, ...*).

- La gestion de différentes normes radiofréquences existantes (*basées sur les standards radio dans les bandes 860 -960 MHz : RFID, GSM, Sigfox par exemple*), nécessite implicitement l'utilisation de plusieurs antennes.

Cependant l'objet communicant est souvent compact et il est d'usage d'avoir recours à la notion d'antennes multifréquences, antennes de tailles souvent réduites, cohabitant avec d'autres systèmes électroniques parasites. Le co-design des antennes et des puces doit être nécessairement envisagé pour obtenir les performances souhaitées en tenant compte des contraintes (*environnement, CEM, miniaturisation, rayonnement, ...*).

- Le domaine de l'IOT est vaste et quelle que soit l'application ou le domaine d'usage visé, la communication est liée à différentes normes radiofréquences existantes, basées sur les nombreux standards radiofréquences. Qu'elle soit champ proche ou champ lointain, voire les deux, elle nécessite implicitement l'utilisation de plusieurs antennes dans un volume très limité. L'objet communicant est souvent compact et il est d'usage d'avoir recours à la notion d'antennes multifréquences, antennes de tailles souvent réduites, cohabitant avec d'autres systèmes électroniques parasites, dans un environnement contraint. Le co-design des antennes et des puces doit être nécessairement envisagé pour obtenir les performances souhaitées. Bien entendu l'étude CEM de ces systèmes est devenue une obligation.



3 **L'énergie/ Gestion de l'énergie et récupération de l'énergie**

- Des progrès très significatifs ont été accomplis au niveau de la consommation électrique des microcontrôleurs et des transmetteur-récepteurs radio embarqués dans les objets, par exemple par l'abaissement de leur tension d'alimentation. L'autonomie des objets connectés alimentés par batterie s'en est trouvée grandement améliorée.

Cependant, les solutions d'alimentation par batterie (*Lithium-Ion ou autre*) sont peu satisfaisantes du point de vue de la maintenance du produit (nécessité de changer la batterie régulièrement) ainsi que sur le plan environnemental (*utilisation de métaux rares pour la fabrication, recyclage pas toujours possible techniquement ou économiquement trop coûteux etc...*). Il s'avère donc nécessaire de développer des solutions simples et efficaces de collecte de l'énergie ambiante.

- De plus, du fait de l'émergence du edge computing, les objets font face à une demande grandissante en puissance de calcul pour l'exécution d'algorithmes de Machine Learning très énergivores, même si l'apparition sur le marché de processeurs dédiés devrait palier en partie à cette demande.
- La sécurité représente un autre poste de consommation électrique majeur. D'où la nécessité de développer des algorithmes et protocoles de cryptographie hyper-légers spécifiques à l'IoT pour augmenter l'autonomie des objets connectés.

4 **Harmonisation de l'infrastructure/ Intégration et agrégation multi-protocoles**

- La diversité des infrastructures et des protocoles IOT disponibles constitue un frein au déploiement en volume, même si à l'opposé, leur l'unicité n'est ni nécessaire, ni souhaitable. Côté Radio Fréquences, se côtoient principalement des LPWANs Low Power Wide Area Network tels LoRa et Sigfox, le Bluetooth Low Energy souvent relayé par les smartphones, ou encore le NBIOT futur en 5G géré par les opérateurs de télécommunication - Et de l'autre côté des passerelles edge plus ou moins intelligentes.

Les données sont agrégées vers ou dans le cloud avec différents protocoles de distribution, propriétaires ou standardisés tels OPCUA, MQTT, ONEM2M en capitalisant éventuellement sur la sécurité et la robustesse des protocoles IT https, mqtt,...

L'enjeu principal reste de retenir la technologie adaptée à ses cas d'usage et d'éviter les solutions trop propriétaires, ou les conventions d'usage parfois imposées qui restreindraient la solution à tel ou tel cloud public.

5 **IA dans les objets et les passerelles/ Apprentissage dans les objets**

- Embarquer l'intelligence artificielle directement sur la cible (*ou à proximité (sur les passerelles par exemple) offre aux utilisateurs un système capable de prendre des décisions même en absence de réseau, réduire les temps de latence tout en économisant de l'énergie.*

Les enjeux de l'IA embarquée consistent alors d'être en capacité de proposer les bons algorithmes afin d'obtenir le meilleur compromis performance / coût / consommation énergétique tout en l'adaptant aux besoins des utilisateurs finaux (*sans oublier les aspects sécurité qui permettent de protéger ainsi la vie privée des utilisateurs*).

6 **IA dans les objets et les passerelles/ Détections vidéo au niveau des passerelles (verrou spécifique à un Use Case)**

- Voici un verrou spécifique « **l'intégration d'IA dans les devices et gateway** » lié à un use case et qui permet de présenter les différents challenges technologiques cités ci-dessus.

Avec l'appui d'algorithmes de réseaux neuronaux profonds, de nouvelles caméras de sécurité voient le jour et vont permettre de reconnaître des humains et des véhicules avec un haut degré de précision...et venir en aide aux espèces vulnérables d'un parc animalier par exemple. Spécialisées dans le traitement de la vision, ces caméras auront pour ambition d'empêcher les braconniers d'agir, en alertant assez tôt les gardes forestiers pour qu'ils les interceptent - et ce grâce aux algorithmes d'intelligence artificielle.

Le edge computing et le "Very Edge Computing" (*IA basée au niveau du capteur*) sont accélérés.

7 Accessibilité des données (contexte GDPR)

- Les modèles à valeur ajoutée autour de l'Internet des Objets nécessite l'exploitation de données à des fins de services commerciaux. Les réglementations ont longtemps été floues à ce sujet, jusqu'à l'apparition du règlement de l'Union Européenne RGPD (*Règlement Général sur la Protection des Données*), qui régit le droit à l'utilisation des données.

Dans ce cadre, les plateformes technologiques devront intégrer l'acceptance explicite de l'utilisateur quant à l'utilisation, le transfert à des tiers et l'effacement de ses données. Par la suite, ces données devront être stockées et transmises de manière sécurisée.

8 Sécurité

- La sécurité des objets au niveau composant, système, et communication est une demande forte constatée par les laboratoires en 2021.
- La sécurité au niveau du composant et la sécurité de bout en bout (*objet, protocole, réseau, données...*) sont des enjeux majeurs. A titre d'exemple l'existence de Passerelles edge-computing sécurisées est un élément clé pour un IoT sécurisé.
- La sensibilisation des entreprises utilisatrices de l'IoT et des institutionnels est également nécessaire en parallèle pour un passage de la conscience du problème à sa prise en compte effective.

(La sécurité des objets est adressée dans la FDR sécurité).

9 Accessibilité des données

- L'accessibilité à des données fiables doit être réalisée dans un cadre réglementaire adapté (*place de marché des données reliant des offreurs de données à des utilisateurs de données*).

5.3 Projets en cours

Dès à présent, le Pôle SCS a favorisé l'émergence de projets innovants en lien avec **les enjeux ci-dessus**. Des exemples de projets collaboratifs **labellisés et sélectionnés par le financeur public** sont fournis en annexe.

D'autres projets ont été déposés avec succès avec SCS comme Chef de file du projet « **IoT4Industry** »¹⁷ qui vise à co-financer¹⁸ et mettre en œuvre des centaines de démonstrateurs grandeur nature intégrant l'IoT dans les outils et moyens de production d'entreprises industrielles européennes souhaitant numériser leurs processus.

En outre, des projets ambitieux H2020 sont en cours de dépôt, «Smart Anything Everywhere».

Enfin, un **nouvel IoT Center (IPCEI Région Sud)** sera bientôt opérationnel. Ce centre de ressources et de prototype pour l'IoT est porté notamment par **STMicroelectronics** dans le cadre d'un projet Européen collaboratif pour le financement de l'industrie microélectronique (*Projet Nano2022*).

En parallèle, des initiatives en faveur de l'intégration de technologies **BlockChain** dans l'IoT sur des secteurs cibles tel que le transport et la logistique sont en cours.

6. Enjeux de formation

6.1 Etat des lieux

La Région SUD est un territoire d'excellence dans le domaine des hautes technologies et de leurs méthodes de production avec des acteurs dans la formation et l'éducation qui sont :

	Aix-Marseille Université (UFR de Sciences, IUT d'Aix-Marseille, Polytech Marseille)
	Ecole Centrale de Marseille
	CNRS
	Centre Microélectronique de Provence de l'École des Mines de Saint Etienne
	YNCREA Mediterranée (ISEN) Ecole d'ingénieurs en électronique
	Ecole Nationale Supérieure des Arts et Métiers d'Aix-en-Provence , hébergeant un institut de formation aux méthodes du Lean Manufacturing (<i>Dynéo</i>)
	ITII , école d'ingénieurs en alternance
	Université de Nice-Sophia Antipolis (Polytech Nice)

Des formations variées diplômantes sont disponibles en Région en **mode alternance, formation initiale ou continue** (*adaptées à tout type de public en formation initiale ou en activité*).

¹⁷ <https://www.iot4industry.eu/>

¹⁸ Financement de PME jusqu'à 60 000 euros pour la faisabilité, le prototypage ou la démonstration de projets visant l'intégration de technologies dans des cas d'usages industriels

L'IoT bénéficie de l'environnement de formation lié à la filière électronique d'une part et à celui des réseaux et du logiciel d'autre part. **L'électronique** est de plus en plus utilisée dans des systèmes embarqués avec des contraintes d'environnement sévères.

Cette tendance impose aux concepteurs de système un recours accru à la **modélisation et à la simulation**, ainsi que la maîtrise de **champs de compétences transverses**.

Cela génère des besoins importants **en termes d'emplois** et d'acquisition de compétences pour les entreprises de la filière. Le renforcement de la formation est un **point clé** pour répondre aux attentes des entreprises.

L'IoT trouve toute sa place dans les cursus personnalisés qui ont été créés pour **répondre aux emplois et compétences** attendus sur des thèmes précis comme l'Industrie

du Futur (*conducteur d'équipement robotisé (automation), technicien de maintenance et de support process*), tant en **production** qu'en **R&D** et en **engineering**.

Les domaines concernés sont la **sécurité numérique**, la **numérisation des procédés industriels**, **l'Intelligence Artificielle**, **l'Internet des Objets** (*Ingénieurs en conception analogique et numérique, en conception de cartes ou équipements de type antennes ou capteurs, techniciens en réalisation de circuits intégrés (design layout)*).

La sécurité de l'IoT donne lieu à des formations spécifiques intégrées dans le **cursus de l'École des Mines** de Gardanne ou accessible en formation continue.

Un descriptif des formations disponibles est fourni (**Cf. Annexe**).

6.2 Enjeux autour de la formation MAJ*

Les enjeux de la formation autour de l'IoT sont nombreux tant pour les formations initiales que pour les formations continues. Il s'agit de former non seulement les experts techniques mais également de sensibiliser les utilisateurs de services IoT :

1

Périmètre, contenu et modalités de formations :

- le développement de la formation initiale par apprentissage, répond à une demande des entreprises et à une volonté gouvernementale. Dans cet optique Polytech Marseille dépose une demande d'accréditation auprès de la CTI d'un nouveau diplôme d'ingénieur pour la rentrée 2022 par apprentissage : ingénieur IOT. Ce diplôme répond à une demande forte des industriels régionaux. On peut également faire état du projet PIA Innovation-micro, le campus des métiers qui visent à répondre aux trois points du pdf : sensibiliser les jeunes aux métiers de l'électronique, former des ingénieurs aux enjeux à venir (*IOT, IA, industrie 4.0..*) et réformer les ingénieurs en poste à ces nouveaux métiers, montée en compétences, évolution des compétences, ... Chaque formation en électronique et informatique, intègre dans ces programmes, l'IOT et l'IA.
- la conception des programmes pédagogiques en adéquation avec les besoins des entreprises et complétés avec des salles ressources dédiées au prototypage et à la caractérisation pour les fabricants d'objets.
- la disponibilité d'un ensemble de formations à fort contenu technologique couvrant l'ensemble de la chaîne de valeur IoT et permettant de répondre à l'ensemble des besoins des entreprises régionales. Les problématiques hardware et composant ainsi que les thématiques Réseaux, Sécurité, Données. L'analyse des données et l'intelligence artificielle sont clés pour des services avancés autour des données de l'IoT. Une attention particulière est portée sur les applications en lien avec les segments stratégiques sur lequel le Pôle et son écosystème se positionnent.
- l'ouverture aux entreprises intervenant aussi bien en amont qu'en aval de la chaîne de valeur (*applications*) pour assurer les formations ou pour former leurs employés.
- la sensibilisation des utilisateurs de l'IoT au sein des entreprises et des institutionnels grâce à des modules de sensibilisation pour les responsables métiers, les acheteurs et les chefs de projets (*enjeux de l'IoT, problématique de sécurité, déploiement d'un projet IoT...*).
- l'offre de parcours de formation adaptés à tout public et à tout âge aussi bien en formation initiale, qu'en alternance et en formation continue.

2

Lien fort avec les entreprises :

- l'adossement des nouvelles formations et des plateformes avec les plans de formation continue des entreprises locales utilisatrices ou offreuses de solution.
- l'organisation de parcours dédiés avec une proximité géographique des lieux de formations pour faciliter leur suivi par les élèves et les enseignants et l'utilisation de méthodes de formation à distance innovantes et interactives.
- la mise en capacité de répondre à la demande toujours croissante d'alternants de niveaux Bac+2 à Bac +5, voire de niveau Bac.
- la possibilité de pourvoir aux offres d'emploi très spécialisées.

3

Lisibilité et rayonnement de l'offre de formation :

- la création de quelques programmes pédagogiques d'excellence permettant d'attirer des talents au niveau Européen.
- la visibilité de l'offre de formation de chacun des acteurs régionaux et d'une offre globale consolidée lisible.

7.

Soutien & croissance des Startups & PME

7.1 Etat des lieux

- A ce jour, plusieurs **actions spécifiques à l'IoT** sont en cours en complément de l'offre générique de soutien du Pôle auprès des startups et PME.
- Un projet d' « **IoT Center** » incluant des capacités de prototypage, de test, de caractérisation sécuritaire et un espace de démonstration (*showroom*) est à l'étude dans le contexte du **programme IPCEI Région Sud**, afin de réduire les temps de développement et de mise sur le marché de **solutions IoT intégrant les composants microélectroniques** à l'état de l'art pour les acteurs économiques de l'écosystème.
- Emergence et montage de projets comme les programmes **EE Innosup IoT4Industry¹⁹** et **AdPack2**.
- Pilotes et déploiements d'expérimentation **Smart-City et Industrie 4.0** en liaison avec les programmes régionaux, le programme **EE Innosup IoT4Industry**.
- Le **plan MicroPACA2020²⁰** initié par SCS en **2018** a généré des actions en faveur de certains acteurs de l'IoT. En particulier, un accompagnement dédié à **l'excellence opérationnelle** et visant à répondre aux enjeux des concepteurs de produits a été imaginé et déployé par le Pôle SCS auprès de **8 entreprises**.

Il vise à identifier les points de progression des startups et PME sur les **4 piliers fondamentaux** que sont le **produit**, le **marché**, les **compétences** et le **financement**, ainsi que les actions à mettre en œuvre pour permettre la croissance et l'accélération.

L'**accompagnement individuel** de chaque entreprise est réalisé de façon suivie dans le **temps de 6 à 12 mois** par des experts de très haut niveau du domaine et **assisté d'un comité de pilotage du Pôle SCS**.

- Evolution, mise à niveau et renforcement des plateformes **CIMPACA** pour prise en compte des nouveaux enjeux liés à l'IoT.



¹⁹ <https://www.iot4industry.eu/>

²⁰ [www.presseagence.fr/lettre-economique-politique-paca/2017/05/22/...](http://www.presseagence.fr/lettre-economique-politique-paca/2017/05/22/)

7.2 Enjeux

IoT

ACCELERATION PERENNE DES TPE/PME ET ETI DU POLE SCS EN LIEN AVEC L'IOT

- Consolidation et évolution du business model des startups et PME existantes pour aborder les phases de déploiement de l'IoT (*objet versus service clé en main en particulier*).
- Intégration de l'IoT dans les offres des entreprises traditionnelles.
- Positionnement vis à vis des écosystèmes émergents de l'IoT en cours de structuration (*marchés verticaux, plateforme, connectivité*).
- Cross fertilisation avec les autres feuilles de route : sécurité, microélectronique, IA pour gagner en compétitivité grâce aux synergies de l'écosystème.
- Développer les relations avec les acheteurs et l'accès aux clients. L'enjeu est l'application effective du Small Business Act.
- Visibilité et mise en avant via des expérimentations terrains portées par les grands groupes et les institutionnels.

« IOTISATION » DES ENTREPRISES REGIONALES

Il s'agit de renforcer la compétitivité et le développement des entreprises régionales dans la continuité de la digitalisation en cours en s'appuyant sur les écosystèmes des pôles applicatifs (*Eurobiomed, Cap Energies, Safe Cluster, Pôle Mer, ...*).

L'IoT est un vecteur d'efficacité opérationnelle.

Une bonne sensibilisation des entreprises aux enjeux de l'industrie 4.0 est un enjeu majeur.

CREATION ET DEVELOPPEMENT DE STARTUPS IOT

Cet enjeu se décline sur plusieurs axes :

- La capacité du territoire à attirer les startups grâce à un positionnement fort sur les thématiques complémentaires que sont l'IoT, l'IA et la sécurité.
- La valorisation des recherches académiques avec création d'entreprises associée.
- L'accompagnement des startups en particulier sur les aspects RH et financement.

Sensibiliser les équipes et les dirigeants de startups sur des sujets autres que leur expertise IoT est nécessaire. Les technologies nommées « Blockchain, IA, apprentissage autonome, renforcement learning... » ne sont pas que des buzz words.

Des opportunités concrètes peuvent naître si ces équipes bénéficient d'une réelle pédagogie sur ces nouveaux concepts émergents. A titre d'exemple, on peut citer les opportunités de conception de nouvelles puces électroniques permettant de réaliser des calculs localement au plus près des objets IoT en s'affranchissant des réseaux (*edge computing*).

Les aspects financement sont critiques dès lors que les startups se positionnent sur des composants hardware nécessitant des moyens financiers plus importants que dans le logiciel au démarrage.

LE DECLOISONNEMENT ENTRE LES DISCIPLINES ET LES EXPERTISES PAR L'INNOVATION

- Expertises sectorielles/ expertises technologiques, composants/cloud...

LA VALORISATION DES DONNEES ISSUES DE L'IOT

Les données générées par l'IoT sont le moteur de nouveaux services et applications. Permettre aux acteurs de l'écosystème de capter la valeur générée est un enjeu majeur.

Cela commence par la facilitation de l'accès aux données (*incitation à la mise à disposition de jeux de données, garantie de traitement de ces données conformément aux bonnes pratiques et règlements en vigueur...*). Cela peut donner naissance à des initiatives de Data Market Place ou Data Lake.

8.

Visibilité & attractivité & communication

8.1 Etat des lieux

A ce jour le Pôle a conduit plusieurs actions spécifiques à l'IoT en complément de ses actions génériques. A titre d'exemples on peut citer la publication de **livres blancs et d'étude** (IoT, Sécurité de l'IoT), l'animation d'un groupe de travail spécifique à l'IoT.

Le pôle a animé plusieurs événements permettant de diffuser la **culture IoT** auprès de différents public (*animation de tables rondes avec des chercheurs et des industriels...*).

Le Pôle a relayé les travaux effectués par les comités de standardisation et les groupes de travail pour une **bonne diffusion dans l'écosystème** (*OneMtoM, ETSI/GSI, Global Platform...*).

Positionnement de l'IoT au cœur de **journées marchés** animées par le Pôle SCS (*IoT pour le retail, IoT pour la santé, IoT pour l'e-administration, IoT pour le transport et la mobilité, IoT pour le transport et la logistique...*).

8.2 Enjeux

Pour la période à venir 2019/2022, plusieurs enjeux ont été identifiés :

- **Localisation d'activités de conception, fabrication voire production de briques technologiques IoT en Région SUD** (*depuis les composants en passant par les protocoles, réseau jusqu'aux applications de l'IoT*).
- **Communication autour d'une stratégie de sécurité intelligente pour l'IoT**: il faut communiquer auprès des « utilisateurs » et donneurs d'ordre que la construction aujourd'hui d'outils capables de traiter les attaques de demain est en cours et en region et que ces outils sauront **s'adapter au degré d'intensité de ces attaques**.
- La mise en œuvre de la nouvelle **loi RGPD** pour être **visible des fabricants d'objets connectés** qui se doivent d'être conforme à la réglementation européenne avec une **gestion de la vie privée et des données personnelles (Privacy)** optimisée et ce grâce aux travaux des acteurs SCS à valoriser.
- Bâtir des **formations attractives et en adéquation avec le besoin des entreprises** locales et notamment les PME. La disponibilité de certains jeunes diplômés polyvalents mais aussi de seniors Experts IoT expérimentés (**à « retenir » avec des salaires ou conditions attractifs, car attirés par les grands groupes nord européens**) est majeure : L'investisse-

ment et la croissance de certaines PME concepteur d'objets ou de solutions IoT **nécessitent une fluidité du marché de l'emploi** pour ces profils très qualifiés et prisés.

- La **transformation digitale des entreprises manufacturières grâce à l'IoT** - pour booster la productivité, optimiser les coûts (*à travers la maintenance prédictive par exemple*).
- **Pérennisation de l'expertise en Sécurité de l'IoT** (*issue de l'industrie de la carte à puce il y a quelques années*) en favorisant l'implémentation de sécurité numérique dans les expérimentations locales et en le valorisant - mais aussi en communiquant sur les travaux de recherche, issus des laboratoires, intégrés dans ces projets.
- Attractivité de SCS vis-à-vis des **clusters européens partenaires** (*plusieurs sont des partenaires clés de SCS et positionnés sur la thématique IoT*) afin de booster **l'internationalisation de nos PME** à travers des missions organisées.



Les actions principales autour de l'IoT pour les 4 années à venir se résument ainsi :

1

GÉNÉRER, VALORISER ET DÉPLOYER DES INNOVATIONS ET DES AVANCÉES TECHNOLOGIQUES

A Intensifier l'animation et la structuration de l'écosystème d'innovation :

1. Des journées thématiques et des masterclass pilotées par des experts
2. Promotion des expertises, des ressources et moyens mutualisés

B Développer des projets de R&D innovants technologiques et usages :

1. Animer un groupe de travail pour mettre en avant les compétences technologiques, les plateformes mutualisées et des idées de projets innovants
2. Réunions d'informations sur les différents dispositifs de financement
3. Accompagnement et labellisation des projets R&D remontés par les acteurs SCS
4. Organiser des conférences marchés/usages notamment en partenariat avec d'autres pôles clusters marchés

C Valoriser les projets de R&D et leurs retombées :

1. Collecter et recenser les différents projets des membres SCS
2. Etablir un catalogue des projets et des produits issus des projets
3. Organiser des conférences et animations avec restitution des résultats des projets
4. Promouvoir le passage à l'industrialisation des prototypes et des produits issus des projets en s'appuyant notamment sur les plateformes mutualisées en microélectronique (IoT center, CIMPaca...)

2

ACCÈS MARCHÉ

A Accélérer l'accès sur les marchés en croissance :

1. Continuer et renforcer les partenariats avec les réseaux « utilisateurs » (*Pôles filière, IMA, cluster EE, Centre 3IA, Communauté FT, UIMM, Mercatel*) et partenaires (*centre 3IA : health, biotech, smart territories*)
2. Organiser des actions d'open Innovation avec les Grands Groupes et collectivités (*région, membre centre 3IA...*) et sourcing de solutions auprès de PME/startups IoT
3. Organiser des animations & espaces d'échanges entre offreurs & End user d'un marché donné



SOUTIEN AUX PMES ET STARTUPS IoT & OBJETS CONNECTÉS

A Accompagner la croissance & efficacité opérationnelle :

1. Accompagner la création de startups (*briques technologiques, offres ou services à base d'IoT*) en liaison avec les SATT et les incubateurs
2. Accompagner le renforcement du financement des startups et des PME notamment en fonds propres
3. Proposer un catalogue d'outils pour l'efficacité opérationnelle (*marketing, stratégie, pitch, salons, ...*)
4. Proposer des accompagnements pour les PME à des conférences et des salons majeurs nationaux et internationaux sur l'IoT & électronique et les marchés associés
5. Mettre en avant des offres et compétences des startups et PME dans des catalogues thématiques (*ex Industrie du Futur, Sécurité de l'IoT..*)



FORMATION

- A Accompagner le développement d'une offre complète de formation initiale et continue dans le domaine de l'IoT en liaison avec les campus des métiers et les besoins des industriels**



VISIBILITÉ & ATTRACTIVITÉ

A Promouvoir l'expertise et les compétences de SCS auprès de la communauté scientifique internationale, des acteurs du marché et des décideurs :

1. Continuer à communiquer et promouvoir les avancées des acteurs de SCS (*technologies, marché, contrat signé, projet...*)
2. Assurer la visibilité de la filière IoT et électronique SCS dans les stratégies régionales (*OIR*), nationale (*CSF électronique & Alliance Industrie du Futur*) et Européenne

10.1 Méthodologie et références

La feuille de route IoT du Pôle SCS a été réalisée avec un processus sur 3 mois qui repose sur des **réunions physiques du comité restreint IoT** et de la Plénière où tous les acteurs SCS ont été invités à participer.

Le comité restreint, composé d'industriels petits et grands et d'organismes de recherche.

Références

La feuille de route IoT s'appuie sur les résultats de différentes études récentes externes listées ci-dessous (DGE/PIPAME, McKinsey, DHL/CISCO, ABI research, Pwc en particulier).

Elle s'appuie également sur les études menées par le Pôle SCS²¹, en particulier :

- La sécurisation de l'IoT
- Etude IoT en 2016
- Livre blanc Réseaux, M2M & Services Mobiles

Les différents travaux réalisés par le Pôle ainsi que l'étude DGE/PIPAME 2018 sont téléchargeables sur le site du Pôle SCS.

Documents de références

- Prospective/ Marché des objets connectés à destination du grand public, DGE/PIPAME, 2018
- Internet of Things, How to capture the value of IoT, McKinsey, 2018
- THE INTERNET OF THINGS: MAPPING THE VALUE BEYOND THE HYPE, McKinsey 2015
- Internet of Things trends in Logistics, DHL Trend Research | Cisco Consulting Services, 2015
- Driving Unconventional growth through IoT, Accenture 2015
- The Industrial Internet of Things /Why it demands not only new technology—but also a new operational blueprint for your business – Pwc 2015
- Etude ABI Research du 23 octobre 2018 « IoT Market Tracker – Worldwide »

10.2 Présentation du Pôle SCS



Le Pôle de compétitivité Solutions Communicantes Sécurisées (SCS) (www.pole-scs.org) est un acteur

important et reconnu dans le domaine des technologies du numérique. Il rassemble plus de **320 membres** (grands groupes, laboratoires de recherche et plus de 200 startups & PME) en Région Sud, représentant **60 000 emplois** dans ce domaine.

Ces acteurs couvrent l'ensemble de la chaîne de valeur des métiers du numérique, du silicium aux usages :

microélectronique, télécommunications et logiciel. SCS se focalise sur **4 domaines technologiques** :

MICRO

Microélectronique

SECURITE

Sécurité numérique

IA

BigData & Intelligence Artificielle

IoT

Internet des Objets

pour servir des marchés en croissance tels que la santé, les smart-cities, le transport & logistique, l'Industrie 4.0, le retail, etc.

SCS est un **acteur de dimension nationale** et européenne. Nationale au travers de son réseau de partenaires et notamment les Pôles Systematic, Minalogic et Images&Réseaux avec lesquels il a signé une charte de collaboration Européenne grâce à son réseau de partenaires au sein de l'Alliance « **Silicon Europe** » (www.silicon-europe.eu).

SCS a reçu **en 2013 le Label Gold**, délivré par l'ESCA (European Secretariat for Cluster Analysis), pour la qualité de l'animation de son écosystème, de son processus de labellisation et de son management.



²¹ <https://www.pole-scs.org/publications/livres-blancs-etudes/>

10.3 Formations diplômantes de Bac à Bac+5 en électronique en Région SUD MAJ*

Parmi les formations diplômantes ingénieurs existantes en Région SUD on peut citer :

FISE

- **Ingénieur** ISMIN de l'École des Mines de Saint-Etienne
- **Ingénieur** Centrale Marseille
- **Ingénieur** Polytech Marseille (*Filière Informatique, Microélectronique et Télécoms, Génie Industriel*)
- **Ingénieur** Polytech Nice Sophia Antipolis (*Filière électronique, Filière informatique, Bâtiments intelligents, Mathématiques appliquées*)
- **Ingénieur** ISEN Toulon (*Filière informatique et Réseaux, Filière Biomedical et E-santé*)
Ingénieur Seatech, Université de Toulon (*parcours ingénierie et sciences des données, information, systèmes*)

FISA

- **Ingénieur** ITII Option EI CFAI Istres / Polytech Sophia
- **Ingénieur** ITII Option Meca CFAI Istres / ENSAM Aix
- **Ingénieur** ITII Option Systèmes Électriques ENSAM Aix
- **Ingénieur** Polytech Nice, Filière électronique et Informatique industrielle
- **Ingénieur** ISEN Toulon (*Filière informatique et Réseaux*)

UNIVERSITAIRES DE NIVEAU BAC+5

- **Master** Nanosciences et Nanotechnologies (AMU, Ecole des Mines de Saint-Etienne)
- **Master** instrumentation, mesure , métrologie (AMU)
- **Master** Électronique, énergie électrique, automatique (AMU, UCA)
- **Master** Sciences des données (UCA)
- **Master** réseaux et télécommunications - parcours IoT (*initiative intéressante avec un master co-habilité entre AMU et l'École des Mines de Saint-Étienne à Gardanne*)

BACHELOR OU LICENCES EXISTANTES EN REGION SUD

- **Master** Techniques
- **Licence** professionnelle EPOCS
- **Bachelor** e-maintenance CFAI Istres
- **Bachelor** Supply chain CFAI Istres
- **CQPM** CatC/D CQPM Cat C/D

DIPLOMANTE BAC+2

Une révolution apparaît avec la transformation des DUT en BUT (*Bachelor*) BAC+3 qui est en marche et dont les programmes sont en cours de finalisation. Réforme prévue en sept 2021.

- BTS Systèmes Numériques Option Électronique & Communication (Lycée Fourcade)
- BTS Electricité & composants
- DUT Mesures physiques (AMU)
- DUT Informatique (AMU, UCA)
- DUT GEII (AMU, UTLN, UCA)
- DUT Réseaux et Telecoms (UCA, AMU)
- BTS Maintenance des systèmes de prod (Lycée Vauvenargues / CFAI Istres)
- DUT GMP Gestion Maintenance Production (AMU)
- CQPM Cat B

NIVEAU BACCALAUREAT (GENERAL, PROFESSIONNEL OU TECHNOLOGIQUE)

- Bac Techno Sti 2d (Lycée Fourcade)
- Bac Pro MEI (Maintenance Équipements Industriels) (Don Bosco, Vauvenargues)
- Bac Pro Électrotechnique (Lycées Langevin, St Eloi)
- Bac Pro SEN Syt Electroniques Numériques
- Généraliste Bac S
- Bac Pro PLP Pilote Ligne de Prod

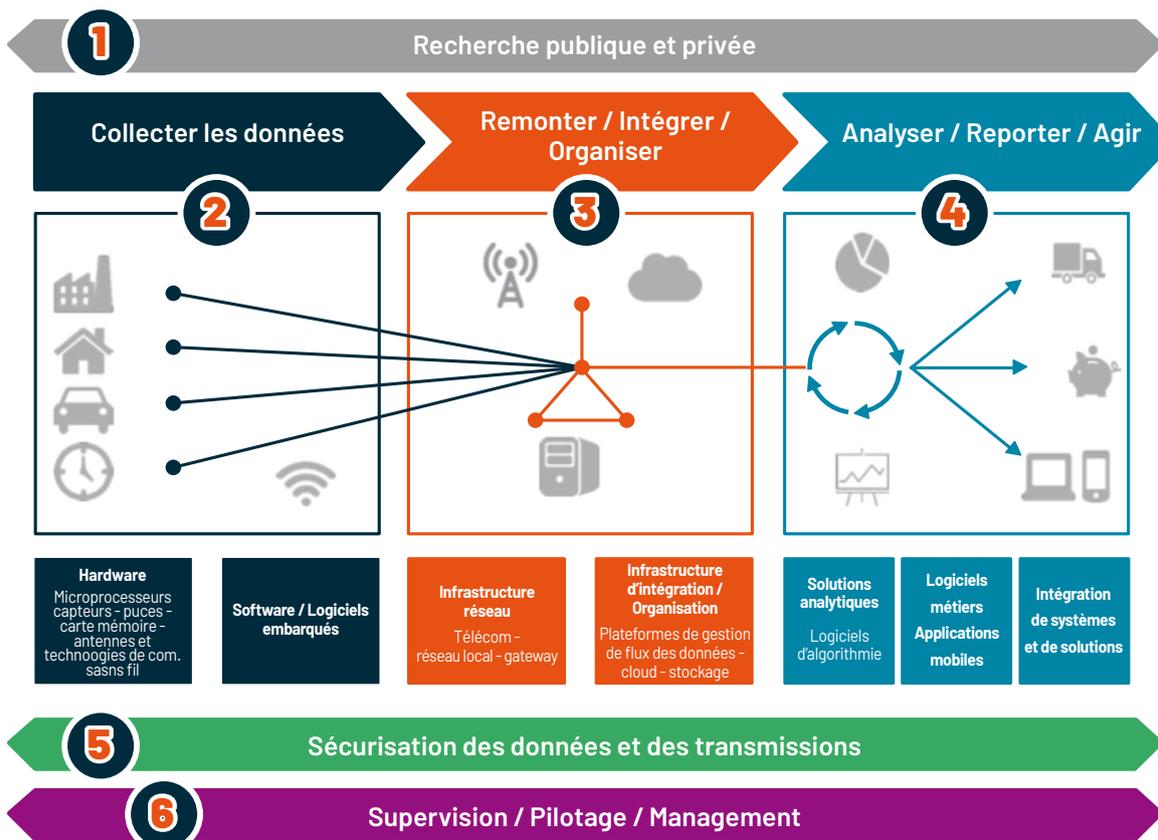


10.4 Cartographie des acteurs de l'écosystème SCS

L'écosystème de SCS comprend des acteurs présents sur l'ensemble des blocs de la chaîne de valeur technologique à l'exception des fonderies et des sous-traitants de packaging. Cette couverture de la grande majorité de la chaîne de valeur permet à l'écosystème de conserver une forte expertise et de développer avec l'aide des laboratoires de recherche des projets innovants collaboratifs au bénéfice de la filière.

Grands groupes et ETI

Des grands groupes comme STMicroelectronics, Gemalto (*Thalès company*), HPE, Orange, Dicaposte, Schneider Electric, Enedis, Thales Alenia Space, Kontron, sont actifs à différents maillons de la chaîne de valeur, du composant à l'intégration dans des solutions applicatives.



Startups et PME

Le tissu de PME et de startups se développe comportant des pure players développant des briques ou des services pour l'IoT ou des solutions intégrées (*Traxens, suivi de containers, pilotage de piscine...*) ou des sociétés connectant leurs offres existantes.

Une liste indicative des PME du Pôle est fournie.

1 Recherche publique et privée :
AIX MARSEILLE UNIVERSITÉ / CEA / EMSE / EURECOM / I3S / IM2NP / INRIA / ISEN / LEAT / SATT SUD EST / UCA / UNIVERSITÉ TOULON / W3C

2 Collecter les données :
ADIPSYS / AMINOGRAM / ASYGN / AXYN ROBOTIQUE / CETRAC.IO / EDITAG / FEELIGREEN / I-MC / INNEOSENSE / INSIGHT SIP / IONOSYS / KAPSYS / LUCIELABS / MIOS / MOTEBO / NANOZ / NAWA TECHNOLOGIES / NEOWAVE / ONDILO/STARCHIP/SWAP//TRAXENS/TRUSTED OBJECTS

3 Remonter / Intégrer / Organiser :
4G TECHNOLOGY / ABEWAY / AITIVITY / ANYCES / APICAL / ASALOG / AXYN ROBOTIQUE / EUKLES / FEELIGREEN / FENOTEK / FINGERTIPS (EX SPIN-OFF) / FOCUSSIA / IOTHINK SOLUTIONS / GINKOLEA / KONTRON / NAUVELIS / NEWSTEO / SNAPSYS TELECOM / VDSYS

4 Analyser / Reporter / Agir :
ADD / ATG TECHNOLOGIES / BIOCEANOR / ERIDANIS / EZAKO / HD-SIGNS / IGNILIFE / INOUID / NEWSTEO / OLYTHE / SENSORIA ANALYTICS / TELAQUA / VULOG

5 Sécurisation des données et des transmissions :
HIMYDATA / HOGO / KEEEX / NEOTION / PROVE & RUN / SMARTTV / SMART PACKAGING SOLUTIONS (SPS) / TRUSTONIC / TEXPLAINED / TRUSTAZUR / WISEKEY

6 Supervision / Pilotage / Management
KEOLABS / NERYS

10.5 Fiches des différents laboratoires de recherche IoT en Région SUD MAJ*

En matière de recherche fondamentale et de recherche appliquée, une étude des principaux laboratoires sur le territoire de SCS a permis d'identifier les centres de recherche **ci-dessous**.

Ces organismes sont particulièrement présents sur l'IoT avec des expertises complémentaires (*Composants et systèmes embarqués, réseau et connectivité/radiofréquences, cloud/fog et edge computing, logiciel, données et intelligence artificielle...*).



10.6 Segmentation Marché IoT par application et usages

L'IoT fait l'objet de nombreuses études de marché. L'étude ABI Research du 23 octobre 2018 « IoT Market Tracker – Worldwide » est particulièrement pertinente. Cette étude en anglais classifie les marchés par types d'applications et usage, suivant les définitions suivantes :

ASSET MANAGEMENT

Asset Tracking

Primarily readers and tags used to track and locate assets using tag types including cellular, Bluetooth (BT), Wi-Fi and 802.15.4 in wide-area and local area/indoor settings.

Inventory Management

Primarily barcode scanners and Personal Digital Assistants (PDAs), ingress/egress scanners.

ENERGY MANAGEMENT

Smart Metering

Communication enabled electrical meters located at single family homes, Multi-Dwelling Units (MDUs), and commercial buildings.

Smart Grid

Smart meter data concentrators/aggregators and connected energy transmission and distribution equipment.

Water and Gas Meters

Communication-enabled water and gas meters installed at single family homes, MDUs, and commercial buildings/facilities.

Commercial Building Automation and Security

Commercial building Heating, Ventilation, and Air Conditioning (HVAC) control and monitoring; lighting control and monitoring; fire and life safety systems consist of smoke, fire, and toxic substance sensors. Access control consists of the physical security systems of a building and represents a much newer building system market segment. Equipment consists of Identification (ID) card scanners, biometric scanners, and door controllers. Other category consists of vertical transport control (for elevators and escalators).

Other Energy Management Applications

Electric charging stations and related infrastructure, solar power and wind mill monitoring and control.

SECURITY MANAGEMENT

Home Security and Automation

Security and building automation for homes. This category covers a range of applications and sensors, including connected thermostats, door locks, video cameras, contact sensors, and motion detectors, etc...

Video Surveillance

Internet Protocol (IP) and CCTV cameras and surveillance systems for commercial and government applications.

LOCATION/TRACKING (Note: Agriculture segment listed below includes forecasts for fleet tracking)

Fleet Management

Includes fleet management for the commercial trucking industry and trailer tracking. Also includes the nontrucking industry, including construction, government, emergency services, private transportation, services (including utilities), and local delivery.

OEM Telematics

Factory-installed telematics used for safety and security, concierge services, and infotainment in passenger vehicles.

Aftermarket Telematics

Consumer telematics installed by the consumer or non-automaker third party for applications such as teen driver monitoring, sub-Prime auto financing, broadband-to-the-car, and stolen vehicle recovery.

People and Animal Tracking

Tracker devices used for tracking seniors, children, pets, prisoners, Alzheimer's/autism patients, lone workers.

Heavy Transport Vehicles and Equipment

Mobile industrial equipment such as earth-moving equipment, railroad engines, boats/ships.

MONITORING/STATUS

Condition-Based Monitoring/Maintenance

Stationary equipment not included in asset tracking: weight scales; refrigeration units and ovens used in restaurant, manufacturing, and warehousing industries; connected pumps, fluid flow meters, and tanks used in utilities, manufacturing, pipelines, warehousing, and storage; connected manufacturing equipment used for milling, cutting, joining, and assembling raw materials and Work in Progress (WIP); gas stations (car wash, gas tanks, gas dispensers); retail (lottery terminals, gaming terminals); mining equipment; generators and battery monitoring.

Usage-Based Insurance (UBI)

Insurance telematics that set user insurance rates based on driving behavior.

Home Appliances

Home appliances such as coffee machines, washer/dryer, refrigerators, freezers, stoves, dishwashers, etc...

SMART CITIES

Smart Parking

Connected meters for individual parking spaces and parking ticketing machines.

Smart Street Lighting

Connected lighting systems in streets and parking lots.

Intelligent Transportation

Electronic toll collection; vehicle-to-infrastructure communications used for rail, commercial, and passenger vehicles.

Other Smart Cities Applications

Connected trash and refuse container monitoring; connected environmental, chemical, and radiation monitoring applications.

HEALTHCARE

Patient Monitoring

Regulated wearable wireless-enabled devices, appliances, and gateways used in doctor-prescribed monitoring applications for remote and on-site professional healthcare use.

Home Monitoring

Wearable and wireless-enabled devices, appliances, and gateways used for aging in place, personal emergency response systems (*PERS*), and ambient assisted living applications.

Well-Being and Fitness Wearables

Wearables worn for sports, fitness, and wellness applications, such as pedometers, heart-rate monitors, activity trackers.

Healthcare Equipment Monitoring

Healthcare equipment monitoring for imaging (*Magnetic Resonance Imaging (MRI), X-ray, etc.*), lab diagnostic, and patient monitoring equipment.

OTHER VALUE-ADDED APPLICATIONS (*Primarily Retail and Finance Applications*)

ATMs (*Banking*)

Automated Teller Machines (*ATMs*) at bank locations and in retail locations, primarily malls, grocery, convenience stores, pharmacy chains, and mass-market retailers.

PoS (*Point of Sale*)

Mobile and fixed terminals used for conducting financial transactions.

Digital Signage

Digital display screens that are used to display content that can either be information-based, advertising-based, or programming information.

Vending

Vending machines are defined as machines that dispense any number of items, including snacks, coffee, cold beverages, and other consumer products.

Connected Kiosk

Kiosks that dispense mostly non-consumable items, such as DVDs and coins, and provide services such as bill payment, airport check-in, and product information. The primary categories are retail, entertainment, travel, financial services, municipal/government, healthcare, information, and other.

Wearables

Wearable glasses and wristwear used to assist employees in completing work activities.

Connected Agriculture

Stationary to low-mobility machines and systems used in agriculture operations, including irrigation systems, environmental sensors, animal support machines, and tank monitoring. Includes fleet tracking/monitoring of mobile equipment, such as tractors and combines, etc...

10.7 Exemples de projets SCS liés à la technologie IoT MAJ*

Ci-dessous sont listés quelques exemples de projets monopartenaires ou collaboratifs innovants et labellisés par SCS et issus des actions SCS autour de l'innovation.

IOTIZE



Le projet **IOTIZE** vise à développer un module permettant de connecter des objets à internet via un smartphone. Celui-ci fera le lien, de manière sécurisée, entre un dispositif mobile sans fil et un objet physique. Il se connectera à un smartphone via une liaison sans fil (NFC, BLE, Wi-Fi...), au port de debug des microcontrôleurs contenus dans des systèmes. L'originalité réside dans sa caractéristique « Plug - Configure - Play » lui permettant de contrôler toute application à base de microcontrôleur, sans modification, matérielle ou logicielle, sur le système embarqué.

GEOLOC



Le projet **GEOLOC** vise à combiner les informations issues des différents standards supportés par un objet (LoRa, LTE-M) mais aussi (BLE, Wifi, GPS), ainsi que de différents capteurs pour améliorer la précision de la géolocalisation tout en maîtrisant la consommation ; à améliorer les techniques existantes de géolocalisation ; d'utiliser les informations de géolocalisation pour améliorer l'efficacité des transmissions entre l'objet et l'infrastructure ; à minimiser la consommation globale de l'infrastructure et de l'objet connecté.

SMART PESEE



Le projet **Smart Pesee** vise à développer et commercialiser un système innovant et low cost de pesée de camion (dispositif très compact de quelques cm³). Il s'agit d'un système électronique autonome composé d'un capteur de pesée d'un nouveau type, qui pourra transmettre par Bluetooth vers un Smartphone ou un autre dispositif de réception.

AROMACARE



L'**AromaCare** est un diffuseur innovant qui permet un traitement complémentaire personnalisé du patient selon sa problématique de santé/bien-être. Le dispositif utilise des capsules d'aromathérapie prêtes à l'emploi et de part sa connectivité, il facilite le paramétrage et la programmation, la gestion de l'ensemble des chambres concernées, facilite le réassort du consommable et apporte une traçabilité.

4TRAX



Plateforme Mondiale d'Information Conteneurs, dédiée à l'écosystème du transport multimodal conteneurisé. Le projet **4TRAX** éprouve et durcit une solution complète comprenant le composant embarqué sur les conteneurs, les serveurs centraux, les applications pilotes, une plateforme de développement collaborative, l'épreuve sécuritaire de la solution ainsi que des analyses sur ses impacts organisationnels, économiques et sociétaux.

3C

Cashierless Concept Centriloc



L'objectif du projet est de réaliser une preuve de concept pour le self checkout dans le retail, qui permettrait de valider la faisabilité de notre solution pour la détection et la discrétion d'un client parmi d'autres individus à proximité sans l'utilisation de reconnaissance visuelle ainsi que la détection et le suivi d'articles pris en main et/ou déposés n'importe où dans le magasin.

NOS FINANCEURS





Business Pôle - 1047 route des Dolines,
Allée Pierre Ziller, Bâtiment B, Entrée B, 1er étage
06560 Valbonne - Sophia Antipolis

Place Paul Borde
13790 Rousset

contact@pole-scs.org
www.pole-scs.org