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

2. l'Internet des Objets

2.1 : Définition et concept

2.2 : Son architecture

2.3 : Les défis à relever

2.3.1 : l'Interopérabilité

2.3.2 : Sécurité et confidentialité

2.3.3 : Les coûts énergétiques

3. Au cœur du secteur automobile

3.1 : La quatrième révolution industrielle

3.1.1 : Définition et concept

3.1.2 : Les nouveaux moyens de production

3.1.3 : Quant-est-il de la main d'œuvre

3.2 : l'Emergence des véhicules connectés

3.2.1 : Principe

3.2.3 : Pour répondre à quels besoins

3.2.2 : Architecture

3.3 : De nouveaux moyens de communications

3.2.1. : Du véhicule à l'utilisateur

3.2.2. : Entre véhicules

3.2.3 : Du véhicule à l'infrastructure réseau

3.3 : Les enjeux

3.3.1 : Assurer la sécurité du conducteur

3.3.1 : Sa collaboration avec l'intelligence artificielle

3.3.2 : Son interaction au sein de la Smart City

4. Conception d’un système embarqué en cas d’infarctus

4.1. Principe

4.2. Fonctionnement

4.3. Sécurité

4.4. Coût

Cette idée est en attente de validation.

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.

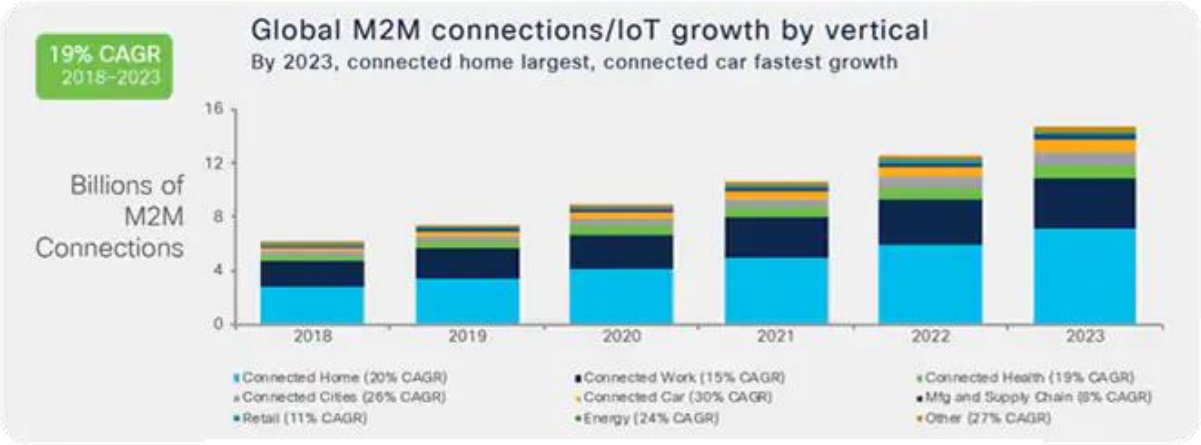

Figure 1 : Cisco Annual Internet Report, 2018–2023

Bien que son emprise s'étende dans différent 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 futures évolutions technologiques.
- 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].

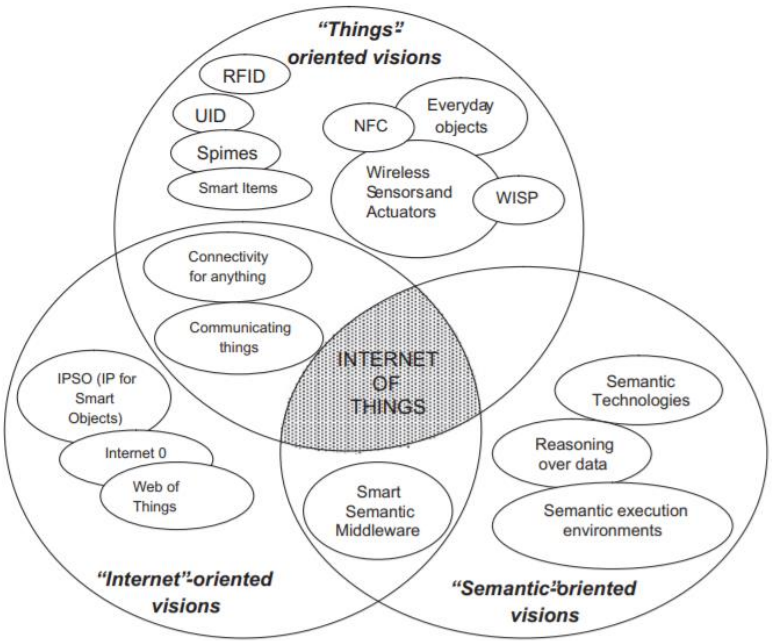

Figure 2 : Convergence des différentes visions de l'IoT (L. Atzori et al)

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 par l'intermédiaire des 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 leurs analyses. 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 ;

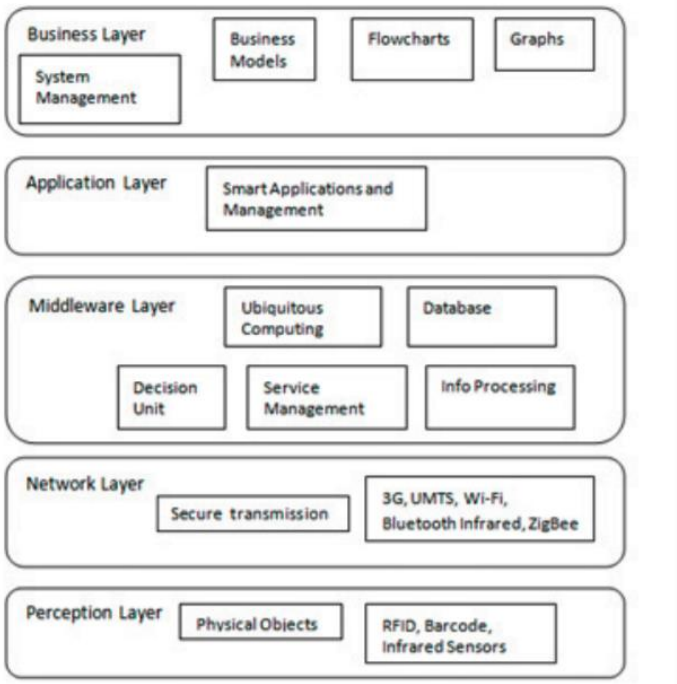

Figure 3 : Architecture IoT (Rishika Mehta et al)

2.3. Les défis à relever :

L'apparition des nouvelles technologies augmentent 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*, 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 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 [9], 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 [10] [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 l'utilisateur 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 [11].

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, rattaché au réseau de l'établissement, usurpant ainsi 10 Go de données qui furent rapidement exfiltrer en direction de la Finlande [12].

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 [13] :

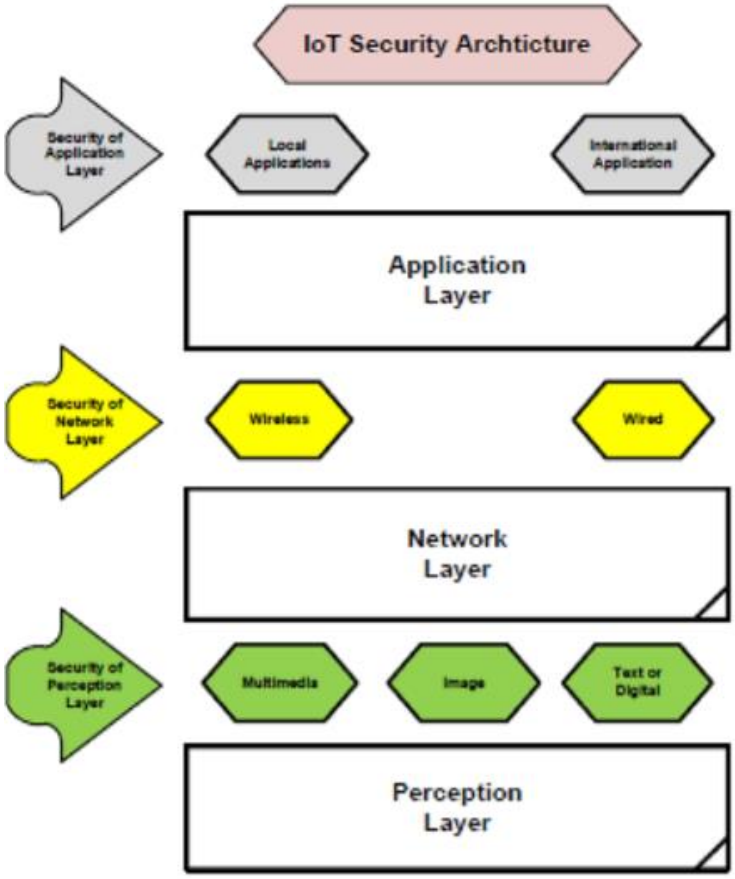

Figure 4 : Architecture IoT sécurisée (Padmavathi G, Sujithra M)

De la même façon, il faut pouvoir garantir l'anonymat de l'utilisateur, et la confidentialité de ses données. 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.

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 – Keyur K Patel, Sunil M Patel, P G Scholar, Carlos 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 - Luigi Atzori, Antonio Iera, Giacomo 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 - Nicolas Seydoux, Mahdi Ben Alaya, Nathalie Hernandez, Thierry Monteil, Ollivier Haemmerlé (2015).
https://hal.archives-ouvertes.fr/hal-01166052/document

[7] SOA vs MVSOA : Une architecture orientée services multivues - Adil Kenzi, Bouchra El Asri, Mahmoud Nassar, Abdelaziz Kriouile (2008).

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

[8] Internet of Things : Vision, Applications and Challenges - Rishika Mehta, Jyoti Sahni, Kavita Khanna (2018).

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

[9] A functional approach to information system interoperability - H. yliopisto. Department of Computer Science, F. Eliassen, and J. Veijalainen (1988).

[10] Interoperability in Internet of Things: Taxonomies and Open Challenges – Mahda Noura, Mohammed Atiquzzaman, Martin Gaedke (2019).

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

[11] IoT Security, Privacy, Safety and Ethics – Hany F Atlam, Gary Wills (2019)

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

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

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

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

[14] A Brief Survey on IoT Privacy: Taxonomy, Issues and Future Trends – Kinza Sarwar, Sira Yongchareon, Jian Yu (2019).

https://www.researchgate.net/publication/332296369_A_Brief_Survey_on_IoT_Privacy_Taxonomy_Issues_and_Future_Trends

[15] Industry 4.0 Concept : Background and Overview – Andreja Rojko

https://online-journals.org/index.php/i-jim/article/view/7072

[16] Connected Car & IoT Overview – Asmaa Berdigh, Khalid El Yassini, Kenza Oufaska (2018)

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

[17] Strategic response to Industry 4.0 : an empirical investigation on the Chinese automotive industry – Danping Lin, C. K. M. Lee, Henry Lau, Yang Yang (2018)

https://www.researchgate.net/publication/323297465_Strategic_response_to_Industry_40_an_empirical_investigation_on_The_Chinese_automotive_industry

[18] Internet of Things in Industries: A Survey – Li Da Xu, Wu He, Shancang Li (2014)

https://www.researchgate.net/publication/270742269_Internet_of_Things_in_Industries_A_Survey

[19] Connected Car Architecture and Virtualization – Husein Dakroub, Adnan Shaout, Arafat Awajan (2016)

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

[20] IOT DIAGNOSTICS FOR CONNECTED CARS – Gheorghe Panga, Sorin Zamfir, Titus Constantin Balan, Ovidiu Popa (2016)

https://www.researchgate.net/publication/304561884_IOT_DIAGNOSTICS_FOR_CONNECTED_CARS

[21] THE CONCEPTS OF CONNECTED CAR AND INTERNET OF CARS AND THEIR IMPACT ON FUTURE PEOPLE MOBILITY – Agnieszka Szmelter-Jarosz (2017)

https://www.researchgate.net/publication/317958726_THE_CONCEPTS_OF_CONNECTED_CAR_AND_INTERNET_OF_CARS_AND_THEIR_IMPACT_ON_FUTURE_PEOPLE_MOBILITY

[22] Use of IoT Technology to Drive the Automotive Industry from Connected to Full Autonomous Vehicles – X. Krasniqi, E. Hajrizi (2016)

https://www.researchgate.net/publication/311853969_Use_of_IoT_Technology_to_Drive_the_Automotive_Industry_from_Connected_to_Full_Autonomous_Vehicles

[23] Role of Internet of Things in Smart Passenger Cars – G. Vidhya Krishnan, M. Valan Rajkumar, D. UmaKirthika

https://www.researchgate.net/publication/317287532_Role_of_Internet_of_Things_in_Smart_Passenger_Cars

[24] Securing the Internet of Automotive Things – Blackberry (2018)

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-cybersecurity-iot-auto-industry.pdf