Année universitaire 2019-2020

Licence pro

« Métiers des Réseaux Informatiques & des Télécommunications »

Parcours « Internet des Objets »

Mémoire de fin d'études présenté pour l'obtention du grade de licence

Le développement de l'Internet des Objets : quel impact sur le secteur automobile ?

Présenté par **Luc Pascual**

Numéro d'étudiant : **1109001197j**

Sous la direction de **Sébastien Druon**, enseignant au département R&T

Mémoire de fin d'année à l'IUT de Béziers

1. Introduction :

Nous vivons dans une ère qui se veut de plus en plus connectée, les communications que nous connaissons font désormais preuve de beaucoup plus d'autonomie, facilitant ainsi la tâche de l'Homme dans son quotidien. Des objets de tout type tels que des capteurs, des véhicules ou même des villes peuvent dorénavant bénéficier d'une connexion à Internet ; la technologie qui se cache derrière cette interconnexion de masse est surnommée l'Internet des Objets (IoT).

Cela fait maintenant une dizaine d'années que l'IoT (terme inventé pour la première fois en 1999 par l'entrepreneur britannique Kévin Ashton) rencontre un essor considérable, et particulièrement au cours de ces dernières années, comme le montre la Figure 1.

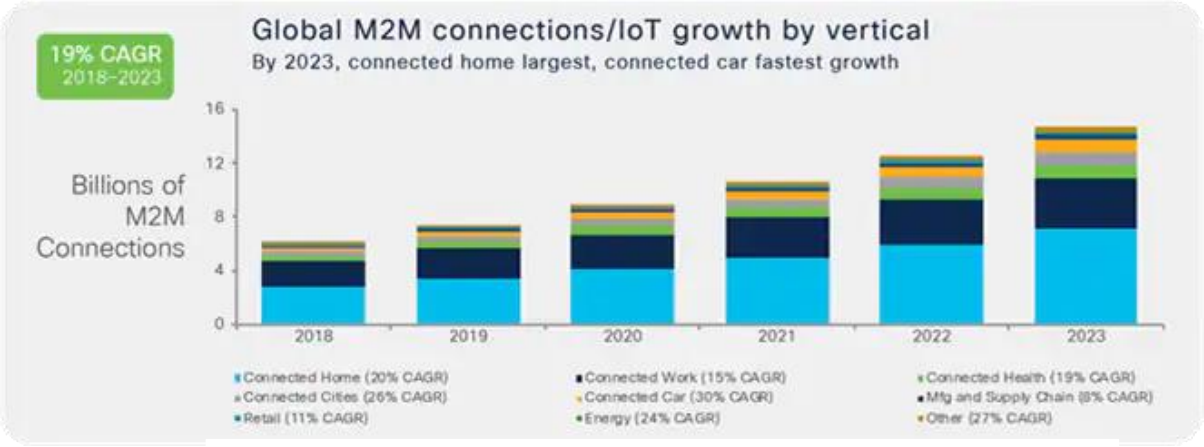


Figure 1 : Cisco Annual Internet Report, 2019

Bien que son emprise s'étende dans différents domaines tels que la santé ou le bâtiment intelligent, nous avons choisi dans ce mémoire de nous pencher sur le secteur automobile, qui laisse de plus en plus place à la numérisation, afin de donner naissance à un nouveau type de transport dit intelligent et connecté.

En effet, le marché global des voitures connectées est estimé à 217,7 milliards de dollars pour 2027 contre 42,6 milliards de dollars environs en 2019 [1] avec un TCAC* de 22,3 %.

Nous allons essayer d'apporter un début de réponse, en nous concentrant sur les enjeux de l'industrie automobile, face à cette révolution numérique :

- Dans un premier temps, nous définirons en détail le concept d'IoT et expliquerons son fonctionnement, ainsi que les défis à relever.
- Deuxièmement, nous évaluerons son impact dans le secteur automobile tout en exposants les enjeux qu'il soulève.
- Dernièrement, nous concevrons un système embarqué répondant à un besoin.

2. l'Internet des Objets

2.1. Concept et définition :

Internet, une invention qui n'a de cesse de nous surprendre et qui permet à la majorité d'entre nous, l'accès à la plus grosse bibliothèque d'informations jamais créée, tout en nous offrant une interconnexion mondialement reconnue. Son omniprésence nous interroge sur ses perspectives d'utilisation, notamment en termes de collecte et d'analyse de données [2].

En effet, de plus en plus de technologies dépendantes d'Internet voient désormais le jour, et cette montée en puissance transforme les moyens de communications. Au tout début, les messages n'étaient transmis qu'entre ordinateur, mais dorénavant, l'apparition du M2M (machine-to-machine) à complètement chamboulé notre vision des choses, laissant ainsi place à des échanges ne nécessitant aucunes interventions humaines.

L'Internet des Objets, plus connu sous sa version anglophone Internet of Things (IoT), caractérise un réseau qui permettrait de connecter n'importe quoi à Internet, dans le but d'établir une communication par échange d'informations ; des informations utilisées à des fins de traçage, de surveillance, et d'administration [3].

De ce fait, nos « objets » du quotidien, subissent actuellement une transformation en étant doté d'une d'intelligence, leur permettant de comprendre leur environnement et d'agir en conséquence [4].

Toutefois, il est difficile de donner une définition officielle de l'IoT, car chacun peut se faire sa propre interprétation de ce que cette technologie signifie, en fonction du domaine dans laquelle elle est employée. Ce flou général n'en est pas moins traduit par les deux termes qui le composent ; effectivement l'Internet et l'Objet présentent deux axes de vision différents selon l'étude mené par Luigi Atzori, Antonio Iera et Giacomo Morabito [5] :

- Une première centrée infrastructure réseau.
- Une seconde, portée sur « l'objet » en lui-même.

En outre, il faut bien garder en tête ces deux paradigmes lorsque nous parlons d'IoT.

Vient s'ajouter à ça la sémantique, qui traite des normes de communication cherchant à favoriser l'interopérabilité et le traitement des données ; l'un des enjeux principaux dans ce domaine, comme nous le verrons par la suite [6].

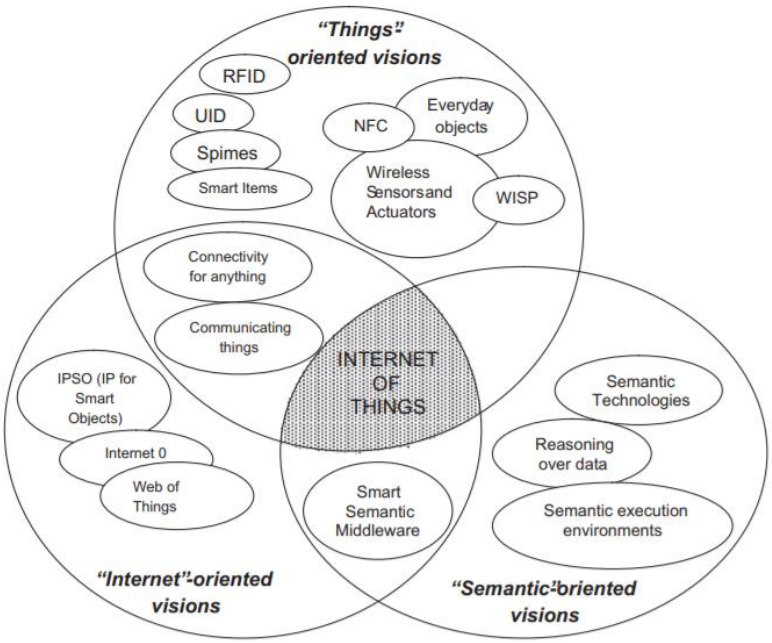


Figure 2 : Convergence des différentes visions de l'IoT (L. Atzori et al, 2010)

2.2. Son architecture :

Son fonctionnement se base sur une architecture dite orientée services (SOA), dont le but est de décomposer des fonctionnalités complexes et isolées, en un ensemble de services basiques et interconnectés, accessible par l'intermédiaire d'interfaces et de protocoles standards [7].

Dans le cadre de l'IoT, ces services sont découpés en 5 layers (couches) [8] :

- La première intitulée « **Perception Layer** » ou bien « **Device layer** », regroupe les appareils physiques, et se charge de l'identification et de la collecte des données grâce aux capteurs.
- La seconde « **Network Layer** » ou « **Transmission Layer** » garantit l'acheminement sécurisé des data recueillies, en direction du système de traitement.
- En troisième position, la couche « **Middleware** » va stocker les données transmises par la couche « Network » dans une BDD (base de données), avant de procéder à leur analyse. Une fois ces data traitées, elle pourra proposer toutes sortes de services aux couches inférieures.
- Quatrièmement, la couche « **Application** », qui fait office d'interface entre les utilisateurs et Internet, et (grâce aux data traitées par la couche Middleware) assure la gestion globale de l'application.
- Puis en dernière position, « **Business Layers** », qui en se référant aux données contenues dans la BDD, va permettre de prédire les actions futures.

Voici une vue d'ensemble de ces 5 couches, avec les éléments qui s'y rattachent ;

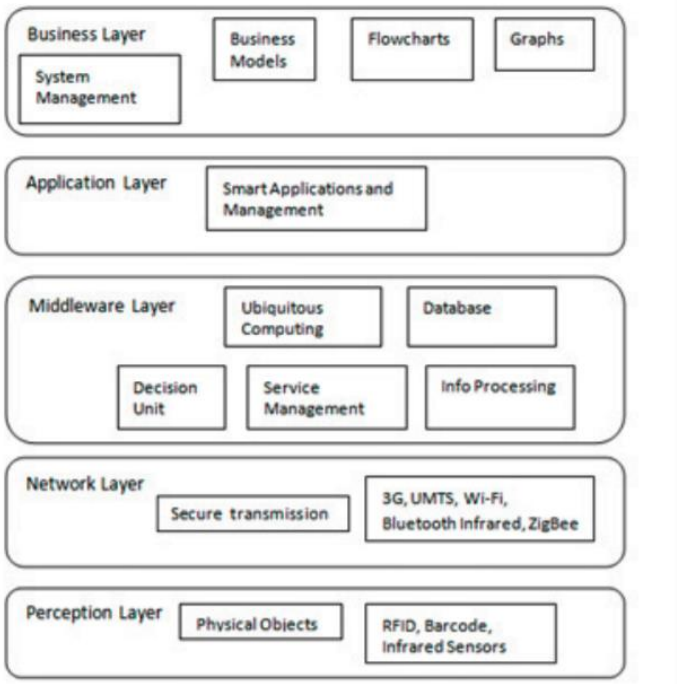


Figure 3 : Architecture IoT (Rishika Mehta et al, 2018)

2.3. Les défis à relever :

L'apparition des nouvelles technologies augmente de jours en jours, aussi bien dans notre société que notre quotidien, toutefois, certains de ses critères demandent à être étudiés en profondeur, avant de pouvoir passer à une implémentation qui se veut globale. La question de ses enjeux ne cesse de susciter l'attention, notamment en termes de sécurité et de confidentialité.

En 2013, Mahmoud Elkhodr, Seyed Shahrestanie et Hon Cheung, évoquaient justement dans leur étude intitulée *The Internet of Things : Vision & Challenges* [9], les différents aspects sur lesquels nous devons nous pencher, afin de permettre une utilisation sécurisée et optimale de ces nouveaux moyens de communications. De la même façon, Keyur K. Patel, Sunil M. Patel, P. G. Scholar et Carlos Salazare, ont également traité la question en 2016 dans leur article de recherche *Internet of Things-IOT : Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges* [3].

Bien que 3 années, durant lesquelles l'IoT n'a eu de cesse d'évoluer, séparent ces 2 recherches, les défis à relever sont plus ou moins restés les mêmes ; voici une liste de ces derniers.

2.3.1. L'interopérabilité :

L'interopérabilité est primordiale, puisqu'elle permet la mise en place d'un standard de communication entre des réseaux, et systèmes très différents les uns des autres. Bien que ce problème de conformité ne soit pas nouveau [10], il faut en faire une priorité, car l'IoT opère dans des domaines tous très hétérogènes, où chaque fabricant conçoit ses propres produits. Ces technologies ce doivent donc d'être sur le même pied d'égalité, afin d'échanger leurs informations tout en se comprenant mutuellement.

Son implémentation générale, repose avant tout sur la réussite de 5 aspects [11] [3] :

- Premièrement, **l'interopérabilité des systèmes**, qui assure la communication M2M en garantissant la bonne transmission des bits. Il existe tous un tas de protocoles de communications utilisés par certains dispositifs, mais qui s'avèrent inadaptés pour d'autres, d'où la nécessité de développer des normes communes.
- Deuxièmement, **l'interopérabilité réseau**, qui comme son nom l'indique, se charge de la transparence des échanges entre les réseaux. Que nous ayons affaire à un réseau Wi-Fi, GSM ou à basse consommation et longue portée tels que LoRa et Sigfox, il faut qu'un pont face le lien entre toutes ces infrastructures.
- Le troisième aspect, **l'interopérabilité syntaxique**, va quant à elle uniformiser les différent formats et structure de message, sous une même forme grammaticale. De ce fait, les messages seront encodés et décodés de la même manière.
- **L'interopérabilité sémantique**, dont le principe est de véhiculer des données qui se veulent significatives. Si les données perdent leur sens, cela compliquera la tâche de la personne en charge de l'analyse, qui ne saura les exploiter de manière sécurisée.
- Et enfin**, l'interopérabilité des plateformes**, qui doivent parfaitement s'implanter dans un écosystème IoT, afin de fournir des applications et des produits fonctionnants sous n'importe quel type de plateforme. A l'aube d'une ère où tout se veut connecté, nous devons pouvoir accéder à n'importe quel service sans rencontrer de difficulté.

En les respectant, nous pourrons surmonter les frontières qui font barrages entre les systèmes et les secteurs d'application.

2.3.2. Sécurité et confidentialité des données :

Qui dit connecté à Internet, dit mondialement attaquable par des personnes mal intentionnées, en outre, nous pouvons facilement imaginer les dégâts qui pourraient être causés à l'échelle d'un domicile ou d'une ville. De nombreux problèmes de sécurité liés à l'Internet des Objets subsistent, comme la sécurisation des liaisons sans fil, des échanges entre réseaux, ou bien la protection de la vie privée des utilisateurs, qui peut à tout moment fuiter.

De ce fait, le moindre appareil intelligent dont la sécurité n'est pas suffisante, représente un point d'accès permettant ainsi la défaillance du réseau auquel il est rattaché. Comme l'expliquent Hany F Atlam, chercheur, et Gary Wills, docteur en ingénierie, tous les systèmes IoT sont reliés au même titre qu'une chaîne, il suffit donc d'accéder à un seul de ses maillons pour nuire à l'ensemble [12].

C'est ce qui est notamment arrivé à un Casino, qui s'est vu pirater sa BDD, répertoriant la liste des clients VIP de l'enseigne. Pour ce faire, les pirates sont passés par le thermomètre connecté de l'aquarium, relié au réseau de l'établissement, usurpant ainsi 10 Go de données qui furent rapidement exfiltrer en direction de la Finlande [13].

Etant donné que le nombre d'appareils connectés ne cesse de croître, les constructeurs ont opté pour l'utilisation des technologies sans fil, qui facilitent ainsi l'installation et assurent une connectivité permanente. Malheureusement, la simple utilisation d'une antenne réceptrice permet la réception de toutes les ondes électromagnétiques qui nous entoure, d'où l'enjeu primordiale de sécuriser ces échanges.

Cette sécurité vise en priorité les couches *perception*, *network* et *application*, de l'architecture IoT :

Dans le cadre de la couche *perception*, la sécurité opère sur 3 sous-couches, dont chacune va traiter le format de donnée qui lui correspond :

- **La première, nommée multimédia**, qui utilise entre autres des techniques de compression multimédia, de cryptage, d'horodatage ou bien d'identifiant de session.
- **La seconde, intitulée image**, qui effectue la compression d'image et réalise les contrôles de redondance cyclique, afin de vérifier que les données n'ont pas été altérées.
- **La dernière, information textuelle**, dont les moyens reposent sur le cryptage, la compression, et l'anti-brouillage.

Pour la couche *network*, il existe également 2 sous-couches, selon si nous avons affaire à un réseau sans fil ou câblé. A ce niveau-là, ce sont les techniques de transfert de clé à travers des canaux sécurisés, d'authentification, et d'algorithmes de détection qui prévaut.

La couche *application*, va quant à elle garantir la sécurité de l'application grâce aux pare-feux, aux antivirus, ou par l'intermédiaire des autorisations accordées, etc…

Elle se divise également en 2 sous-couches, selon si l'application est utilisée à échelle locale ou internationale [14] :

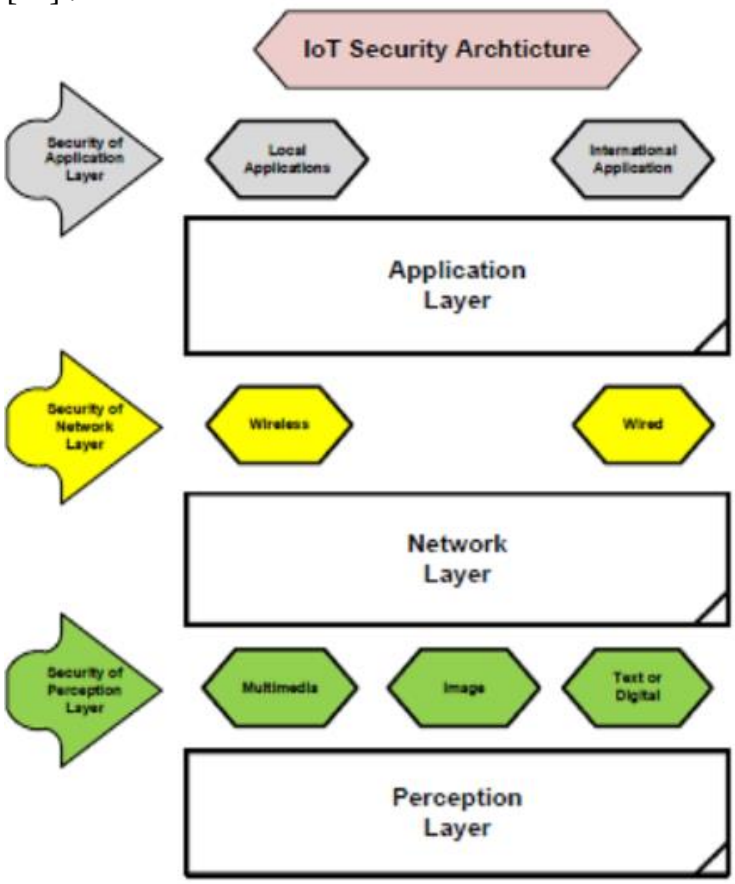


Figure 4 : Architecture IoT sécurisée (P. Ganapathi, M. Sujithra, 2016)

De la même façon, il faut pouvoir garantir l'anonymat de l'utilisateur, et la confidentialité de ses data. Aujourd'hui, des tas de données personnelles sont exploitées par les entreprises afin de nous fournir des services en fonction de nos goûts, il suffit de se pencher sur les publicités affichées sur notre navigateur pour en prendre conscience.

Cette confidentialité est très discutée dans l'IoT, car la moindre information peut potentiellement présenter un risque. La température interne d'un domicile, ou la mise en marche de la climatisation, par exemple, indique la présence de ses hôtes, ce qui peut être utilisé en vue de préparer un cambriolage.

De plus, étant donné que les systèmes IoT s'échangent des data, qu'arrive-t-il de nos données privées ? Car même si nous décidons de supprimer ces dernières de nos appareils, elles subsistent à travers les autres équipements.

2.3.3. Gestion du Big Data

La monté fulgurante de l'IoT, a entrainé une forte production de data, qui s'avèrent compliquées à gérer. Cette masse de données, dépasse largement les architectures de gestion traditionnelles, ce qui engendre un impact considérablement sur la capacité de calcul, et nous pousse à trouver de nouvelles solutions en termes de collecte, de gestion et d'exploitation [15].

Qui plus est, ces données sont d'une grande diversité, et majoritairement non-structurées, c'est-à-dire qu'elles sont contenues dans un format qui ne facilite guère leur compréhension, à l'instar d'une image, d'un fichier audio, ou d'un commentaire [16]. De la même manière, il existe également des données dites semi-structurées, dont la structure diffère du modèle établi par les bases de données relationnelles (MySQL, MariaDB, ORACLE…), mais qui, par l'intermédiaire de balises ou de marqueurs, permet la récupération d'informations significatives. C'est nouveaux formats basés sur un structure irrégulière, voire inexistante, sont néanmoins bénéfiques pour l'IoT, puisqu'ils nous donnent la possibilité de remédier à l'hétérogénéité des data, issues de BDD variées.

La définition du Big Data ne se limite pas qu'à cette imposante masse de données, c'est aussi un concept caractérisé par 3 axes principaux appelé « règle des 3V » : Volume, Vélocité et Variété [17] [18] :

Le Volume, comme son nom l'indique, évalue la quantité de données, qui se mesure en téra (10^{12}) voir pétaoctets (10^{15}) en provenance de grands groupes tel que Twitter ou Facebook [19], pour une part mondiale s'élevant à environ 64,5 zettaoctets (10^{21}) d'ici 2021 ; selon les statistiques de la plateforme Statista [20]. Comme l'explique Zeel Doshi, Rashi Agrawal, Pratik Kanani, ingénieurs informatiques, et Mamta C. Padole, titulaire d'un doctorat en informatique et ingénierie, dans leur étude intitulée « *Big Data, Big Challenges* », les base de données traditionnelles deviennent inefficace face à des data qui se chiffrent en pétaoctets ; ce qui engendre des coûts très élevés pour les entreprises cherchant à mettre à jour leur infrastructure de stockage.

En soit, ce volume soulève beaucoup de contraintes, comme la durée de cryptage, la surveillance, ou bien le filtrage des data, qui s'avère complexe face à cet océan de données.

La Vélocité, traite de la vitesse à laquelle Les informations sont produite, et l'enjeu que représente une étude en temps réel. Aujourd'hui, les systèmes IoT délivrent un nombre incalculable de données à grande vitesse, ce qui pousse les entreprises à développer de nouveaux systèmes de traitement.

Il existe des programmes dédiés à l'analyse et au stockage du Big Data, comme l'application open source Hadoop ou le framework de traitement de flux Apache Storm, mais chacun présente des inconvénients, qui hissent ces technologies en dessous de nos espérances.

Hadoop par exemple, découpe la masse de données en plusieurs « nœuds » de taille identique, et les traite parallèlement, en un minimum de temps, avant de les stocker [21].

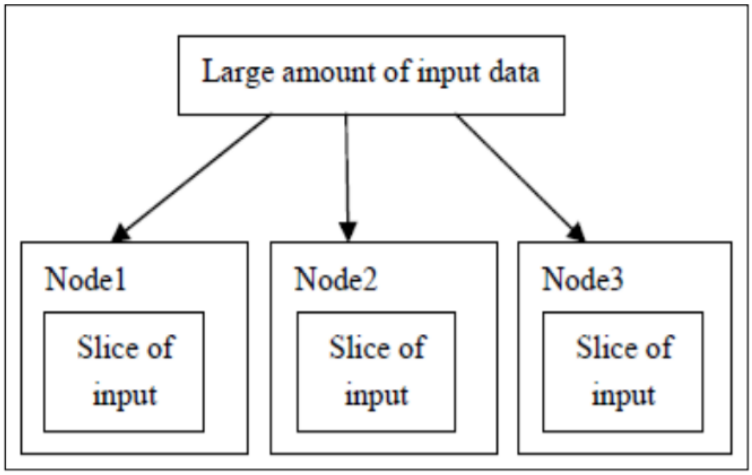


Figure 6 : Les données distribuées par les nœuds Hadoop (2020) [21]

A l'opposé, Apache Storm est capable de directement analyser, et transformer le flux de données, en très peu de temps (de l'ordre du million de tuple* traité par seconde [22]), mais ne peut fournir des solutions de stockage [17] [23]. Il faut donc le rattacher à une BDD, mais encore faut-il que cette dernière, soit capable de gérer la vitesse d'arrivée des data.

La Variété, car comme nous l'avons vu précédemment, il existe une variété de données qui rendent l'étude délicate. A l'échelle d'une entreprise, cela se caractérise par des informations du même type, mais dont le format diffère ; exemple avec une image .jpeg qui peut tout aussi bien être en .png ou en .gif.

Vient s'ajouter à ça la dimension qui consiste à séparer les informations pertinentes, de celles qui ne le sont pas ; compte tenu des nouvelles structures de données [17].

Deux autres éléments sont venus compléter les piliers du Big Data, transformant ainsi la règle des 3V, en 5V :

Nous retrouvons **la Véracité**, qui a pour but de créer un lien de confiance entre la personne en charge de l'analyse, et les data. Effectivement, si la fiabilité des données n'est pas au rendez-vous, elle ne sera pas capable de porter un jugement, et ne saura les exploiter convenablement. Etant donné que la majorité des informations recueillies sont utilisées en vue de prendre des décisions, il faut impérativement s'assurer de leur conformité.

L'un des aspects les plus importants du Big Data, est de transformer cette « infobésité » en valeur ajoutée ; c'est ce que traduit le dernier V : **Valeur**. La plupart du temps, les data analysées ne présentent que très peu de valeur, comparé à leur volume d'origine, d'où l'intérêt de rentabiliser les investissements afin d'augmenter les recettes [24].

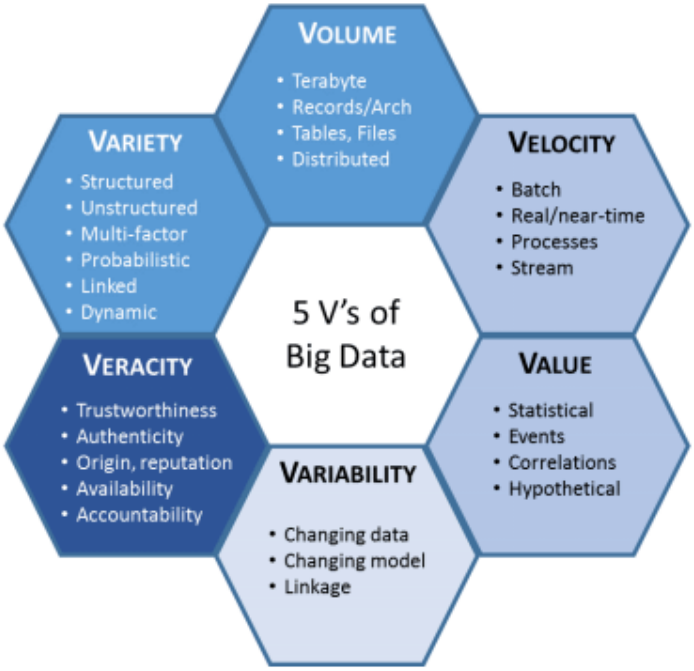


Figure 7 : Caractéristiques des 5V du Big Data (B. Shaqiri, 2017)

2.3.4. L'enjeu énergétique :

L'IoT connecte des milliards de dispositifs à travers le monde, ce qui entraîne une forte croissance des demandes en énergie. Dans une optique de développement durable, les constructeurs cherchent à diminuer la consommation de leurs produits, afin d'offrir des technologies plus respectueuses de l'environnement. En effet, certains appareils consomment plus d'énergie que nécessaire, engendrant ainsi un impact environnemental plus élevé, et des frais inutiles ; d'où l'intérêt de limiter ce gaspillage.

Cette nouvelle vision est qualifiée de « Green IoT », et cherche à s'appliquer à tous les domaines de l'Internet des Objets, en utilisant des techniques à haut rendement énergétique. Ces améliorations touchent aussi bien les hardwares que les logiciels, en passant par les technologies de communication et de cloud. Dans le cadre des réseaux sans fil par exemple, elle consiste à optimiser les techniques de radiodiffusion, de routage, et à implémenter des algorithmes intelligents, dans le but de réduire la taille des données, et les besoins en capacité de stockage [26]. A l'instar des objets contenus dans les réseaux LPWAN (Low Power Wide Area Network), qui se réveillent uniquement pour transmettre quelques Kbits de données, ce qui réduit considérablement la consommation énergétique comparait aux réseaux mobile 3G, 4G [27].

Les capteurs demandent également une étude approfondie, car comme l'explique R. Ahmed, professeur assistant au département d'informatique et d'ingénierie de KNIT à Sultanpur, bien qu'ils n'aient besoin que de très peu d'énergie pour fonctionner, cela représente une très grosse part à l'échelle de plusieurs milliards [28]. Il faut donc choisir chaque composant avec soin, afin de limiter les besoins en énergie au strict minimum.

Les technologies vertes de l'IoT n'en sont qu'à leur début, mais leur cause est noble, car elles mettent l'accent sur une diminution intelligente de l'empreinte carbone, à une époque où la pollution numérique se veut de plus en plus conséquente [29]. Avec l'arrivée imminente de la 5G, son enjeu est d'autant plus crucial, car beaucoup se questionnent sur l'impact de cette nouvelle technologie. En effet, suite au cinquième sommet mondial sur l'efficacité des TIC* qui s'est déroulé à Amsterdam en septembre 2019, un rapport officiel intitulé « 5G Telecom Power Target Network » a été partagé par Huawei. Dans ce dernier, on apprend qu'un appareil fonctionnant sur une bande 5G, consommerait 300 à 350 % plus d'électricité qu'un équipement 4G, pour une même configuration [30].

Au contraire, certains affirment que la 5G serait susceptible de réduire la consommation d'énergie, notamment grâce à des modes veilles avancés [31] ; il faut donc étudier en profondeur la question, afin de vérifier son aspect écoresponsable.

3. Au cœur du secteur automobile

3.1. La quatrième révolution industrielle :

Le monde a connu 3 révolutions industrielles aux cours des derniers siècles, qui ont chacune provoquées de grands bouleversements sur les plans économiques et social. L'apparition de la machine à vapeur, a permis de développer le transport maritime et ferroviaire, donnant ainsi naissance à de nouvelles opportunités commerciales. Les chaînes de productions nous ont offert le moyen d'augmenter notre productivité, tandis que l'automatisation des machines, a rendu la tâche des travailleurs moins contraignante [32]

Internet a complétement bouleversé nos vies, en changeant nos moyens de communication et de consommation. C'est dotant plus le cas avec l'émergence de l'Internet des Objets, qui par son caractère intelligent et autonome, attire l'œil des industriels, qui optent de plus en plus pour des solutions connectées. Ce changement est d'une telle ampleur, que l'on parle d'une quatrième révolution industrielle.

3.1.1. Définition et concept :

Le concept d'industrie 4.0 (ou smart factory), fut introduit pour la première fois en 2011, lors de la Foire de Hanovre, en Allemagne, dont le thème était porté sur les solutions d'automatisations industrielle [33]. Selon l'Institut technologique de maintenance industrielle situé au Québec, cette nouvelle révolution a pour objectif de donner aux humains, machines et produits, la possibilité de communiquer entre eux, tout en étant connecté [34]. L'usine 4.0 ne se limite pas qu'à l'utilisation des nouvelles technologies, mais évalue également leurs impacts sur la société, notamment la collaboration Homme-machine, qui implique de devoir former les travailleurs à de nouveaux moyens de production. De la même façon, elle cherche à résoudre les problèmes liés à l'automatisation, qui remplace de plus en plus les salariés au sein de l'industrie [35].

De ce fait, son but n'est pas de remplacer l'Homme, mais plutôt de l'aider dans ses travaux, en mettant à sa disposition des processus beaucoup plus rapide, qui échangent des informations en temps réel et sans difficultés [36]. Le cycle de fabrication est également modifié, en s'orientant désormais vers une production à faible volume, de produits uniques et personnalisables. En effet, les clients pourront, grâce à l'IoT, communiquer avec les machines lors de la phase de réalisation, ce qui permettra de leur proposer de nouveaux services ; c'est le concept de la « smart production ». Malgré la diminution de son volume de production, la

« smart factory » devrait accroître sa productivité, en réduisant de 50 % le temps entre la conception d'un nouveau produit, et sa livraison [37]. L'usine intelligente répond parfaitement aux besoins des constructeurs automobiles et de leurs sous-traitants, car elle permet le suivi des données de productions, tout au long de la chaîne de valeur [38].

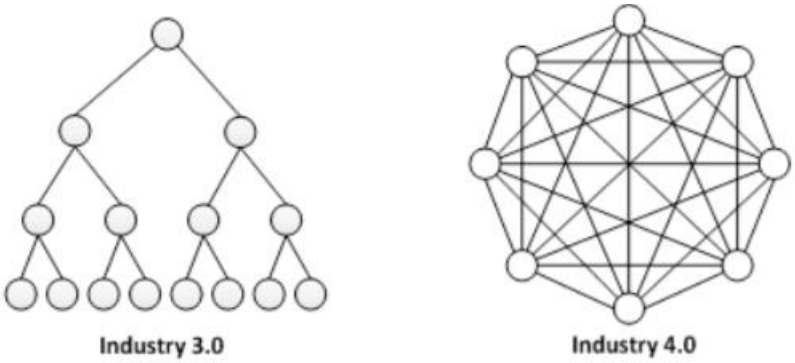


Figure 8 : Les flux d'information au sein de l'industrie 3.0 vs 4.0 (2016) [37]

Les facteurs clés de cette « smart production », sont la mise en réseau horizontale et verticale, qui change complètement l'organisation au sein de l'entreprise. Sur le plan horizontal, nous retrouvons tous les systèmes connectés entre eux, comme les unités de production, les systèmes de stockage et les appareils IoT ; mais également les communications externes à l'entreprise, comme les relations partenariales. Son rôle est de rendre la coopération harmonieuse entre les différentes machines et processus [39].

L'intégration verticale, quant-à-elle, vise à dépasser les barrières de la hiérarchie, en garantissant l'utilisation des données de production, à un niveau supérieur. Les data pourront donc être directement transmises vers le système ERP* ou le cloud, en vue de prendre des décisions relatives au personnel, au marketing ou autres. Lier ces deux paradigmes, permettra de rendre l'usine beaucoup plus intelligente et flexible, au profit des fabricants.

3.1.2. IoT et production industrielle :

L'usine de demain, repose sur l'utilisation des technologies numériques (IoT, Big Data, cloud…) et des systèmes cyber-physique (SCP). Ces derniers résultent de la fusion des processus industriels, avec les technologies de communication modernes basées sur Internet. Ils caractérisent tous les appareils intelligents qui sont capable, en toute autonomie, d'échanger des informations, de déclencher des actions, et de se contrôler mutuellement [35]. Leur utilisation engendre l'optimisation et l'amélioration de la production, principalement grâce à

leurs capteurs IoT, qui collectent une grande quantité de données, en vue d'analyser les erreurs ; mais aussi de prévoir les comportements futurs, afin d'agir en conséquence [40]. Ces data peuvent, effectivement, nous renseigner sur l'état des machines, ce qui permet de planifier une potentielle maintenance. Les SCP sont étroitement liés à l'Internet des Objets, qui leur confère une connexion Internet permanente, par laquelle, les données relevées, vont être acheminées, en direction des différents services.

De plus, les industriels utilisent également les puces RFID*, afin de localiser et identifier les pièces, tout au long de la chaîne de production. Dans l'industrie automobile, cette technologie est notamment employée pour faire le lien entre une carrosserie et son client [41]. Avec l'émergence des transports intelligents, et plus particulièrement de la voiture connectée, ce secteur est d'autant plus concerné par l'IDO.

L'avancée majeur de la technologie, a permis aux industriels d'opter pour de nouvelles solutions comme l'intelligence artificielle, la réalité augmentée et l'impression 3D. Voici une vue d'ensemble de toutes les technologies employées dans l'industrie 4.0.

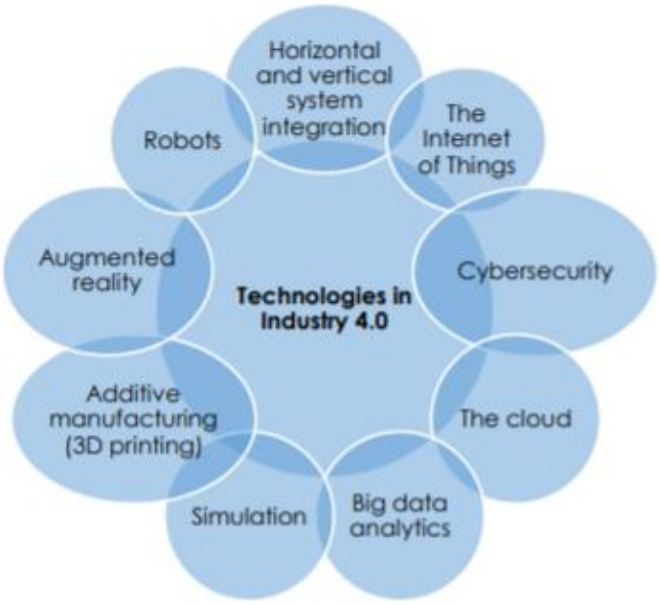


Figure 9 : Les technologies relatives à l'industrie 4.0 (2016) [42]

3.1.3. Qu'en est-il de la main d'œuvre ?

Comme nous l'avons évoqué auparavant, l'automatisation industrielle rattachée à l'IoT, va entrainer une diminution fulgurante de la main d'œuvre, ce qui va directement toucher les travailleurs. Bien que la montée en force des nouvelles technologies puisse paraître effrayante, leur rôle est avant tout d'aider le salarié et non de le supplanter. L'utilisation de la réalité

augmentée par exemple, va permettre au technicien d'accéder à l'information plus rapidement, tandis que les robots collaboratifs, l'accompagnent en exécutant des manipulations difficiles. Il est cependant vrai que les emplois non qualifiés, dans lesquels les ouvriers exécutent des tâches simples et souvent répétitives, risque d'être substitués par des robots, au cours des 10/20 prochaines années [43]. En effet, les robots peuvent effectuer plusieurs fois la même tâche avec une rapidité, et une précision, supérieures à celle d'un Homme, ce qui engendrera l'accroissement de la production.

Toutefois, cette évolution n'est pas entièrement négative, car elle entrainera une réduction des charges du travail manuel, ce qui permettra de transférer les travailleurs vers des tâches plus satisfaisantes avec à la clé, des emplois plus qualifiés et mieux rémunérés [43]. Dans la même optique, le professeur Juergen Maier, commissionné par le ministère britannique des affaires, de l'énergie, et de la stratégie industrielle, nous annonce une croissance de l'industrie manufacturière estimée entre 1,5 et 3 % par an, ce qui conduirait à une augmentation nette de 175 000 emplois, et une diminution des émissions CO_2 de 4,5 %, au fil de la future décennie [44].

Cette ère de la digitalisation, va marquer une transition avec les méthodes d'apprentissage traditionnelles en utilisant les derniers outils de formation adoptés par les organisations. Les employés devront acquérir de nouvelles compétences, mais également recevoir une orientation spécifique, afin de s'assurer qu'ils sachent en quoi consiste leur travail et comment le réaliser. La nécessité d'améliorer les acquis des salariés est primordiale, car l'organisation au sein d'une entreprise est toujours très dynamique, ce qui est d'autant plus le cas avec l'usine intelligente qui utilise un large panel de technologies [45]. L'Allemagne, pionnier en la matière, a notamment ouvert à travers tout le pays, des centres de formation et d'éducation dédiés à l'industrie 4.0, qui couvrent aussi bien la scolarité des moins de 18 ans, que celle des étudiants en étude supérieur. Ces derniers proposent des formations professionnelles, qui permettent de rentrer plus rapidement dans le vif du sujet, afin que les élèves puissent appréhender la complexité d'une usine du futur [46].

Le débat de l'impact industrielle 4.0 sur l'avenir du travail continu à faire parler de lui, car il est difficile de prévoir avec précision les changements que cela va apporter, mais nous savons que les emplois existants, pourraient très bien être remplacés par des nouveaux. Face à ces changements, les travailleurs devront se tenir au goût du jour, en acquérant de nouvelles

compétences, qui leurs permettront d'obtenir une compréhension globale du fonctionnement, et de l'organisation, au cœur de l'industrie intelligente.

3.2. L'émergence des véhicules connectés :

L'Internet des Objets s'est développé avec une telle rapidité, que son utilisation devient une nécessité presque fondamentale dans notre quotidien. Ses technologies peuvent se retrouver dans tous les domaines, tels que la santé, l'agriculture, et le bâtiment intelligent. Dans le secteur automobile notamment, les constructeurs voient en l'IoT, une possibilité d'améliorer le confort, et la sécurité à bord d'un véhicule, ce qui conduit à la conception de nouveaux transports dit intelligents. Ces transports intelligent ont pris une telle ampleur aux cours des dernières années, qu'on estime, en France, le nombre de véhicule connecté en circulation, à 12,8 millions pour 2022, contre 3,1 en 2017 [47].

3.2.1. Principe :

Un véhicule connecté, est un transport muni d'une connexion Internet, qui utilise des capteurs embarqués, afin d'améliorer l'expérience des utilisateurs, et la qualité de vie à bord. Ils peuvent, par exemple, renseigner les personnes sur la température du liquide de refroidissement, la pression des pneus, ou bien l'état du moteur, et contrôler ces éléments sans intervention humaine, par l'intermédiaire d'actionneurs [48].

La connectivité Internet, offre la possibilité au conducteur d'obtenir des données de navigation, et de gérer le contenu de divertissement audio/visuel, aussi bien à l'avant qu'à l'arrière. Les constructeurs privilégient l'utilisation des commandes vocales, ce qui permet de garder les yeux sur la route, et les mains sur le volant. La connexion assure également la communication entre les véhicules (V2V), mais aussi avec l'infrastructure du réseau routier (V2I), comme les feux tricolores [49].

Les constructeurs, concessionnaires et fournisseurs automobiles, misent beaucoup sur l'IDO, car ils y voient une manière de fluidifier le trafic, et de suivre l'état d'usure des véhicules, afin d'en informer leurs clients. Les voitures de chez Tesla en sont un très bon exemple, car elles présentent à elles seules, un gros dispositif IoT avec de nombreuses propriétés connectées intégrées.

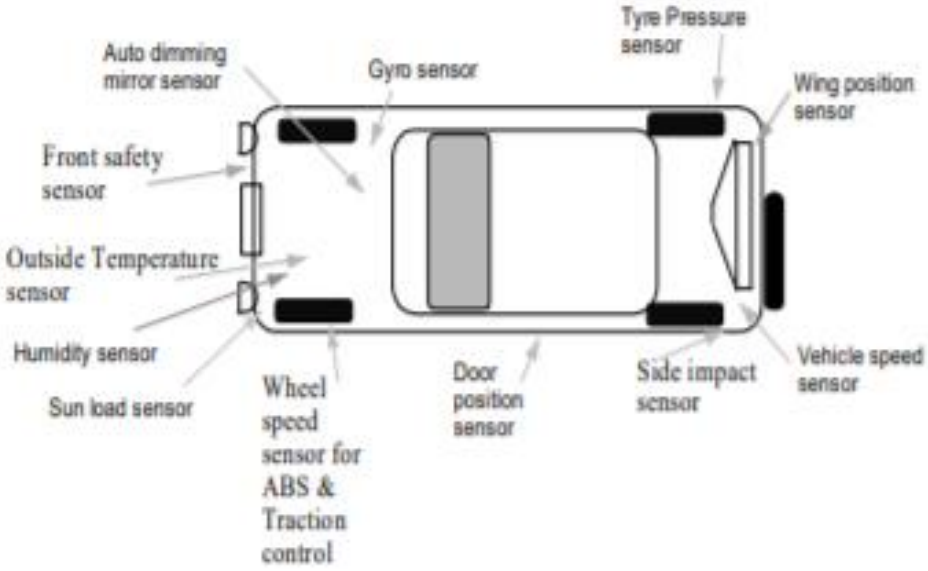


Figure 10 : Les différents capteurs utilisés dans la voiture connectée (2017) [48]

3.2.2. Pour répondre à quels besoins ?

Adopter ces nouveaux transports intelligents, rendra notre quotidien beaucoup plus rapide et plus sûr, en répondant à plusieurs besoins spécifiques, comme par exemple la diminution du nombre d'embouteillages et d'accidents de la route. En effet, grâce à la communication inter-véhicule, le conducteur sera à même de choisir le meilleur itinéraire, ce qui le fera arriver plus rapidement à destination. Appliquer cet échange d'informations à l'ensemble du trafic, permettra une répartition de la circulation plus pragmatique, entrainant ainsi une réduction considérable du nombre d'accident et de mort sur la route. Le fait d'éviter les embouteillages, et de renseigner le conducteur sur les places de parking les plus proches, par exemple, devrait également réduire la consommation de carburant, ce qui l'aidera à faire des économies tout en limitant son impact sur l'environnement.

Les données en temps réel sur le moteur, le système de lubrification ou de transmission, seront utilisées pour prévenir les pannes, ce qui informera les utilisateurs sur l'état général de leur véhicule. Si une panne survient malgré ce suivi, le conducteur sera toujours à temps d'utiliser les informations de son tableau de bord pour localiser les stations-service et garage près de sa position. De la même façon, lors d'un accident, le système d'urgence se déclenchera en envoyant des data en direction des secours, ce qui accélérera la prise en charge.

Opter pour les technologies de l'IoT embarquées, rendra donc la conduite moins contraignante, et transformera considérablement l'expérience du conducteur et de ses passagers.

3.2.3. Architecture :

La connexion Internet d'une voiture connectée repose soit sur l'utilisation du smartphone de l'utilisateur, soit sur un modem appelé « unité de commande télématique (TCU) » qui se compose entre autres d'un microcontrôleur, d'un GPS, et d'une interface externe dédiée à la radiocommunication (GSM, LTE, Wi-Fi).

Il existe plusieurs manières de connecter une voiture, et chacune de ces solutions optent pour différentes formes de technologies associées, ce qui impacte directement l'architecture de communication ; il en existe 5 :

- **Car-to-Network** : dans ce cas de figure, le véhicule est simplement connecté aux réseaux cellulaires type 2G, 3G, 4G.
- **Car-to-TSP :** ici, la communication se fait par le biais d'un véhicule fournisseur de services télématiques. L'utilisateur se connecte à ce point d'accès qui en retour, partage ses données avec lui.
- **Car-to-Cloud :** comme son nom l'indique, cette connexion repose sur l'utilisation d'un cloud. Le véhicule s'y rattache grâce au réseau, afin d'y récupérer les data stockées.
- **Car-to-Car :** communication inter-véhicule sans-fil à courte distance (V2V), comme nous l'avons vu précédemment et que nous développerons par la suite.
- **Car-to-Infrastructure :** en utilisant cette connexion, le conducteur se relie à son environnement, et procède à des échanges d'informations avec les éléments qui y sont reliés (feux tricolores, limitation de vitesse, etc…) [50].

En ce qui concerne l'architecture du véhicule, nous y retrouvons plusieurs sous-réseaux qui collaborent les uns avec les autres directement, ou indirectement, par l'intermédiaire d'une unité de commande électronique (UCE) spéciale appelée « passerelle UCE ». Cette passerelle diffère des UCE classiques, qui de leur côté, contrôlent les dispositifs physiques intégrés dans la carrosserie. Qualifiés de calculateurs embarqués, ils peuvent notamment se renseigner sur l'état général du véhicule grâce aux différents capteurs, ou bien commander les actionneurs, afin d'agir sur le moteur ou les pneus par exemple. Ils ont également en charge la sécurité, en détectant et en mémorisant les potentiels défauts des capteurs et actionneurs. De nos jours, les transports connectés se composent en général de 50 à 100 UCE, ce qui permet de couvrir la totalité des dispositifs.

De ce fait, les véhicules connectés peuvent être assimilés à des véhicules embarqués, ou à une plateforme multicouche, équipée d'une passerelle, reliant les sous-réseaux du véhicule, au réseau externe [51]. L'intérêt que présente la combinaison des différents réseaux sans fil, est de fournir aux équipements la connectivité qui répond le mieux à leurs exigences. Effectivement, nous pouvons citer les systèmes dédiés à l'info-divertissement, qui par leur aspect informatif, nécessitent une plus grande bande passante que certains dispositifs, qui bénéficient d'une tolérance au panne réseau plus indulgente.

La communication intra-véhiculaire sans fil (IVWSN), cherche à fournir des performances semblables aux technologies filaires utilisés pour la transmission en temps réel, en fournissant une gigue*, un débit, et une fiabilité similaire. En diminuant le nombre de câble, nous pourrons, par la même occasion, réaliser des économies, car le véhicule sera moins lourd et consommera donc moins de carburant [52].

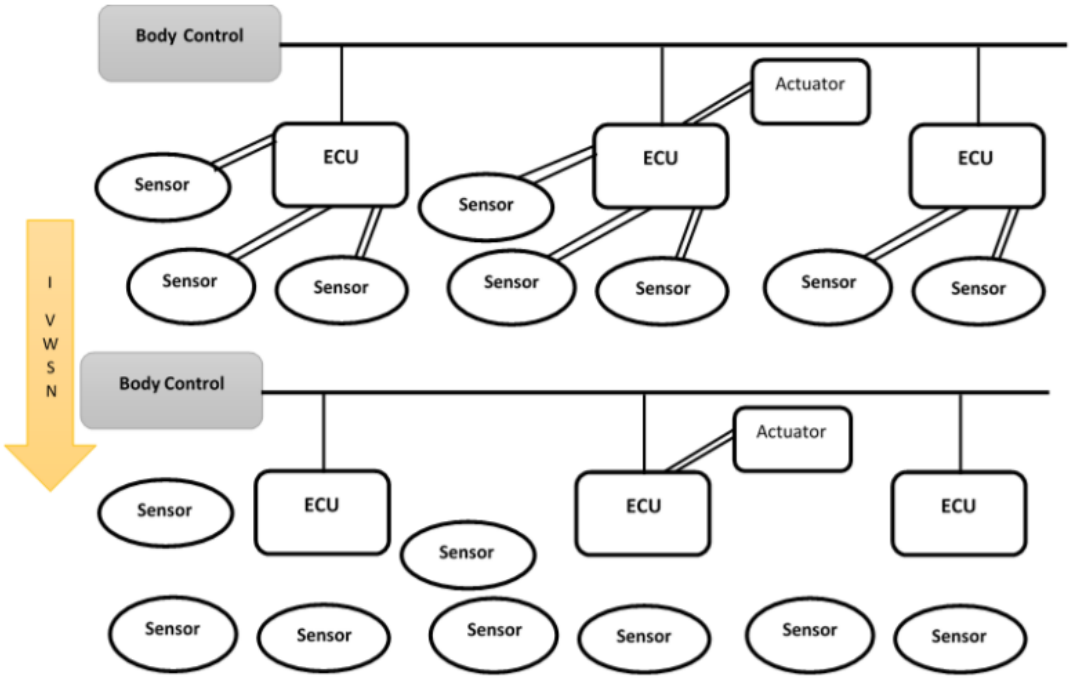


Figure 11 : Réseaux de capteurs sans fil intravéhiculaire (IVWSN) (2018) [51]

Bien que le souhait des spécialistes soit de limiter l'utilisation des technologies filaires, ces dernières sont toujours employées. Afin de remédier à l'augmentation du nombre de câbles, le concept de « bus de terrain » a été implémenté. Un bus de terrain, n'est autre qu'un bus série permettant de relier les UCE aux éléments du véhicule connecté (vitre, freins, moteur, etc…), ce qui soulage l'architecture réseau en réduisant le nombre de fils, et par la même occasion, le coût du système automobile.

A ses débuts, les constructeurs automobiles concevaient leurs propres technologies de bus de terrain, ce qui compliqua la tâche des sous-traitants qui se retrouvaient face à des vendeurs automobiles, aux attentes différentes. Afin de faciliter les échanges, le bus de série CAN (Controller Area Network) fut normalisé au début des années 90, et devint ainsi, la technologie la plus employée dans le secteur de l'industrie automobile.

Toutefois, utiliser un CAN pour des tâches aussi simples que le démarrage du véhicule ou le contrôle des fenêtres électriques, s'avéra bien trop coûteux et compliqué ; ce qui incita les constructeurs à opter pour des protocoles plus simples, offrant des fonctionnalités similaires à moindre coût. C'est notamment le cas pour le bus LIN (Local Interconnect Network), qui peut être implémenter en tant que sous-réseau du CAN, afin de gérer les capteurs et actionneurs rattachés aux vitres, au toit ouvrant, ou aux sièges. Nous retrouvons également le système de transmission de données MOST (Media Oriented Systems Transport) qui par son débit de transmission plus élevé, résout les problèmes de latence du CAN, pouvant survenir avec les applications multimédia à forte bande passante (kit mains-libres, lecteur DVD, etc…).

Les fonctions de base du véhicule, comme le système de freinage ou le contrôle de la direction, sont assurées par le bus FlexRay. Grâce à un cycle de communication composé de deux segments temporels (statique et dynamique), la technologie FlexRay permet de prioriser les messages en fonction de leur niveau d'alerte. En effet, la portion statique s'occupe des messages critiques (de l'UCE aux freins par exemple), tandis que la portion dynamique se charge des messages moins importants [51] [53] [54].

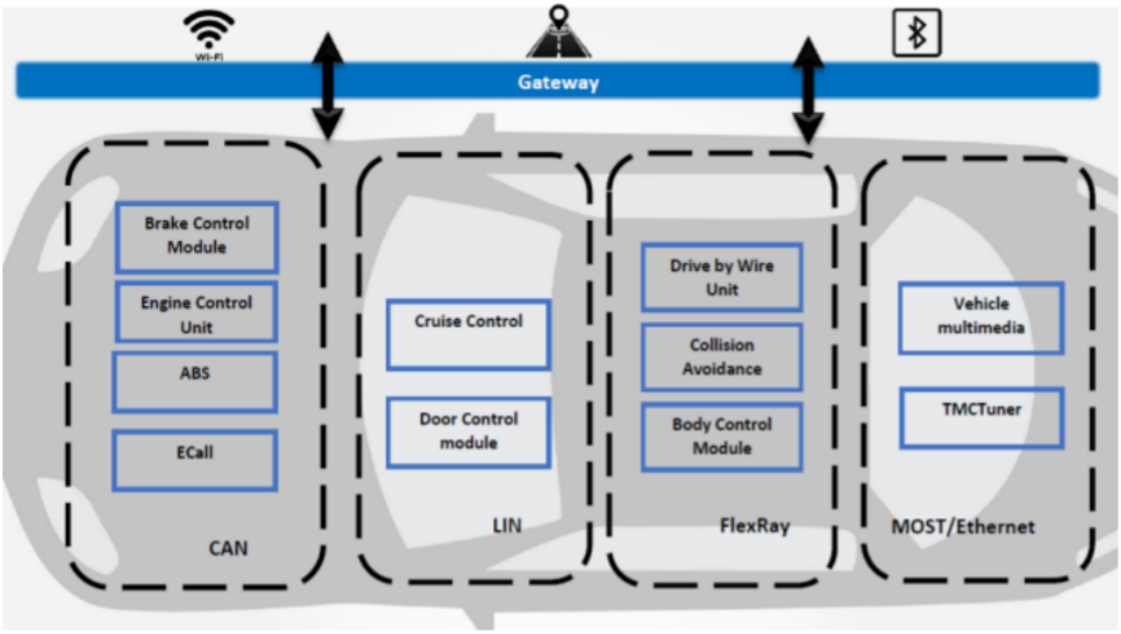


Figure 12 : Architecture de la voiture connectée (2018) [51]

3.3. De nouveaux moyens de communication :

Avec le souhait d'améliorer la sécurité routière, la fluidité du trafic, et les systèmes d'info-divertissements, les constructeurs automobiles ont décidé de miser sur un tout nouveau système de communication intitulé V2X (Vehicle-to-Everything). Comme son nom l'indique, cette technologie vise à initier une communication entre le véhicule et son environnement, afin de dynamiser la circulation, tout en réduisant la consommation de carburant.

En effet, selon l'étude mené par Amrita Ghosal et Mauro Conti intitulé « Security Issues and Challenges in V2X: A Survey », les embouteillages en 2014, représentaient rien qu'aux États-Unis, environ 6,9 milliards d'heures perdues pour une consommation atteignant les 3,1 milliards de galon. Ces deux facteurs entrainèrent une perte financière annuelle à hauteur de 160 milliards de dollars, d'où la nécessité de trouver une solution.

3.2.1. Du véhicule au piéton :

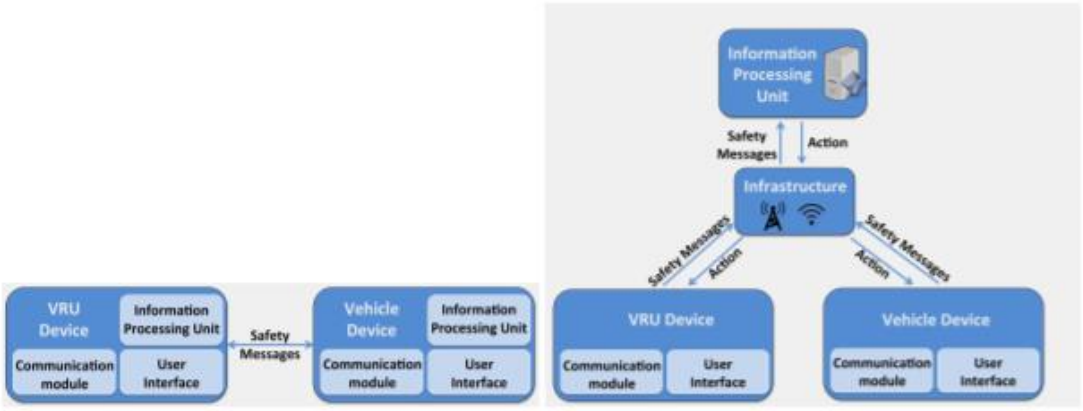
L'objectif de la communication V2P (Vehicule-to-Pedestrian), est d'instaurer un échange d'informations entre les véhicules connectés, et les usagers vulnérables de la route (UVR), qui regroupent les piétons, les cyclistes ainsi que les deux-roues. En effet, bien que le taux de mortalité routière en 2019 soit 0,3 % plus bas qu'en 2018, les UVR représentent toujours une part importante, notamment dû à une hausse du nombre de décès chez les cyclistes.

Effectivement, d'après l'estimation provisoire réalisée par l'Observatoire national interministériel de la sécurité routière (ONISR), environs 3 239 personnes auraient perdu la vie sur les routes de France en 2019. Le nombre d'usagers vulnérables de la route décédés, s'élève à 1 403 personnes, ce qui représente tout de même 43 % des accidents mortels en 2019, d'où la nécessité d'améliorer la sécurité des conducteurs et des UVR [55] [56]

Les UVR, comme l'explique J. Sewalkar et J. Seitz, enseignants à l'Université Technologique d'Ilmeneau, en Allemagne, diffèrent les uns des autres selon plusieurs critères : la mobilité, la vitesse, et les modes de déplacement. Les cyclistes et les deux-roues, par exemple, se déplacent beaucoup plus rapidement qu'un piéton, mais lorsque ces derniers traversent au passage piétons, les deux autres sont arrêtés au feu rouge, il faut donc faire preuve de pragmatisme en prenant en compte tous ces paramètres.

Pour fonctionner, les véhicules et les UVR doivent s'échanger, périodiquement, des messages sur leur environnement, et fusionner ces informations avec les données récoltées par les capteurs (vitesse, direction, position…). Cette communication peut s'initier directement

entre les nœuds voisins (réseau ad hoc), ou au travers d'une infrastructure de communication dédiée.



Communication V2P directe Communication V2P indirecte

Figure 13 : Exemple d'architecture de communication V2P (2019) [55]

La technologie V2P repose sur trois phases : la détection, le suivi, et la prédiction de trajectoire. Toutes ces étapes sont effectuées par une unité de traitement de l'information, qui dès la fin de l'analyse, avertie le dispositif du véhicule et de l'UVR, sur les risques potentiels d'accident de la route. Voici comment s'exerce la communication V2P en fonction du type d'UVR rencontré :

- **Piéton** : exploite les capteurs du smartphone afin d'obtenir les informations nécessaires, puis utilise une connexion Wi-Fi direct, ou indirect, afin de transmettre les données. La vitesse de marche, permet notamment de pouvoir classer la personne :
    1. **Enfant** : marche lente et trajectoire imprévisible
    2. **Adulte** : caractéristiques typiques (vitesse d'environs 1,4 $m.s^{-1}$)
    3. **Personne âgée** : marche lente pouvant être assistée (canne, fauteuil roulant, chien, etc…)
- **Cycliste** : à la manière du piéton, la technologie V2P utilise le smartphone du cycliste (vitesse habituelle environnant les 4,2 $m.s^{-1}$). Connexion Wi-Fi ou Bluetooth.
- **Deux-roues :** l'échange de données peut s'effectuer grâce au smartphone du conducteur, ou par le biais du système équipant le véhicule. Communication unidirectionnelle (du deux-roues vers les véhicules voisins uniquement), vitesse avoisinant les 50 km/h

Voici quelques cas de figure qui mettent en avant l'aspect prévisionnel du V2P :

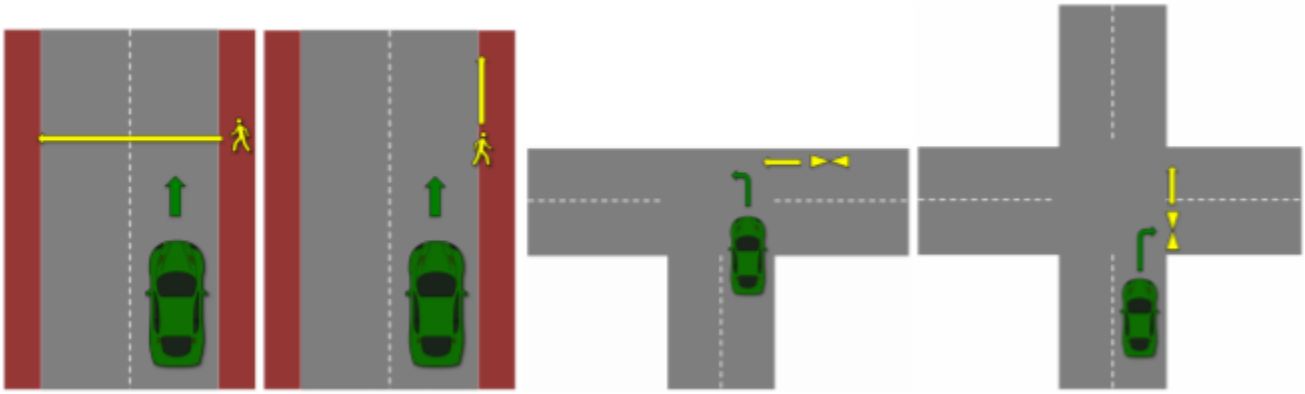


Figure 14 : Divers scénarios qui précèdent l'accident (2019) [55]

3.2.2. Entre véhicule :

Comme nous l'avons vu précédemment, l'intérêt que présente la communication entre les véhicules (V2V), est de pouvoir obtenir des informations en temps réel sur le trafic environnant, afin de diminuer le nombre embouteillages, et d'accidents de la route. Les véhicules pourront se localiser mutuellement (à un quart de km), que vous soyez à l'arrêt où dans un angle mort, et être averti du moindre changement de trajectoire, afin d'anticiper le comportement des conducteurs. Au vu de la circulation qui l'entoure, la communication V2V pourra entre autres, conseiller une vitesse facilitant l'insertion, ou bien détecter les arrêts d'urgence et les véhicules en contresens [57]

L'échange s'effectue majoritaire en point à point (réseau véhiculaire ad hoc ou VANET), mais peut également s'effectuer par l'intermédiaire d'une infrastructure de communication (V2I). Dans le premier cas de figure, les véhicules se connectent les uns aux autres en GSM, ou Wi-Fi (norme 802.11p), afin de former un réseau de nœuds communiquant. Très flexible, cette architecture continuera de fonctionner, même si certains nœuds tombent en panne (à condition d'en avoir en nombre suffisant). Afin d'éviter la redondance des messages, l'information sera simplement rediffusée ; un temps de vie (TTL) pourra éventuellement être utilisé afin de limiter la zone de distribution du paquet.

Les architectures V2V et V2I sont étroitement liées, car elles partagent un même objectif : optimiser le trafic routier. Elles devront donc collaborer afin d'assurer la continuité des services aux conducteurs [58].

3.2.3. Du véhicule à l'infrastructure :

La communication V2I (Vehicle-to-Infrastructure), consiste à partager des informations entre les véhicules connectés, et les éléments qui soutiennent le réseau routier du pays. Dans le cadre de la Smart City par exemple, ces éléments peuvent être des caméras RFID, des feux de circulation ou bien des panneaux de signalisation. Son objectif est de fournir aux conducteurs des données en temps réel sur : la disponibilité des parkings, les embouteillages, les accidents et même l'état des routes. Les data issues des capteurs embarqués du véhicule passent à leur tour être utilisées par l'infrastructure afin de fixer des limitations de vitesse variables, et synchroniser les feux tricolores.

A l'instar du V2V, V2I utilise pour le transfert des données un canal de fréquences dédiées aux communications à courte portée (DSRC). L'accès à l'infrastructure se fait par l'intermédiaire d'un équipement appelé unité de bord de route (UBR), que nous retrouvons installés à intervalle régulier, au cœur de la ville intelligente. Lorsqu'un véhicule munit d'une unité embarquée (OBU) arrive à proximité d'une UBR, un échange d'information se crée, et les messages affichés sur les panneaux statiques, sont relayés en direction de l'interface du conducteur. Les OBU (On-Board Unit) assurent aussi bien la communication avec l'UBR, qu'avec les autres véhicules (dans le cadre du V2V). Ces dernières peuvent notamment transmettre régulièrement des messages d'état en direction des OBU voisines, mais également stocker des instantanés de données, qui seront par la suite relayés à l'UBR. Les données les plus anciennes, seront ensuite écrasées par les nouvelles [57] [59].

Toutefois, l'utilisation du V2X présentent toujours de nombreux défis aux constructeurs automobiles, comme l'interopérabilité entre les différentes technologies embarquées, la fiabilité, la précision des données, ainsi que la conformité à échelle mondiale

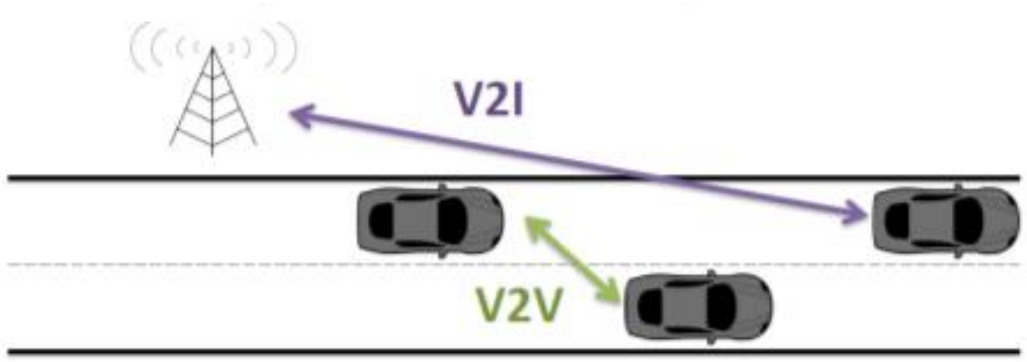


Figure 15 : Echange d'information dans une architecture V2V/V2I (2018) [57]

3.4. Les enjeux :

3.3.1. Assurer la sécurité du conducteur :

L'un des principaux challenges qui revient dès lors que nous parlons d'IoT, est la sécurité. C'est d'autant plus le cas avec l'émergence des véhicules connectés, dont le nombre devrait s'élever à hauteur de 775 millions en 2023, contre 330 millions en 2018, selon l'étude menée par Juniper Research [60]. Son développement est si rapide, qu'il est urgent de mettre en œuvre des solutions permettant d'assurer la sécurité physique des passagers, et de leur environnement.

Pour communiquer avec l'infrastructure, le cloud, ou d'autres véhicules, ces nouveaux transports utilisent des technologies sans fil, ce qui facilite l'accès aux données. Effectivement, Etant donné que le transfert s'effectue par l'intermédiaire des ondes radio, les pirates informatiques peuvent plus facilement intercepter les data, et ainsi, avoir une certaine emprise sur le véhicule. Ces derniers ont notamment la possibilité de tromper le conducteur en lui fournissant de fausses informations de navigation, ou en contrôlant les données issues de ses capteurs, comme le verrouillage des portes ou l'état des airbags. De la même façon, il est tout à fait imaginable qu'un hackeur puisse reprogrammer les unités de commande électronique (UCE) en y introduisant des malwares, ce qui lui permettra d'avoir aussi bien la main sur les capteurs, que les actionneurs [61]. Par conséquence, une personne malintentionnée qui arriverait à accéder au réseau embarqué du véhicule, pourrait s'emparer de tous les dispositifs qui lui sont rattachés ; des pédales jusqu'aux systèmes d'info-divertissement.

Pour arriver à ses fins, le pirate informatique peut utiliser différentes attaques, notamment celles qui visent l'intégrité des données (man-in-the-middle par exemple), ou l'authenticité du conducteur. Les attaques telles que le déni de service, ou le brouillage radio, sont également employées, car elles bloquent l'accès des usagers en rendant les services inaccessibles.

Il existe plusieurs points d'accès pouvant être exploités :

- Premièrement, les éléments liés à l'architecture du véhicule, comme les UCE, le réseau, ou la passerelle de communication.
- Deuxièmement, le smartphone, qui peut aussi bien appartenir au conducteur qu'à un tiers.
- Et en dernière position, l'infrastructure de Cloud Computing.

Selon Anthony Di Prima et Gérôme Billois, experts en cybersécurité des véhicules, le niveau de sécurité des transports connectés est assez faible, ce qui pousse les constructeurs

automobiles à collaborer, dans le but d'améliorer la sécurité aussi bien dans le véhicule, qu'au sein de l'environnement. Il faut d'abord commencer par organiser les composants du plus à risque au moins critique, puis sécuriser les interfaces externes en usant des techniques de cryptage et d'authenticité, ce qui permettra de vérifier la légitimité des tentatives d'accès [61] [63].

3.3.2. Sa collaboration avec l'intelligence artificielle :

Une des principales transformations qui s'opère dans le secteur automobile, est le passage de véhicules pilotés par l'Hommes, à des véhicules conduits par eux même. Pour se faire, l'intelligence artificielle doit être en parfaite osmose avec l'IoT, car c'est grâce aux différentes données collectées par les capteurs, que l'autopilote pourra pleinement s'exprimer. En effet, l'IA du véhicule est connectée à l'ensemble des capteurs et récolte aussi bien les données sur la direction et les freins, que celles en provenance d'applications web comme Google Street View ou Google Maps. De plus, l'Internet des Objets par l'intermédiaire du V2X, va permettre l'échange d'informations entre les véhicules, mais avec la Smart City également ; ce qui viendra compléter les informations récoltées. Par conséquence, les véhicules autonomes pourront mieux anticiper les risques et les événements imminents, ce qui fluidifiera le trafic routier en diminuant le nombre d'accidents et d'embouteillages. Cette collaboration est donc primordiale pour les constructeurs automobiles, car elle permettra de tirer entièrement profit des avantages offert par les nouvelles technologies [63] [64].

L'interaction entre ces deux domaines doit être surveillé de très près, car il est toujours possible de tromper un autopilote en lui fournissant de fausses indications. L'un des meilleurs exemples et celui qui concerne la Tesla Model X, dont le système de pilotage automatique fut berné par une simple projection en 2D. Effectivement, au lieu d'utiliser un capteur LIDAR* afin d'obtenir une représentation de son environnement, ce modèle utilise des caméras connectées. En projetant l'image d'un piéton sur la route, une équipe de chercheurs a réussi à faire croire à l'autopilote qu'un vrai piéton se trouver là, ce qui le poussa à enclencher la manœuvre de freinage ; d'autres tests similaires ont été réalisés, dévoilant un peu plus les failles de ces caméras. En s'aidant d'un drone équipé d'un projecteur, il a notamment été possible d'influencer la vitesse du véhicule, en affichant pendant quelques secondes un faux panneau de circulation. Mais le pire restait à venir, car en projetant une fausse ligne blanche, les chercheurs sont parvenus à faire dévier la Tesla, qui a consciemment suivi cette dernière.

Par conséquence, la simple utilisation d'un drone et d'un projecteur, permet en théorie de générer, à peu près n'importe où, des attaques à distance intraçables.

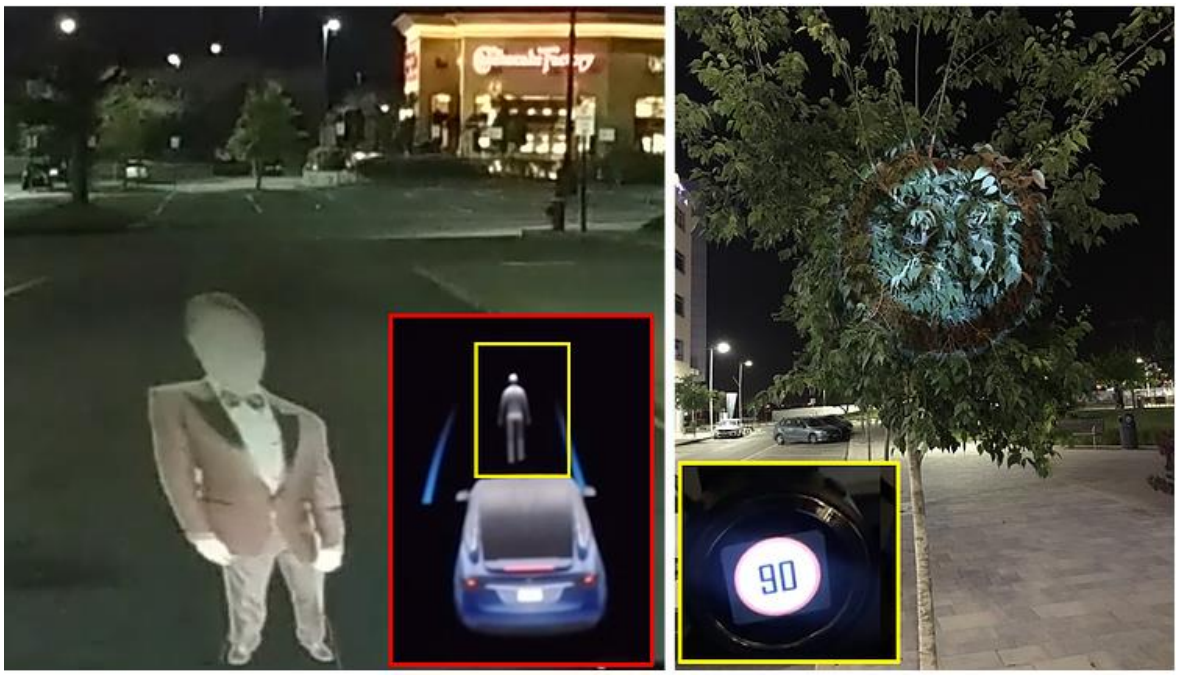


Figure 16 : Attaques fantômes contre les systèmes avancés d'aide à la conduite (2020) [66]

Plus récemment encore, le 1er juin 2020, l'autopilote d'une Tesla Model 3 fut incapable d'éviter un camion renversé sur une des autoroutes Taïwanaise, envoyant ainsi la voiture et son conducteur, s'encastrer de plein fouet dans la remorque de ce dernier. Au vu de la distance à laquelle se trouvait initialement le véhicule, le conducteur avait largement le temps de se déporter, ou de freiner. Nous pouvons constater sur une des caméras de surveillance que peu de temps avant l'impact, une tentative de freinage d'urgence a été amorcée de la part du conducteur ou de l'autopilote, ce qui rend la situation encore plus troublante [67]. Bien que tous ces cas de figure puissent effrayer, opter pour l'utilisation de l'IA embarquée peut se révéler redoutablement efficace. C'est ce que nous prouve le boulanger flamand K. Van Hoesen, qui croisa la route d'un sanglier en partant travailler à 4 heures du matin. Secondé par l'autopilote de sa Tesla, il fut capable d'éviter l'animal avec une précision des plus remarquable [68]

Les systèmes d'aide à la conduite conçus par les constructeurs automobiles ne remplacent pas le conducteur, mais l'assiste au cours de ses trajets. Afin de mettre en circulation des véhicules entièrement autonomes, il est donc primordial que les données récoltées par les différents capteurs embarqués restent fiables, car la sécurité des passagers en dépend.

3.3.3. L'implémentation de la 5G :

L'automobile moderne se transforme de plus en plus en un dispositif IoT, dû à une multitude de capteurs et de systèmes de communication embarqués. Afin d'améliorer la sécurité routière et l'efficacité globale du trafic, les constructeurs automobiles cherchent à réduire le délai de transmission au cours d'une communication V2X, ce qui les a amené à s'intéresser de plus près à la 5G. En effet, bien que cette technologie soit toujours en cours de réalisation, de nombreux pays l'ont déjà déployé, à l'instar de la Corée du Sud qui compte 85 villes dorénavant couvertes par le réseau 5G [68]. Avec un temps de réaction d'1 ms et un débit 100 fois plus rapide que son prédécesseur, la 5G sera à même de répondre au nombre croissant de connexions, engendré par le développement de l'IoT. Effectivement, on prévoit un total de 13,8 milliards d'objets connectés dans le monde à l'horizon de 2024, d'où l'intérêt d'utiliser une technologie cellulaire capable de répondre aux besoins de chacun [70].

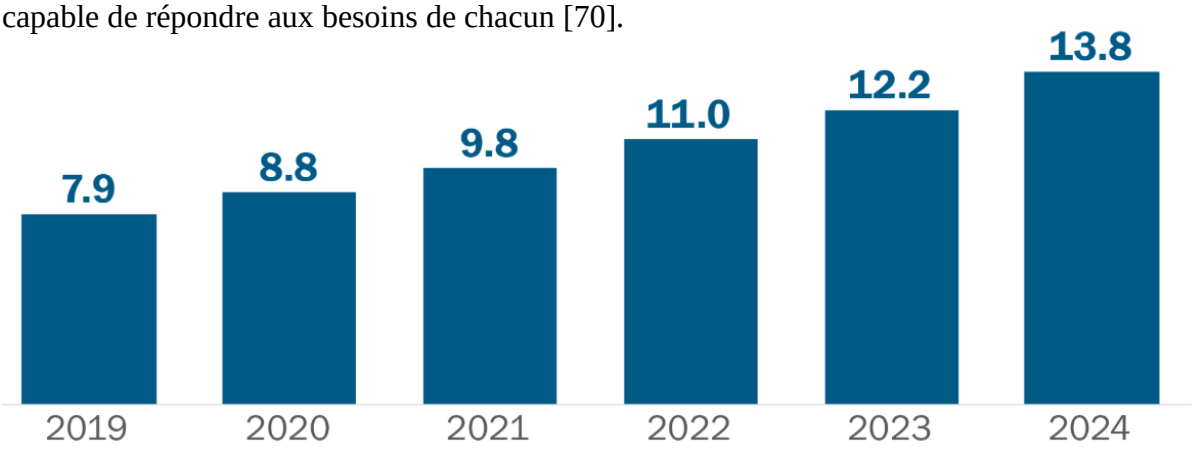


Figure 16 : Nombre total d'objets connectés dans le monde en milliard (2019) [70]

Pour l'instant, les véhicules autonomes ne peuvent pas être entièrement développés, car le temps de latence dans le cadre d'une communication V2X est encore trop important ; ce qui devrait être résolu grâce à la 5G. En effet, cette technologie permettra le transfert d'informations en temps réel tout en offrant, sans risque de saturation, une plus grande densité d'objets connectés au km^2. Cela présente un enjeu aussi bien en termes d'implémentation que de consommation, car comme nous l'avons vu précédemment, les appareils fonctionnant sur une bande 5G devrait consommer beaucoup plus. De la même façon, la couverture sera assurée par des antennes Small Cells, dont la portée se limite à quelques mètres, ce qui impliquera d'en utiliser davantage afin obtenir la même couverture qu'en 4G [30]. Grâce à la transmission en temps réel du Big Data, il sera donc possible de constituer des flottes intelligentes, d'où l'enjeu que cela représente.

4. Conception d'un système embarqué en cas d'infarctus ou d'AVC

Les maladies cardiovasculaires représentent environs 150 000 morts en France, soit à peu près 400 décès tous les jours, ce qui en fait la deuxième cause de mortalité. J'ai décidé de développer un système capable de prévenir l'infarctus et l'AVC, et de réagir en conséquence, après avoir visionné la vidéo d'un motard, dont la route croisa celle d'un homme victime d'une attaque au volant. J'ai été si abasourdi par l'incapacité du conducteur à reprendre le contrôle de son véhicule, que l'idée de trouver une solution germa dans mon esprit. Sur cette vidéo, on peut voir le conducteur coincé sur la pédale d'accélérateur, ce qui l'amène à percuter tout ce qui se présente devant lui, jusqu'à ce que le véhicule s'embourbe sur le bas-côté de l'autoroute https://www.youtube.com/watch?v=O8knc4h05uA.

4.1. Principe :

Ce système embarqué repose sur l'utilisation de deux technologies étroitement liées : l'Internet des Objets et l'intelligence artificielle. Son but est de contrôler, par l'intermédiaire d'un capteur, la fréquence cardiaque et le taux d'oxygène dans le sang du conducteur, afin d'en alerter son véhicule. De plus, les données récoltées pourront directement être exploitées par le médecin traitant, ce qui permettra de suivre l'évolution de la santé du patient. Si les mesures commencent à présenter un risque, le conducteur sera prévenu par l'intermédiaire du tableau de bord, et un message d'alerte envoyé en direction des secours. Dès lors que la crise survient, le véhicule prendra le relai grâce au pilote automatique, et se rangera en toute sécurité.

4.2. Premières réflexions :

4.2.1 : Qu'est-ce qu'un infarctus/AVC ?

Afin de choisir le capteur répondant le mieux à mon besoin, j'ai d'abord cherché à comprendre ce qui caractérise l'AVC et l'infarctus, ainsi que la différence qui figure entre les deux. L'infarctus, lui, est la nécrose du muscle cardiaque appelé myocarde, qui survient suite à l'obstruction d'une artère. Lorsque cette dernière est entièrement bouchée, l'apport en sang et en oxygène est trop faible, ce qui entraine la mort des cellules musculaires cardiaques en quelques heures. De la même façon, un accident vasculaire cérébral (AVC), correspond à l'endommagement d'une ou plusieurs zones du cerveau après l'arrêt brutal de l'irrigation en sang. Dans les deux cas de figure, la prise en charge doit se faire au plus vite, car la vie de la personne en dépend.

4.2.2 : Quels sont les paramètres à contrôler ?

Effectivement, pour que notre solution fonctionne il faut déjà savoir quoi mesurer, or, nous avons vu précédemment que la carence en oxygène était la principale cause des maladies cardio et cérébro-vasculaires ; nous allons donc chercher un moyen de mesurer la quantité d'oxygène dans le sang ainsi que la fréquence cardiaque. En théorie, le taux de saturation sanguin en oxygène (SpO2) peut être calculé en faisant le rapport de la concentration sanguine en oxyhémoglobine (CHbO2) sur la concentration totale d'hémoglobine dans le sang (CHb) ; il nous faut donc choisir un capteur capable d'effectuer ces mesures.

4.3. Fonctionnement :

4.3.1. Le capteur :

Nous allons intégrer au volant du véhicule un oxymètre de pouls (ou saturomètre) sans fil, afin de mesurer le taux d'oxygène et la fréquence cardiaque du conducteur. En effet, grâce à l'émission d'une lumière rouge et infrarouge produites par deux LED, l'oxymètre peut aussi bien calculer la saturation du sang en O2 que la fréquence cardiaque. Son fonctionnement est très simple, il repose sur le taux d'absorption de deux types d'hémoglobines différents : l'oxyhémoglobine et la désoxyhémoglobine. Lorsque l'hémoglobine (protéine responsable de la couleur rouge du sang) capte l'oxygène à hauteur des poumons, elle se transforme en oxyhémoglobine, tandis que la désoxyhémoglobine s'effectue au niveau des tissus. Etant donné que le taux d'absorption de la lumière rouge et infrarouge diffère en fonction de la charge en oxygène, il est donc possible de déterminer la saturation du sang en O2. De ce fait, la désoxyhémoglobine absorbe mieux les lumières rouges que l'oxyhémoglobine, car la libération de l'oxygène est beaucoup plus importante au niveau des tissus que des poumons. A l'opposé, l'oxyhémoglobine retiendra plus facilement les lumières infrarouges, puisque la charge en O2 des poumons est supérieure.

Le conducteur place son doigt entre un émetteur (les LED) et un récepteur de lumière, les deux lumières vont ensuite traverser la peau avant d'être réceptionner par une photodiode qui va calculer la quantité de lumière totale absorbée. Cette quantité va ensuite être utilisée afin de déterminer le taux d'oxygène en pourcentage dans le sang. En mesurant la variation des différents flux sanguins aux extrémités, il sera également possible de retranscrire la fréquence cardiaque de l'utilisateur.

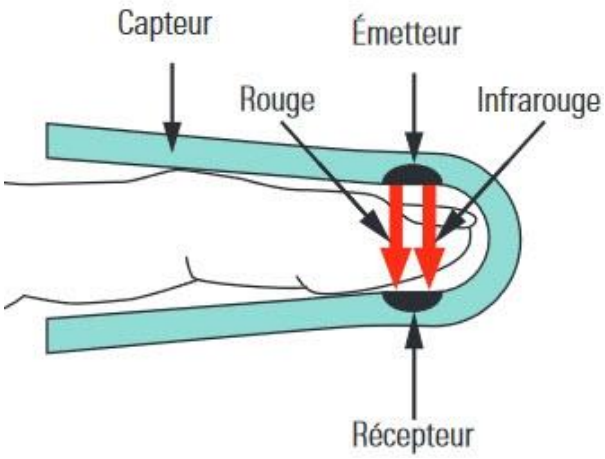


Figure 17 : Comment fonctionne un oxymètre de pouls ? - MediProStore

Afin de garder la sensation de conduite le plus fidèle possible, j'ai décidé de rendre l'oxymètre plus ergonomique en retirant la pince. En effet, je pense qu'un système de doigtier correspond mieux à notre cas de figure, car les gestes du conducteur seront moins entravés. Tout ceci n'est que théorique, mais je pense que nous pourrions utiliser les ondes hertziennes afin d'alimenter notre capteur, ce qui permettra de diminuer le nombre de composant tout en offrant une autonomie quasi illimitée. A l'instar du capteur Bluetooth de chez Wiliot, nous implémenterons un circuit pas plus gros qu'un timbre de poste, équipé d'une petite antenne et d'un convertisseur d'ondes en énergie électrique. Nous utiliserons cette même antenne afin de transmettre les mesures en direction du système d'info-divertissement du véhicule ; en règle générale, l'alimentation d'un oxymètre tourne autour des 3 V, ce qui ne devrait pas poser de problème. Voici la vision que j'ai de ce saturomètre :

Le circuit imprimé sera constitué de polyimide, ou de polyétheréthercétone (PEEK), ce qui le rendra flexible afin d'épouser parfaitement la forme du doigt.

4.3.2. La transmission des données :

Les données du capteur sont transmises en direction d'un Raspberry Pi Zero W auquel vient se rajouter un module PiCAN2, qui lui permet d'être relié au Bus CAN du véhicule. J'ai choisi ce modèle, car il est plus économe en énergie et coûte moins chère que son grand frère le Raspberry Bi 3B+ ; il est certes moins puissant mais ferra amplement l'affaire pour ce que nous allons en faire. J'installe à même l'OS du Raspberry le client MQTT Mosquitto, qui va me permettre de transférer les informations issues du saturomètre.

Avant de continuer il est important de rappeler ce qu'est MQTT : ce protocole est utilisé dans une architecture de type publieur/abonné, c'est à dire que nous aurons des personnes autorisées à publier des données, et d'autres qui les recevront. Les informations publiées sont identifiées par un topic, c'est à ce dernier que les utilisateurs s'abonnent afin de les récolter. Le broker, est le serveur qui fait office de pont entre les publieurs et les abonnés, c'est lui qui se charge d'acheminer les data entre eux. Prenons un exemple : imaginons que Alice possède un capteur de température qui effectue des relevés toutes les 20 minutes, cette dernière identifie ses mesures par le topic « temp » avant de les envoyer dans une BDD par l'intermédiaire du broker. Bob, n'aura qu'à s'abonner au topic « temp » de Alice afin de récolter les données.

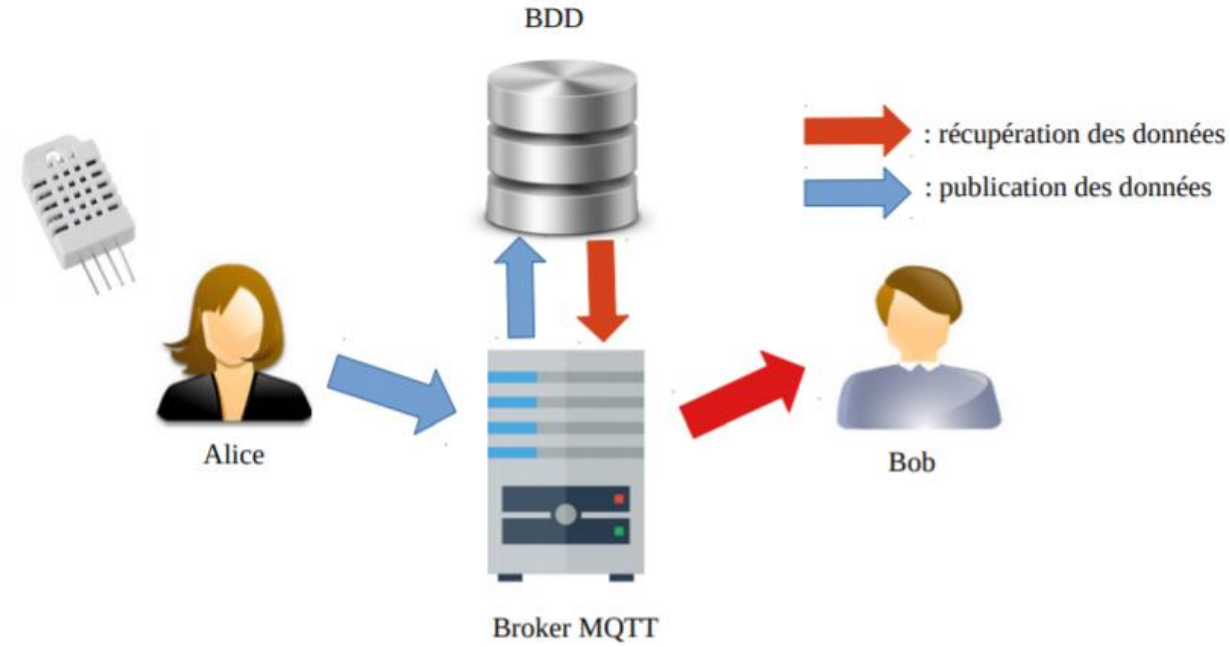


Figure 18 : Exemple de fonctionnement MQTT – PASCUAL Luc

Le Raspberry Pi Zero W, fera donc office de publieur MQTT en transférant les données récoltées en bluetooth en direction de l'unité de contrôle télématique (TCU), qui se charge en autre de la communication avec les réseaux mobiles externes (Wi-Fi, GSM, LTE…).

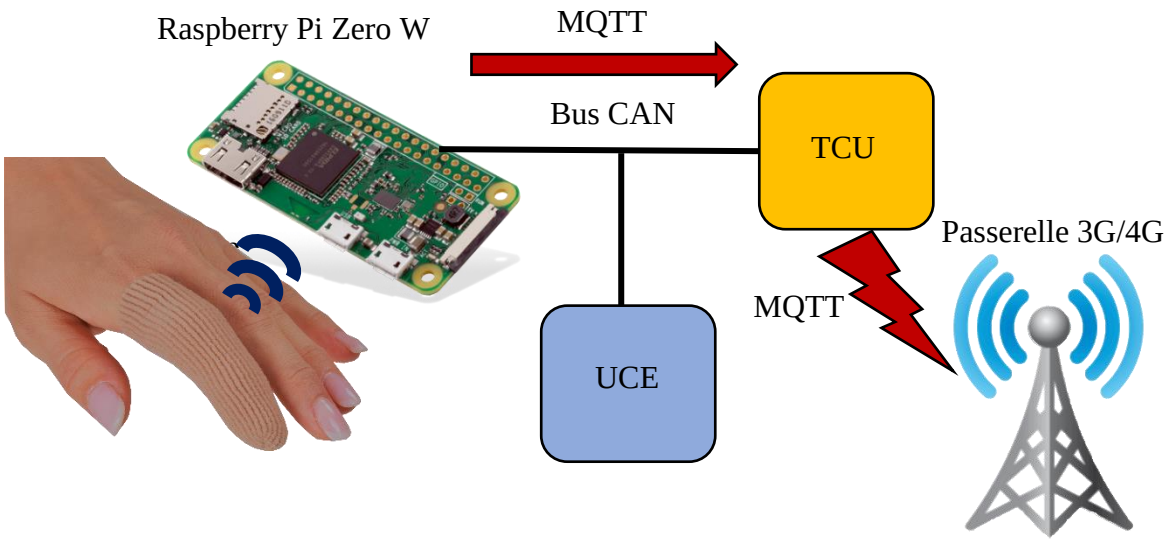


Figure 19 : Première étape de transfert – PASCUAL Luc

Après être passées par une passerelle 3G/4G, les informations se retrouvent sur Internet et circulent jusqu'à l'infrastructure du médecin traitant. De là, les data sont acheminées vers un broker Mosquitto privé couplé à une base de données NoSQL, qui va permettre de gérer un volume important de données. On attribue un topic différent à la fréquence cardiaque et au taux d'oxygène dans le sang, puis on opte pour un affichage graphique, sous Grafana de préférence. Le médecin n'aura qu'à s'abonner aux topics en question afin de visualiser la santé de son patient. J'ai choisi ce protocole au vu de sa communication bidirectionnelle (qui permettra au médecin d'envoyer à son tour des informations), mais aussi à sa manière de gérer les pertes de connexion ; en effet, grâce à la QoS 1 et 2, les données non transmises seront retransmises et acquittées. De plus, sa consommation en bande passante est très faible, ce qui s'accorde parfaitement avec la logique de responsabilité environnementale.

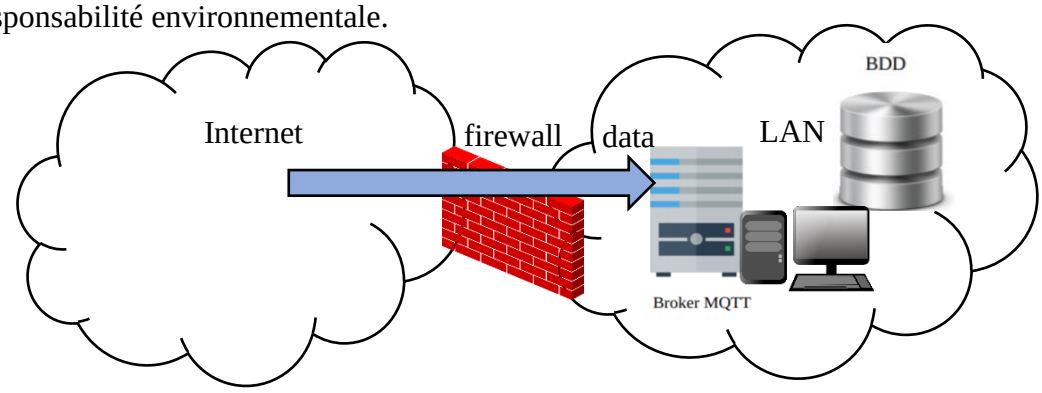


Figure 20 : Deuxième étape de transfert simplifiée – PASCUAL Luc

Afin que le médecin se repère, l'arborescence des topics sera organisée de la sorte :

`patient/nom/prenom/cardiaque` et `patient/nom/prenom/spo2`

Il faudra donc qu'il s'abonne au topic `patient/nom/prenom/#` enfin d'écouter toutes les valeurs.

4.3.3. Le système d'alerte :

Les UCE du véhicule peuvent, par l'intermédiaire du bus CAN, se renseigner sur la fréquence cardiaque et le taux d'oxygène dans le sang du conducteur. Il leur suffit de récupérer les données issues de l'oxymètre en interrogant le Raspberry Pi Zero W, lui-même relié au bus.

La saturation d'oxygène dans le sang est normalement comprise entre 95 % et 100 %, entre 90 % et 94 % elle est insuffisante, et lorsque cette dernière descend en dessous des 90 %, c'est un cas d'urgence. Pour ce qui est de l'infarctus et de l'AVC, le risque se présente au-delà des 120 pulsations/minute (potentielle fibrillation atriale*), il faut de la même manière vérifier que la fréquence cardiaque ne descende pas en dessous des 40 pulsations/minute (bradycardie*), l'UCE récupère donc ces mesures afin de se renseigner sur l'état général du conducteur. Si les relevés s'avèrent anormales, l'UCE alertera le système eCall du véhicule qui, à son tour, établira une communication vocale avec le centre d'appel d'urgence. L'opérateur au bout du fil interrogera directement le conducteur afin de s'assurer de son état (si toutefois ce dernier a la capacité de le faire). En parallèle de l'appel, l'opérateur recevra un paquet contenant un minimum de data (MSD) sur la fréquence cardiaque, le taux d'SpO2, les coordonnées GPS du véhicule, ou encore le nombre de passagers. De plus, si l'utilisateur commence à ressentir des symptômes (paralysie, faiblesse, douleur thoracique…) il pourra lui-même enclencher l'eCall par l'intermédiaire d'un bouton poussoir.

L'eCall est, depuis le 1er avril 2018, obligatoire dans les véhicules nouvelles génération, ce qui permet aux secours d'accélérer la prise en charge.

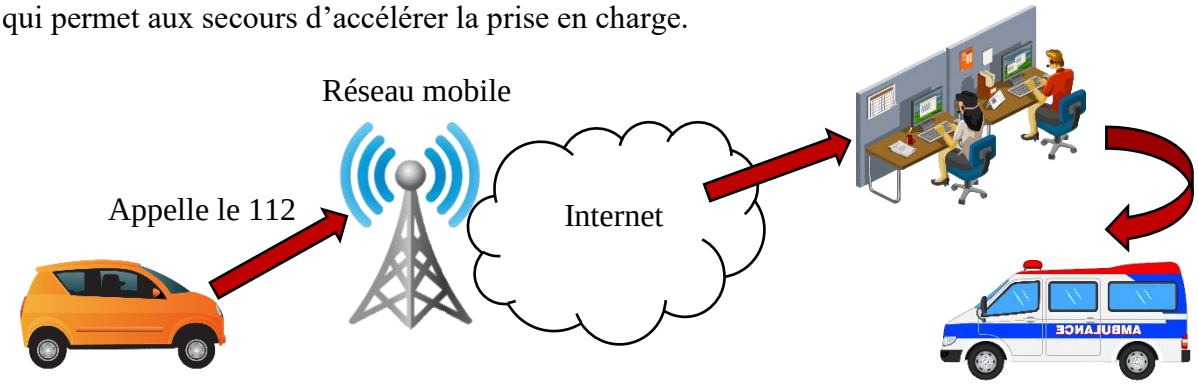


Figure 21 : Fonctionnement de l'eCall – PASCUAL Luc

4.3.4. Le pilote automatique :

Dès lors qu'un conducteur subit une attaque cardio ou cérébro-vasculaire, il perd le contrôle total de son véhicule, pour remédier à ce problème, nous allons essayer de développer un début de solution en mêlant l'Internet des Objets à l'intelligence artificielle. Lorsque que la crise survient, il faut éviter au conducteur de toucher au volant ainsi qu'aux pédales, nous allons donc utiliser les technologies Drive-by-wire, qui cherche à remplacer les organes mécaniques du véhicule par des systèmes électriques ou électromécaniques ; il faut donc par conséquence, revoir l'architecture du véhicule traditionnel.

Pour le contrôle de la direction, c'est le Steer-by-wire qui nous intéresse. Tout d'abord, nous avons un ensemble de capteur qui permettent d'accéder aux données sur l'angle des roues arrière, des roues avant, et du volant. Ces données sont ensuite acheminées en direction de deux unités de commande électronique par l'intermédiaire d'un bus FlexRay :

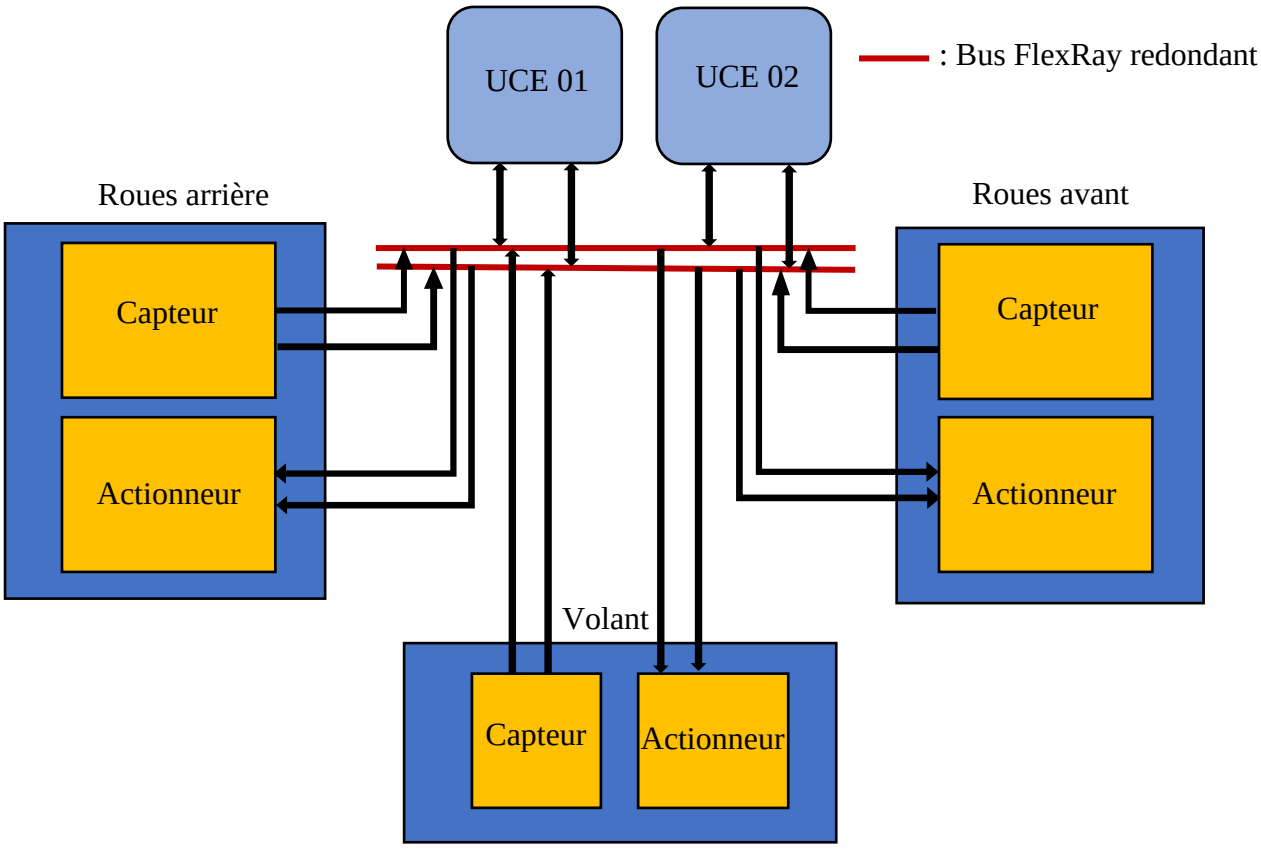


Figure 21 : Architecture Steer-by-wire – PASCUAL Luc

Le volant ainsi que les pédales seront présents en double dans l'habitacle du véhicule, en effet, lorsque les mesures en provenance du saturomètre présentent un risque, la liaison avec le

volant et les pédales principales sera rompue grâce à l'actionneur et le pilote automatique prendra le relais par l'intermédiaire des doubles commandes (by-wire également). Cette idée, bien que théorique, devrait empêcher les gestes brusques du conducteur durant la crise. Le même principe sera appliqué aux freins (Brake-by-wire) ainsi qu'à l'accélérateur (Throttle-by-wire). Les données en provenance des caméras et des capteurs (LIDAR et ultrason) seront traitées par les UCE, qui à leur tour, contrôleront la conduite par le biais des actionneurs. Le pilote automatique cherchera à ranger le véhicule sur le côté en attendant les secours ; le système eCall devra continuer à émettre ses coordonnées GPS en direction des ambulanciers.

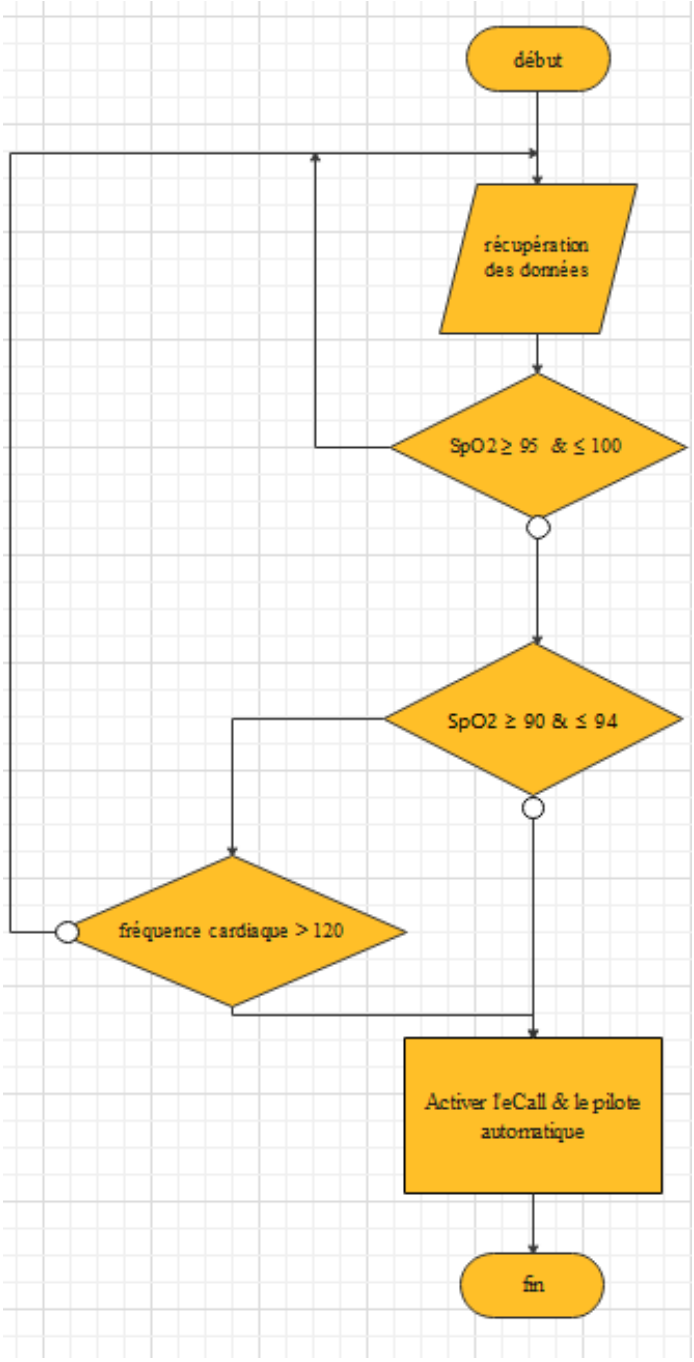


Figure 22 : Logigramme simplifié du système d'alerte – PASCUAL Luc

4.4. Problèmes potentiels

Cette solution n'est toutefois pas exempte de défaut, j'ai décelé quelques problèmes qui pourraient venir troubler le bon fonctionnement du système :

- **Premièrement** : le vernis à ongle, qui peut fausser le résultat de l'oxymètre. En effet, la couleur du vernis peut absorber les lumières émises par le saturomètre et ainsi, empêcher la détection de l'oxygène dans le sang. Il faudra donc laisser un doigt sans vernis ou plutôt opter pour du rouge foncé (le seul n'entrainant aucun modification significative).

- **Deuxièmement** : le frein à main, qui doit être hors de portée du conducteur lors de la crise. Effectivement, pris de panique, ce dernier pourrait avoir tendance à actionner le frein à main si la voiture ne l'obéit plus, il faudra donc opter pour un système by wire à l'instar du volant et des pédales.

- **Troisièmement** : le pilote automatique, qui comme nous l'avons vu précédemment n'est pas totalement infaillible. Il faudra donc attendre que la sécurité des véhicules autonomes soit améliorée.

5. Conclusion

Comme nous l'avons vu au cours de ce mémoire, l'IoT change considérablement notre société, aussi bien d'un point de vue économique qu'infrastructurel. Le secteur automobile est particulièrement impacté par ce développement, qui modifie aussi bien les méthodes de production industrielle, que les moyens de transports nouvelle génération.

En intégrant la communication V2X et l'intelligence artificielle, nous serons à même de profiter au maximum des opportunités que présentent ces nouvelles technologies. A terme, cela permettra de réduire considérablement le nombre d'accident, de fluidifier la circulation, et de mieux gérer les émissions de CO^2. Les constructeurs automobiles font face à un besoin urgent et croissant d'intégrer l'Internet des Objets au cœur de leur processus de fabrication, car ils font face à une très forte concurrence.

Ils devront donc s'adapter à de nouvelles expériences marketing et commerciales, afin de répondre aux attentes de leurs consommateurs, qui s'intéressent de plus en plus aux solutions connectées.

6. Annexe

- **TCAC** : Taux de Croissance Annuel Composé, qui représente la croissance sur plusieurs années.

- **tuple** : liste de valeurs qui ne peut plus être modifiées.

- **TIC** : Technologies de l'Information et de la Communication.

- **ERP** : de l'anglais « Enterprise Ressource Planning », est un progiciel qui permet la gestion de l'ensemble des processus opérationnels au sein de l'entreprise.

- **RFID :** méthode de mémorisation et de récupération de données par l'intermédiaire d'une radio-étiquette.

- **gigue** : variation de la latence ou du délai de transmission au sein d'un réseau informatique.

- **LIDAR** : technologie qui utilise la télédétection par laser.

- **fibrillation atriale** : caractérise une fréquence cardiaque irrégulière et souvent très rapide.

- **bradycardie** : trouble du rythme cardiaque anormalement faible.

7. Bibliographie

[1] MARKETSANDMARKETS (2019).

Global Forecast to 2027.

https://www.marketsandmarkets.com/Market-Reports/connected-car-market-102580117.html?gclid=CjwKCAjwqpP2BRBTEiwAfpiD-2BCY8e3hseyKMZib5sHMXGqO17F9oTJRdHdL1G5Kf8CifkqGqkWVxoCSPgQAvD_BwE

[2] Internet Prediction (2010) Estrin, Deborah and Chandy, K. Mani and Young, R. Michael and Smarr, Larry and Odlyzko, Andrew and Clark, David and Reding, Viviane and Ishida, Toru and Sharma, Sharad and Cerf, Vinton G. and Hölzle, Urs and Barroso, Luiz André and Mulligan, Geoff and Hooke, Adrian and Elliott, Chip (2010) *Internet Predictions.* IEEE Internet Computing, 14 (1). pp. 12-42. ISSN 1089-7801. https://authors.library.caltech.edu/17375/1/Chandy2010p6880Ieee_Internet_Comput.pdf

[3] Internet of Things-IOT : Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges – K. K. Patel, S. M Patel, P G Scholar, C. Salazar (2016).

https://www.researchgate.net/publication/330425585_Internet_of_Things-IOT_Definition_Characteristics_Architecture_Enabling_Technologies_Application_Future_Challenges

[4] Smart Objets as Building Blocks for the Internet of Things – IEEE Internet Computing (2010)
https://ieeexplore.ieee.org/document/5342399

[5] The Internet of Things : A Survey – L. Atzori, A. Iera, G. Morabito (2010).

https://www.researchgate.net/publication/222571757_The_Internet_of_Things_A_Survey

[6] Sémantique et Internet des objets : d'un état de l'art à une ontologie modulaire – N. Seydoux, M. B. Alaya, N. Hernandez, T. Monteil, O. Haemmerlé (2015).

https://hal.archives-ouvertes.fr/hal-01166052/document

[**7]** SOA vs MVSOA : Une architecture orientée services multivues – A. Kenzi, B. El Asri, M. Nassar, A. Kriouile (2008).

http://www.cari-info.org/actes2008I/kenzi.pdf

[8] Internet of Things : Vision, Applications and Challenges – R. Mehta, J. Sahni, K. Khanna (2018).

https://www.researchgate.net/publication/325664149_Internet_of_Things_Vision_Applications_and_Challenges

[9] The Internet of Things : Vision & Challenges – M. Elkhodr, S. Shah, H. S. Cheung (2013)

https://www.researchgate.net/publication/256461848_The_Internet_of_Things_Vision_Challenges

[10] A functional approach to information system interoperability - H. yliopisto.

Department of Computer Science, F. Eliassen, and J. Veijalainen (1988).

[11] Interoperability in Internet of Things: Taxonomies and Open Challenges – M. Noura, M. Atiquzzaman, M. Gaedke (2019).

https://link.springer.com/content/pdf/10.1007/s11036-018-1089-9.pdf

[12] IoT Security, Privacy, Safety and Ethics – H. F. Atlam, G. Wills (2019)

https://www.researchgate.net/publication/332859761_IoT_Security_Privacy_Safety_and_Ethics

[13] An Internet-connected fish tank let hackers into a casino's network – Z. Zorz (2017)
https://www.helpnetsecurity.com/2017/07/27/internet-connected-fish-tank-hackers/

[14] IOT Security Challenges and Issues An Overview – P. Ganapathi, M. Sujithra (2016).

https://www.researchgate.net/publication/301887203_IOT_Security_Challenges_and_Issues_-_An_Overview

[15] Big Data Management Challenges – S. Šuman (2020)

https://www.researchgate.net/publication/339672487_Big_Data_Management_Challenges

[16] An Unstructured to Structured Data Conversion using Machine Learning Algorithm in Internet of Things (IoT) – S. Verma, K. Jain, Dr C. Prakash (2020)

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3563389

[17] Big Data, Big Challenges – P. Kanani, M. C. Padole, Z. Doshi, R. Agrawal (2020)

https://www.researchgate.net/publication/341323217_Big_Data_Big_Challenges

[18] We do not have Systems for Analysing IoT Big-Data – Y. Sasaki (2020)

https://www.researchgate.net/publication/339787416_We_do_not_have_Systems_for_Analysing_IoT_Big-Data

[19] Here's How Much Big Data Companies Make On The Internet – K. Matthews (2018)

https://www.smartdatacollective.com/how-much-big-data-companies-make-on-internet/

[20] Volume of data/information created worldwide from 2010 to 2025 (2020)

https://www.statista.com/statistics/871513/worldwide-data-created/#:~:text=Information%20created%20globally%202010%2D2025&text=The%20total%20amount%20of%20data,reaching%20175%20zetabytes%20in%202025.

[21] Characteristics and Analysis of Hadoop Distributed System – S. R. M. Zeebaree, L. Haji, R. Zebari, H. M. Shukur (2020)

https://www.researchgate.net/publication/341775003_Characteristics_and_Analysis_of_Hadoop_Distributed_Systems

[22] Why use Apache Storm ? – Site officiel
https://storm.apache.org/

[23] Big Data et Machine Learning - 3e éd : Les concepts et les outils de la data science –

P. Lemberger, M. Batty, M. Morel, J-L. Raffaëlli (2019)

https://books.google.fr/books?id=yDulDwAAQBAJ&pg=PT328&lpg=PT328&dq=Apache+Storm+stockage&source=bl&ots=42gpRw_1IE&sig=ACfU3U32-Opvx4M0GMuZCh5U-mLWIS1x8Q&hl=fr&sa=X&ved=2ahUKEwiKpsvZ_ujpAhVQhRoKHV_ACC0Q6AEwBXoECAsQAQ#v=onepage&q=Apache%20Storm%20stockage&f=false

[24] The Magnitude of Big Data 5vs in Business Macroclimate – S.-F Fam, I. Noriszura, W. L. Shinyie (2019)

https://www.researchgate.net/publication/335028796_The_Magnitude_of_Big_Data_5vs_in_Business_Macroclimate

[25] Exploring Techniques of Improving Security and Privacy in Big Data – B. Shaqiri (2017)

https://www.researchgate.net/publication/321050765_Exploring_Techniques_of_Improving_Security_and_Privacy_in_Big_Data

[26] Green IoT — Issues and Challenges – R. Ahmed (2019)

https://www.researchgate.net/publication/333893276_Green_IoT_-_Issues_and_Challenges

[27] Low Power Wide Area Technology – THALES

https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/resources/innovation-technology/low-power-wide-area-technology

[28] Understanding Creen IoT : Research Applications and Future Directions – N. Mehgashree, R. Girija, D. Sumathi (2019)

https://www.researchgate.net/publication/334559712_Understanding_Green_IoT_Research_Applications_and_Future_Directions

[29] Quelle est l'empreinte environnementale du numérique mondial ? – F. Bordage (2019)

https://www.greenit.fr/2019/10/22/12982/

[30] 5G Telecom Power Tager Network White Paper – HUAWEI (2019)

https://carrier.huawei.com/~/media/CNBGV2/download/products/network-energy/5G-Telecom-Energy-Target-Network-White-Paper.pdf

[31] La 5G : l'efficacité énergétique "by design" – Orange (2020)

https://hellofuture.orange.com/fr/la-5g-lefficacite-energetique-by-design/

[32] INDUSTRY 1.0 TO 4.0: THE EVOLUTION OF SMART FACTORIES – J. Thangaraj, R. M. Narayanan (2018)

https://www.researchgate.net/publication/330336790_INDUSTRY_10_TO_40_THE_EVOLUTION_OF_SMART_FACTORIES

[33] HANNOVER MESSE – 2011

https://www.pbkik.hu/download.php?id=11935

[34] Les concepts de l'industrie 4.0 – ITMI Québec (2017) http://www.itmi.ca/fr/accueil/

[35] A Study on Industry 4.0 Concept – C. V. Bidnur (2020)

https://www.ijert.org/a-study-on-industry-40-concept

[36] Industry 4.0 implications in logistics: an overview – L. Barreto, A. Amaral, T. Pereira (2017)

https://www.researchgate.net/publication/320343294_Industry_40_implications_in_logistics_an_overview

[37] Industry 4.0: the Future Concepts and New Visions of Factory of the Future Development – D. Vuksanović, J. Vešić, D. Korčok (2016)
https://www.researchgate.net/publication/303561107_Industry_40_the_Future_Concepts_and_New_Visions_of_Factory_of_the_Future_Development

[38] L'Industrie 4.0 dans la construction automobile – COPA-DATA

https://www.copadata.com/fr/industries/usineintelligente/smart-factory-insights/construction-automobile-intelligente/automotive-3-23/

[39] Intégration horizontale et verticale dans l'usine intelligente – COPA-DATA

https://www.copadata.com/fr/industries/integrationhorizontaleetverticale/#:~:text=Industrie%204.0%20%3A%20mise%20en%20r%C3%A9seau%2C%20communication%20et%20efficacit%C3%A9&text=Deux%20des%20facteurs%20les%20plus,horizontale%20et%20l'int%C3%A9gration%20verticale.

[40] Automotive Industry in the Context of Industry 4.0 Strategy – J. Sinay, Z. Kotianová (2018)

https://www.researchgate.net/publication/331507570_Automotive_Industry_in_the_Context_of_Industry_40_Strategy

[41] Industry 4.0 in the Volkswagen Group – Volkswagen Group (2015)

https://www.youtube.com/watch?v=JTl8w6yAjds

[42] Industry 4.0: A review on industrial automation and robotic – M. A. K. Bahrin, F. Othman, N. H. N. Azli, M. F. Talib (2016)

https://www.researchgate.net/publication/304614356_Industry_40_A_review_on_industrial_automation_and_robotic

[43] FUTURE OF WORK WITH THE INDUSTRY 4.0 – A. Görmüş (2019)

https://www.researchgate.net/publication/336846985_FUTURE_OF_WORK_WITH_THE_INDUSTRY_40

[44] Made Smarter Review – professeur J. Maier (2017)

https://www.gov.uk/government/publications/made-smarter-review

[45] TRAINING THE WORKFOCE FOR INDUSTRY 4.0 – N. Ninan, M. R. Thomas (2019)

https://www.researchgate.net/publication/333447750_TRAINING_THE_WORKFORCE_FOR_INDUSTRY_40

[46] Industry 4.0 : Educating the Workforce of Tomorrow – J. Flynn, D. Schaefer (2018)

https://www.researchgate.net/publication/326610183_Industry_40_Educating_the_Workforce_of_Tomorrow

[47] Nombre de véhicules connectés en circulation en France 2017-2022 – Statista (2018)

https://fr.statista.com/statistiques/669112/projection-nombre-voitures-connectees-circulation-france/

[48] Future Automobile an Introduction of IOT – S. Vasamsetti (2017)

https://www.researchgate.net/publication/329125371_Future_Automobile_an_Introduction_of_IOT

[49] Internet Of Things (IoT) In The Smart Automotive Sector: A Review – R. K. Bajaj, M. Rao, H. Agrawal (2018)

http://www.iosrjournals.org/iosr-jce/papers/Conf.CRTCE%20-2018)/Volume%201/7.%2036-44.pdf?id=7557

[50] Connected Car Architecture and Virtualization – H. Dakroub, A. Shaout, A. Awajan (2016)

https://www.researchgate.net/publication/301272903_Connected_Car_Architecture_and_Virtualization

[51] Connected Car & IoT Overview – A. Berdigh, K. El Yassini, K. Oufaska (2018)

https://www.researchgate.net/publication/326461095_Connected_Car_IoT_Overview

[52] Intra-Vehicular Wireless Sensor Network – Commission européenne CORDIS (2010 – 2014)

https://cordis.europa.eu/project/id/256441/fr

[53] Architecture réseaux et électroniques embarqués automobile – M. A. M. Oubrahim, K. Tahiry, A. Farchi (2019)

https://hal.archives-ouvertes.fr/hal-02297021/document

[54] CAN, FlexRay, MOST versus Ethernet for vehicular network – L. SVB, A. Sawant (2018)

https://www.researchgate.net/profile/Dr_Svb/publication/327222246_CAN_FlexRay_MOST_versus_Ethernet_for_vehicular_networks/links/5b813f1e299bf1d5a726f533/CAN-FlexRay-MOST-versus-Ethernet-for-vehicular-networks.pdf

[55] Vehicle-to-Pedestrian Communication for Vulnerable Road Users: Survey, Design Considerations, and Challenges – P. Sewalkar, J. Seitz (2019)

https://www.researchgate.net/publication/330451361_Vehicle-to Pedestrian_Communication_for_Vulnerable_Road_Users_Survey_Design_Considerations_and_Challenges

[56] Bilan sécurité routière 2019 – Ministère de l'intérieur

http://www.datapressepremium.com/rmdiff/2008914/diff_2017092010220103515.pdf

[57] Proposition d'une structuration dynamique d'un réseau de communication intervéhiculaire pour les ITS – L. Rivoirard, M. Wahl, P. Sondi, M. Berbineau (2018)

https://www.researchgate.net/publication/325904968_Proposition_d'une_structuration_dynamique_d'un_reseau_de_communication_intervehiculaire_pour_les_ITS

[58] Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application – S. Raghay (2014)

https://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf

[59] Highly Automated Vehicle Systems – chapter 9 : Vehicle to Infrastructure interaction (V2I) – P. Gáspár, P. Aradi, A. Décsei-Paróczi, S. Aradi, Z. Szalay (2014)

http://moodle.autolab.uni-pannon.hu/Mecha_tananyag/jarmurendszerek_iranyitasa_angol/

[60] In-vehicle commerce opportunities drive total connected cars to exceed 775 million by 2023 – Juniper Research (2018)

https://www.juniperresearch.com/press/press-releases/in-vehicle-commerce-opportunities-exceed-775mn?ch=Connected%20car

[61] Security of communications in connected cars Modeling and safety assessment – T. Sanae, Y. Tabii, A. Ramrami (2017)

https://www.researchgate.net/publication/318798975_Security_of_communications_in_connected_cars_Modeling_and_safety_assessment

[62] Security issues and vulnerabilities in connected car systems – T. Bécsi, S. Aradi, P. Gáspár (2015]

https://www.researchgate.net/publication/281447339_Security_issues_and_vulnerabilities_in_connected_car_systems

[63] Cyberattaque : quelle sécurité pour la voiture connectée ? – Interview par Delphine Sabattier (2019)

https://www.zdnet.fr/actualites/video-le-niveau-de-securite-des-voitures-connectees-est-assez-faible-39879711.htm

[64] How Do Autonomous Car Work ? – J. Ondruš, E. Kolla, P. Vertal, Ž. Šarić (2019)

https://www.sciencedirect.com/science/article/pii/S2352146520300995/pdf?md5=242dbaeafaa95c732e35369d50c08a48&pid=1-s2.0-S2352146520300995-main.pdf

[65] L'IoT propulse le véhicule autonome vers de nouveaux types de services de mobilité - ERTICO, Institut VEDECOM, Communauté d'agglomération Versailles Grand Parc (2020)

https://autopilot-project.eu/wp-content/uploads/sites/16/2020/02/2020-02-06-CP-AUTOPILOT-FINAL-EVENT.pdf

[66] Phantom of the ADAS: Phantom Attacks on Driver-Assistance Systems – B. & D. Nassi, R. Ben-Netanel, Y. Mirsky, O. Drokin, Y. Elovici (2020)

https://pdfs.semanticscholar.org/0842/8fb2ce2732afbc9d91a63359cc603a25602a.pdf

[67] Tesla en Autopilote : une vidéo d'un choc violent rappelle qu'il faut rester vigilant – M. Claudel (2020)

https://www.numerama.com/vroom/627803-tesla-en-autopilote-une-video-dun-choc-violent-rappelle-quil-faut-rester-vigilant.html?fbclid=IwAR02a_YPJaon4qoXLu4anszOJjFrVLRXHjIoJh83O3G04ab_YmwOQUOr11Y

[68] Watch Tesla Autopilot avoid running over a pig in the middle of the road – F. Lambert (2020)

https://electrek.co/2020/06/08/tesla-autopilot-avoid-pig-video/

[69] The State of 5G Deployments, The Battle for 5G Supremacy Heats Up – VIAVI (2020)

https://www.viavisolutions.com/fr-fr/literature/state-5g-deployments-2020-poster-chart-en.pdf

[70] 451 Research – 451 Research's Analysis of the Internet of Things Market Indicates that Total Connected Devices Will Reach 13.8 Billion by 2024

https://451research.com/451-research-analysis-of-iot-market-indicates-total-connected-devices-will-reach-13-billion-by-2024