Livre blanc

Les véhicules connectés à l'aune des cyberattaques

orange Business

bca expertise

Sommaire

Avant-propos

Savez-vous que d'ici 2025, 85% des véhicules neufs seront connectés[1] ?

Tous les véhicules sont devenus des objets connectés et communicants. De ce fait, ils peuvent faire l'objet d'attaques cyber ou être impliqués dans des sinistres dont la causalité et la responsabilité appellent à de nouveaux périmètres et modalités d'investigation. Cette tendance de fond s'amplifie avec l'intégration de plus en plus répandue de technologies sophistiquées d'autonomisation de la conduite basées sur l'intelligence artificielle et des capteurs toujours plus nombreux et toujours plus intelligents. Cet état de fait, ainsi que les projets des constructeurs de véhicules génèrent des impacts sur l'ensemble des acteurs de la mobilité notamment sur l'expert automobile et plus globalement sur la protection des données et la gestion des risques associés aux véhicules.

Par ailleurs, ce sujet se trouve à la croisée de multiples domaines technologiques et réglementaires : l'innovation autour des véhicules connectés avec la numérisation qui avance rapidement dans le secteur ; la nécessité pour les constructeurs de trouver de nouveaux gisements de valeur ; la digitalisation à l'œuvre chez les fournisseurs de services ; une composante télécom car les véhicules récents sont nativement connectés.

Dans cette première édition du Livre Blanc, véritable panorama et état de l'art à visée pédagogique, vous trouverez :

- Une synthèse des constats et défis du risque cyber dans le domaine automobile ;
- Le contexte réglementaire pour les véhicules connectés, qui évolue face aux cyber menaces ;
- Une description des menaces sur les métiers de l'automobile.

Les évolutions technologiques liées aux véhicules connectés provoquent un certain enthousiasme qui parfois brouille la limite entre réalité et fantasme. Il s'agira de déterminer quelle part de réalité et quelle part de science-fiction se trouvent au cœur de ce sujet.

[1] IHS Automative https://autotechinsight.ihsmarkit.com/shop/product/5003189/2020-connected-car-industry-trends-autoteq5g-presentation

Les auteurs

Antoine Jove, BCA Expertise

Directeur Général de BCA Expertise

BCA Expertise est le leader de l'expertise automobile en France pour tous types de véhicules. Chaque année, grâce à ses 1500 collaborateurs et collaboratrices, BCA Expertise réalise un million d'expertises (automobiles, deux roues, poids lourds autocars, matériel agricole). BCA expertise propose des prestations adaptées incluant des solutions innovantes mises à disposition de chaque client.

Saïd Zerdoumi, BCA Expertise

Expert en automobile.

Il est spécialiste national dans les nouvelles technologies et la recherche de responsabilités.

David Kernanec, Orange Consulting

Senior manager, secteur smart cities et industries

Orange Consulting est la branche conseil d'Orange Business. Le cabinet accompagne la transformation digitale des entreprises, des acteurs publics et des territoires, en France et à l'international.

Guillaume Martin, Orange Consulting

Consultant

Il est consultant au sein du secteur public d'Orange Consulting.

Chapitre 1

« Auto-mobiles » : les voitures sont-elles devenues des smartphones ?

Chapitre 1 :

« Auto-mobiles » : les voitures sont-elles devenues des smartphones ?

1. Les véhicules sont devenus des objets connectés

Les véhicules sont devenus par leur fonctionnement, leur utilisation, leur essence, leurs applications, des objets connectés. Cette connectivité se traduit par une production croissante de données. Le marché de la monétisation des données automobiles est en pleine expansion. Il pourrait atteindre à l'horizon 2030, entre 250 et 400 milliards de dollars à condition qu'il y ait une libéralisation de la data[2].

+ 25 %

de croissance annuelle du parc mondial de véhicules connectés depuis 2018

1.1. Un fort potentiel de croissance

Il existe donc un potentiel de croissance impressionnant du secteur des véhicules connectés en Europe et plus particulièrement en France. D'après l'étude de Fortune Business Insights, le marché dans son ensemble a atteint en 2023 une valeur de 30.44 milliards de dollars avec un taux de croissance annuel de 7%. Le marché européen des voitures connectées est aux alentours de 17 milliards de dollars avec un taux de croissance annuel de 3%. Quant aux camions connectés, le marché suit une tendance similaire avec un taux de croissance annuel de 12% pour atteindre 13 milliards de dollars.

En outre, en observant les estimations à l'échelle mondiale, le marché des voitures connectées devrait atteindre 142.49 milliards de dollars en 2026 avec un taux de croissance annuel de 16%. Ces différents chiffres et estimations illustrent le poids considérable de cette industrie, en particulier pour les constructeurs automobiles.

700

millions de voitures connectées en 2025

Les clients français font partie des principaux consommateurs de services connectés en Europe avec un parc de véhicules connectés estimé à 10,7 millions de véhicules en 2024.

[2] Tous les chiffres de ce paragraphe sont issus de l'Etude KPMG 2023, monétisation des donnés automobiles, quelles opportunités autour de la libéralisation de l'accès à la donnée ?

1.2. Définition et typologie des véhicules connectés

Un véhicule connecté est un véhicule qui échange, c'est-à-dire qu'il émet et reçoit via différents canaux et protocoles des données avec son écosystème :

- La plateforme du constructeur ;
- Internet ;
- Les applications correspondantes.

Ceci pour répondre à des objectifs de sécurité (entretien, maintenance), d'optimisation de la conduite et de propositions d'offres commerciales. Il intègre des systèmes de connectivité sans fil qui lui permettent de collecter des données qu'il peut utiliser et exploiter par la suite. Les données collectées par le véhicule sont nombreuses et variées. Il existe des données qui sont liées au pilotage (géolocalisation, information sur la distance avec un autre véhicule) et d'autres qui concernent la vie à bord via des applications pour la musique stockée ou encore le visionnage de films.

Sur décision de l'Union Européenne, tous les véhicules neufs doivent être connectés afin de pouvoir passer automatiquement un appel d'urgence en cas d'accident : il s'agit du système eCall. Depuis 2015, le Parlement européen a rendu obligatoire l'équipement par les constructeurs de tous leurs nouveaux modèles de véhicules du système eCall.

Bénéfices attendus

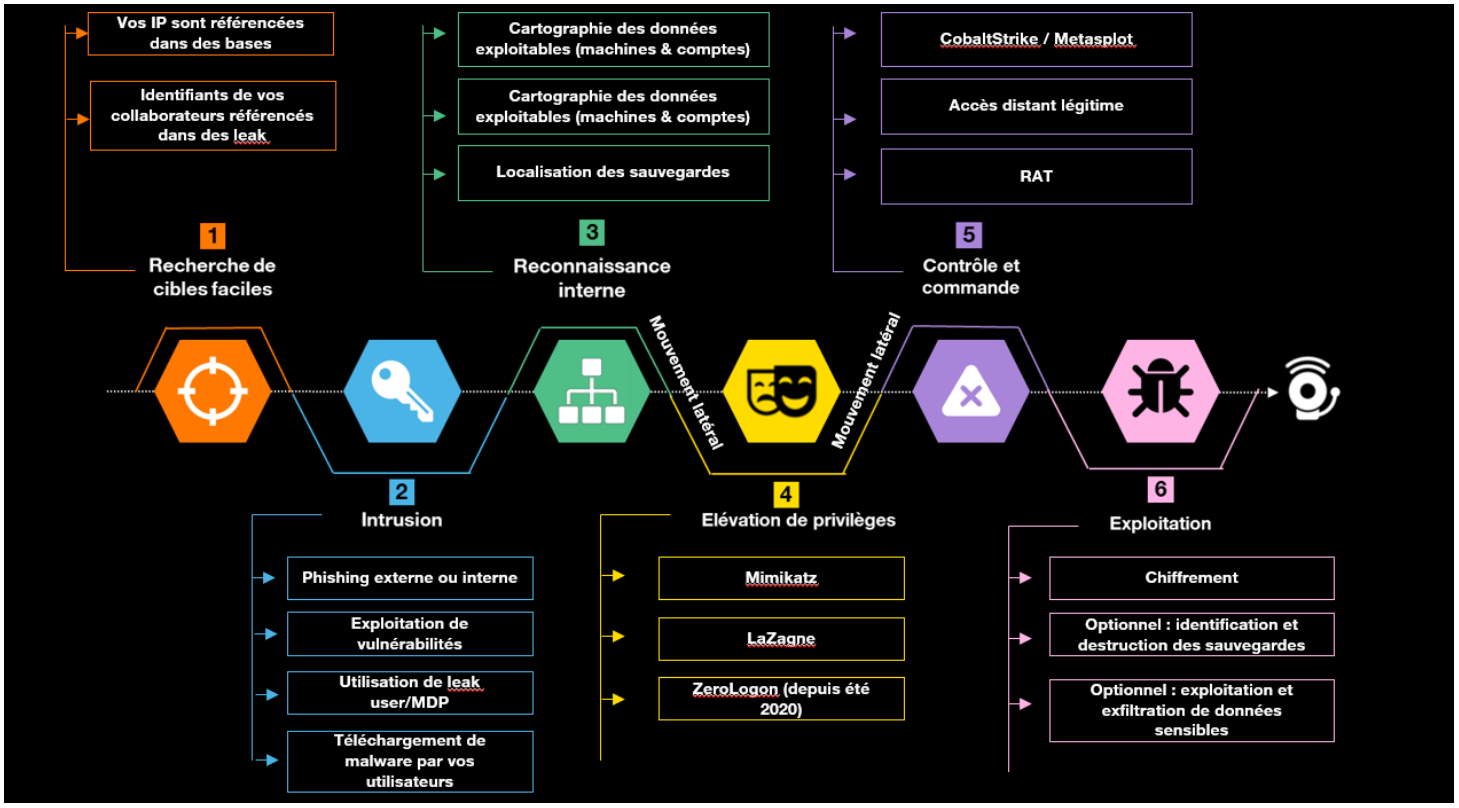
On attend plusieurs bénéfices de l'utilisation de véhicules connectés :

- Davantage de sécurité et de confort (amélioration de la sécurité routière, réduction du stress et de la fatigue, gain de temps pour d'autres tâches) ;
- Une réelle mobilité intelligente (optimisation des temps de trajet, meilleure exploitation de l'infrastructure routière et une réponse adaptée aux nouveaux besoins de mobilité).

Les connexions établies depuis le smartphone du conducteur passeront progressivement via l'électronique du tableau de bord du véhicule qui sera directement connecté.

Comme l'ensemble des objets connectés, les véhicules sont et seront confrontés aux cyberattaques. De nombreuses techniques existent déjà et ne se limitent pas au secteur auto.

Figure 1 : les techniques utilisées par les cyber attaquants [3]



[3] Source : Webinar Orange Cyberdefense, Protégez nos citoyens, protégez vos usages digitaux, https://www.youtube.com/watch?v=tOYB0ai0ekA

La technologie des véhicules connectés est protéiforme

Le Véhicule à Véhicule (V2V)

Le V2V est une technologie intelligente qui permet l'échange de données d'un véhicule à un autre. L'objectif de son usage est de réduire les embouteillages en villes et les accidents qui ne sont pas liés aux drogues et alcools. Elle utilise des communications qui sont à courte portée. Cela permet aux véhicules connectés d'avoir accès aux informations des autres véhicules situés dans l'environnement du véhicule connecté, tels que la vitesse, la circulation ou encore les états des routes.

Exemples :
Les détecteurs d'angles morts, les régulateurs de vitesse et les systèmes de freinages d'urgence.

Le Véhicule à Infrastructure (V2I)

Le V2I est une technologie qui permet de transmettre des données concernant les situations des véhicules connectés à une signalétique intelligente. En d'autres termes, cela permet de communiquer des données qui relèvent par exemple des informations du trafic et des embouteillages. Ces données permettent de prévenir les conducteurs des véhicules connectés et les alertent des éventuels dangers et situations du trafic. Cela permet d'améliorer la sécurité et de proposer une aide aux conducteurs pour l'évaluation de la circulation.

Exemples :
Les systèmes généralisés d'alertes, les conditions particulières de circulation et les limitations spécifiques de vitesse.

Le Véhicule à Tout (V2X)

Le V2X est une technologie qui permet une communication perpétuelle entre les véhicules et leur environnement. Dès lors, chaque véhicule disposant de cette technologie peut communiquer avec les autres et les infrastructures connectées. (V2X). Le V2X comprend aussi bien le V2V et le V2I.
L'environnement peut désigner :

- Les autres véhicules, on parle de V2V ;
- L'infrastructure, on parle de V2I ;
- Les piétons, on parle de V2P ;
- Le réseau de téléphonie mobile, on parle V2N.

Exemples :
Les notifications sur les comportements de conduite, sur les embouteillages à proximité du véhicule connecté.

Autres typologies existantes

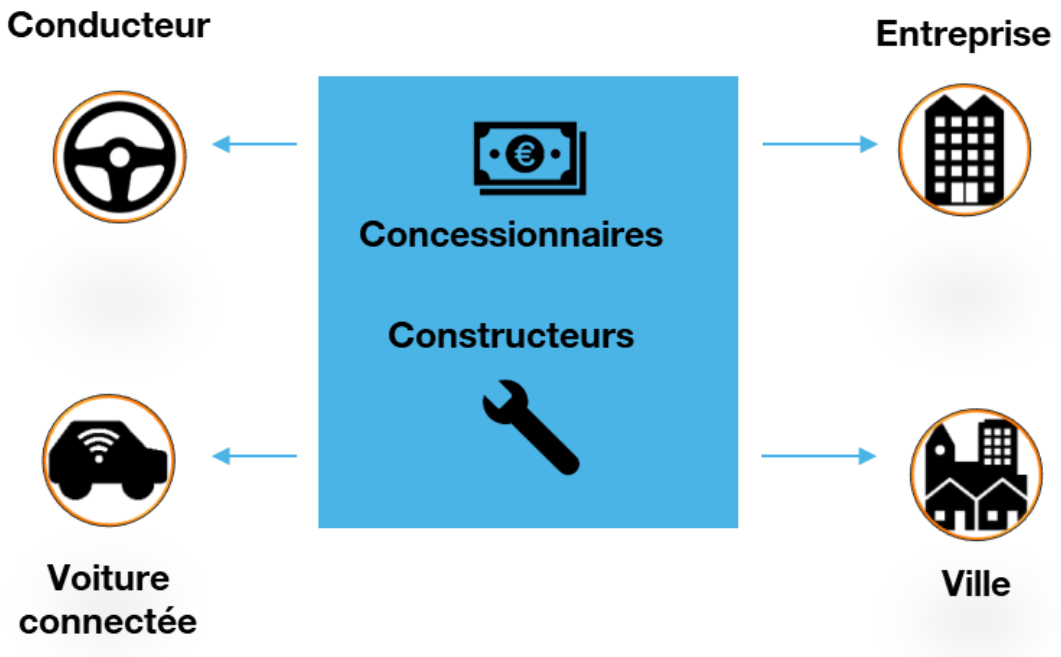
Véhicule to Grid (V2G)	Utilisation des batteries des véhicules électriques comme source d'énergie dans un réseau électrique.
Véhicule à réseau (V2N)	Communication de véhicule à véhicule à partir des réseaux téléphoniques comme le LTE.
Brain to Vehicle (B2V)	Connexion du cerveau d'un conducteur à son véhicule. Non exploité actuellement.

Il existe aussi la connectivité au service de :

- L'acte de conduite (environnement de conduite) ;
- L'efficience du déplacement (environnement de conduite) ;
- Potentiel de mobilité (l'accès au moyen de mobilité).

À travers toutes ces connectivités, le véhicule se présente comme étant serviciel pour le conducteur mais également pour son environnement.

Modélisation des flux de données liés au véhicule connecté



La connectivité, pour quoi faire ?

L'échange de données entre le véhicule et son environnement permet de développer de nouveaux services.

1. Sécurité

Le véhicule connecté reçoit des informations sur son environnement (état de la route, problèmes de visibilité, présence d'objets sur la chaussée). Il peut émettre des signaux de détresse en cas d'accident. La connectivité des véhicules permet de développer des fonctions d'aide qui vont améliorer la sécurité au sein du véhicule connecté et en dehors (aide au dépassement, aide à l'évitement, freinage en cas d'obstacle masqué…).

2. Offres commerciales

Les données remontées d'un véhicule connecté vers des serveurs vont être à l'origine de nombreux services comme le changement des pneus, la programmation d'entretiens ou encore la maintenance prédictive.

3. Optimisation de la conduite

Les données du véhicule connecté permettent de rendre compte de la réalité sur la route. Ainsi, cela permet de prendre en compte l'état de la circulation, d'améliorer la dynamique de la conduite et d'éviter les ralentissements et bouchons.

4. Un environnement plus coordonné

La récolte et le partage de données captées par chaque véhicule connecté permettent d'améliorer la coordination entre les véhicules au niveau des voies et de leur occupation.

1.3. De l'informatique embarquée aux véhicules autonomes électriques : 40 années de disruptions technologiques continues

Les véhicules connectés sont l'illustration de dizaines d'années de disruptions technologiques continues dans le marché de l'automobile. En effet, la carte Sim, l'Internet des Objets (IoT), les réseaux cellulaires impactent l'évolution des véhicules connectés.
De nombreux constructeurs émergent comme Tesla et JAC (constructeur auto chinois), jouant un rôle prépondérant sur le marché du véhicule connecté. Les acteurs publics sont également présents en participant à la réglementation du marché. Dès lors, chaque véhicule sera équipé, quelle que soit sa motorisation, d'un boîtier, d'un micro et d'un haut-parleur déclenchant automatiquement un appel d'urgence en cas d'accident.

De nos jours, le véhicule est devenu un « smartphone sur roues » avec des applications tierces qui communiquent avec des entreprises comme Waze et Apple.
Dans la plupart des cas, le constructeur automobile n'est pas dans ce cycle de communication.

Désormais, le véhicule donne plus d'informations qu'un smartphone de base car il communique des informations telles que la vitesse, les conditions de route, des informations sur le conducteur. Alors qu'un ordinateur dispose d'un seul système d'exploitation pour faire marcher tous ses logiciels, une voiture dispose pour chaque fonction d'une carte spécifique composée d'un processeur embarquant un logiciel qui va permettre d'exécuter cette fonction.

Les véhicules connectés ont donc de plus en plus de fonctionnalités. Cela se traduit par plus de puces embarquées, plus de connexions entre elles et plus de données produites. Des données supplémentaires sont intégrées par les systèmes multimédias pour prendre en compte le fait qu'il s'agisse d'un véhicule (l'ajustement du volume sonore en fonction de la vitesse en est un exemple).

Nous pouvons distinguer deux environnements distincts.

1. L'environnement type avec du multimédia : les personnes téléchargent leurs applications. Il s'agit d'un smartphone mis dans une voiture.
2. Un environnement plus moderne, caractérisé par une plus grande maîtrise des systèmes propriétaires.

En laissant des entreprises comme Google et Apple gérer les applications, les constructeurs automobiles perdent la relation client. Néanmoins, cela leur permet de réduire et maîtriser leur coût et de faciliter la gestion des applications (l'intégration de celles-ci, les mises à jour, la correction de bugs).

L'impact de l'Intelligence Artificielle (IA)

En outre, l'avènement de l'Intelligence Artificielle dans les véhicules connectés n'est pas sans conséquences. Elle joue un rôle dans le partage des données et enrichit l'expérience utilisateur de nouveaux services. L'IA rend l'expérience utilisateur plus fluide, en gérant les interactions entre les différents modes de transports et propose une offre de transport la plus adaptée aux clients.

Si l'on se concentre sur les véhicules électriques, l'IA pourra signaler le lieu et le moment où les utilisateurs pourront recharger la batterie de leur véhicule. Cela permettra une meilleure optimisation de la batterie.

Comme ces divers exemples l'attestent, l'IA va révolutionner l'expérience des conducteurs avec une proposition de services personnalisés et en assistant le conducteur tout au long de l'utilisation de son véhicule.

1.4. Acteurs présents sur le marché des véhicules connectés

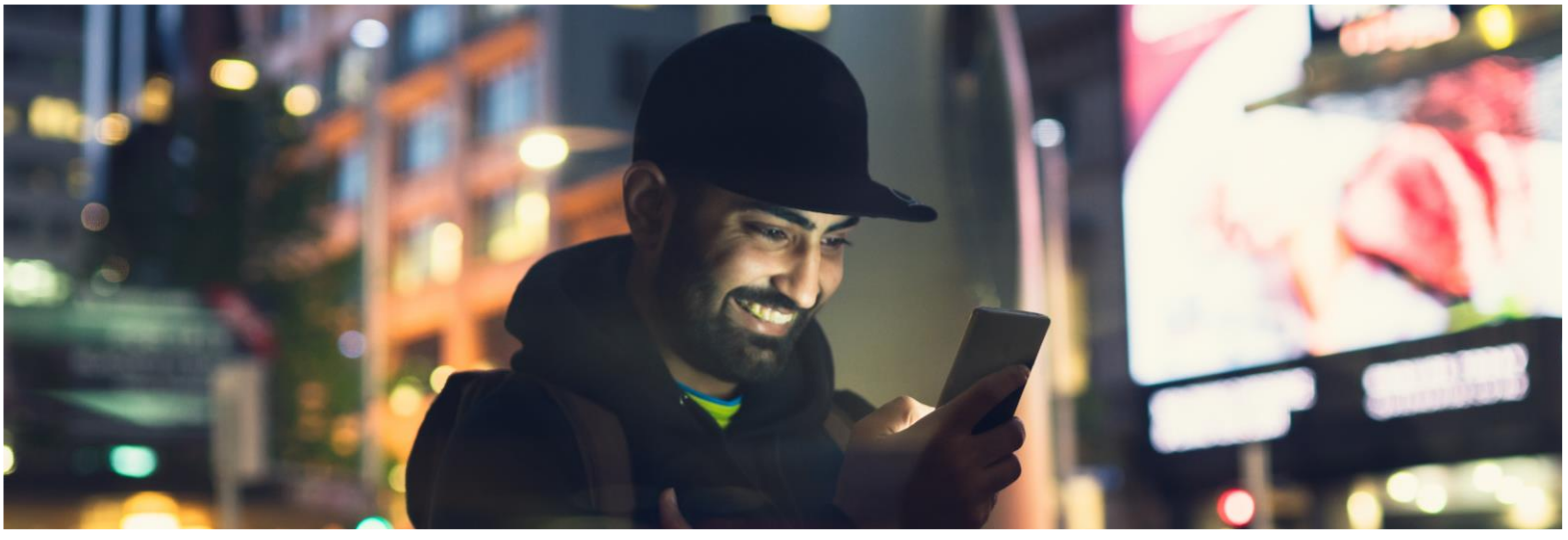
Le marché des véhicules connectés est composé des acteurs traditionnels de l'automobile tels que les constructeurs « historiques », les assureurs et les divers corps de métiers de ce secteur (les experts, les techniciens, les garagistes…).

Avec la connectivité des véhicules, de nouveaux acteurs ont émergé car ce marché présente des opportunités non négligeables. Ces différentes évolutions imposent une transformation des métiers des acteurs « historiques » (constructeurs, après-vente, entretien et réparation, assureurs, expert auto) et ouvrent l'accès à de nouveaux acteurs comme les GAFAM et de nombreuses start-up.

*

Chapitre 2

Mobilités connectées de demain : un enjeu pour la cité



Chapitre 2 :

Mobilités connectées de demain, un enjeu pour la cité

Les villes sont confrontées en permanence aux enjeux de mobilité. Elles sont le lieu où coexiste une multitude d'acteurs.

2.1 Les villes à l'épreuve de nouvelles mobilités urbaines : véhicules individuels, transports collectifs, logistique urbaine, électrification

Les villes sont confrontées à de nombreux enjeux pour bien gérer la mobilité multimodale :

- Interconnexion entre les différents modes de transport ;
- Optimisation des services publics ;
- Sécurité des différentes mobilités qui s'entrecroisent y compris les véhicules autonomes.

De plus, les transports collectifs passent de plus en plus en « énergie décarbonée ». Ainsi, l'enjeu commun de l'ensemble de cet écosystème est d'assurer l'authentification de ces communications numériques. Il est nécessaire que l'origine et la destination soient sûres et qu'il n'y ait pas de substitution d'identifiant qui compromette la sécurité de tous ces flux.

Avec le développement du véhicule électrique, on constate une croissance du nombre de bornes de recharges installées dans les villes et territoires. Ces bornes de recharges sont des nouvelles surfaces d'attaques. Celles-ci doivent se sécuriser contre des véhicules qui peuvent les attaquer mais il est également de la responsabilité du constructeur du véhicule de protéger son interface recharge contre un éventuel piratage d'une borne électrique.

La voiture est en diagnostic permanent dès qu'elle interagit avec son environnement

Dans un futur pas si lointain, les villes feront face au nombre croissant de véhicules autonomes. Ceux-ci cohabiteront avec des piétons, des cyclistes, n'étant pas forcément connectés. L'autonomisation sera assurée grâce au mobilier urbain, aux infrastructures qui se déploieront. En définitive, il est envisageable qu'à terme, les deux modes de communication (cellulaire et wifi) cohabitent. L'un ne peut fonctionner sans l'autre. En effet, un véhicule transmet l'information à un autre véhicule grâce à un protocole de communication sans fil.

Le véhicule connecté à son environnement

2.2 Les véhicules : des objets connectés au sein de l'internet des objets (IoT) pourvoyeurs de données

Les véhicules connectés fournissent de nombreuses données comme celles de roulage. D'un point de vue technique, les données de géolocalisation peuvent être collectées, à la demande du client. Les données sont collectées dans le but de garantir la conformité des véhicules. Dès lors, plus le constructeur a des informations sur la conduite, plus il peut affiner un business model pour vendre son véhicule. Cela permet l'amélioration en continu, le maintien en condition opérationnelle et prédictive.

Le panel des véhicules concernés ne se limite pas aux véhicules légers. Il y a également les poids lourds et les bus qui sont concernés par exemple. Plusieurs échanges ont eu lieu avec des régies de transports concernant « l'Alerting Safety ». Cela permet aux utilisateurs de partager rapidement des informations sur les risques de sécurité liés aux défauts des équipements techniques entre une multitude d'acteurs des transports (les fournisseurs de services, les acteurs de la logistique, les acteurs ferroviaires…).

2.3 Normes et règlements : quelles perspectives, quel agenda ?

Le développement majeur des véhicules connectés entraîne un cadre législatif en perpétuelle adaptation. Le véhicule connecté est au croisement de nombreuses réglementations (la loi d'orientation des mobilités de décembre 2019, le Cyber Security Act, la loi climat et résilience de 2021, le Data Act).

Cyber Resilience Act

Le Cyber Resilience Act vise à protéger l'ensemble des acteurs (consommateurs et entreprises) qui achètent et utilisent des produits ou des logiciels comportant un composant numérique. Ce texte a pour objectif de garantir un cadre d'exigences en matière de cybersécurité ; il instaure :

- La planification, la conception et le développement des produits, avec des obligations à respecter ;
- Les règles harmonisées lors de la mise sur le marché de produits ou de logiciels comportant un composant numérique ;
- L'obligation d'assurer le devoir de sollicitude pour l'ensemble du cycle de vie de ces produits.

Dès son entrée en vigueur, les parties prenantes disposeront de 24 mois pour s'adapter aux nouvelles exigences, à l'exception d'un délai de grâce plus limité de 12 mois en ce qui concerne l'obligation de déclaration imposée aux fabricants.

L'UN R 155

L'UN R155 vise à garantir la sécurité des véhicules routiers en établissant une norme pour leur cybersécurité. Ce texte aborde les exigences générales en matière de cybersécurité des véhicules.

- Il préconise l'intégration de la cybersécurité dans la conception et le développement des véhicules, pour garantir qu'ils puissent résister aux cyberattaques ;
- Il exige des tests réguliers de cybersécurité tout au long du cycle de vie du véhicule.

Cette réglementation met également l'accent sur la collaboration entre les constructeurs automobiles et leurs fournisseurs pour sécuriser les véhicules de manière exhaustive, et ce sur l'ensemble de leurs chaînes de valeur.

Dans le contexte de l'augmentation de connectivité dans les véhicules, les risques de cyberattaque et d'incidents augmentent. L'un des buts de la norme UNR 155 est d'imposer la détection et la gestion des incidents de sécurité pour les véhicules pendant toute leur durée de vie. Il s'agit plus largement d'un système de management de la cybersécurité des véhicules. Néanmoins, lorsqu'on parle de système d'information classique, on parle de composants qui ont une durée de vie de 5 ans maximum.

Un véhicule Cyber-sécurisé, jusqu'à la fin de sa vie : une exigence réglementaire

Un « club conformité »[4] a été mis en place par la CNIL qui a permis d'identifier trois scénarios de traitements de données selon que celles-ci sont :

- Stockées dans le véhicule sans retransmission ;
- Transmises afin de fournir des services complémentaires ;
- Collectées pour bénéficier ensuite d'actions automatiques (assistance à la conduite).

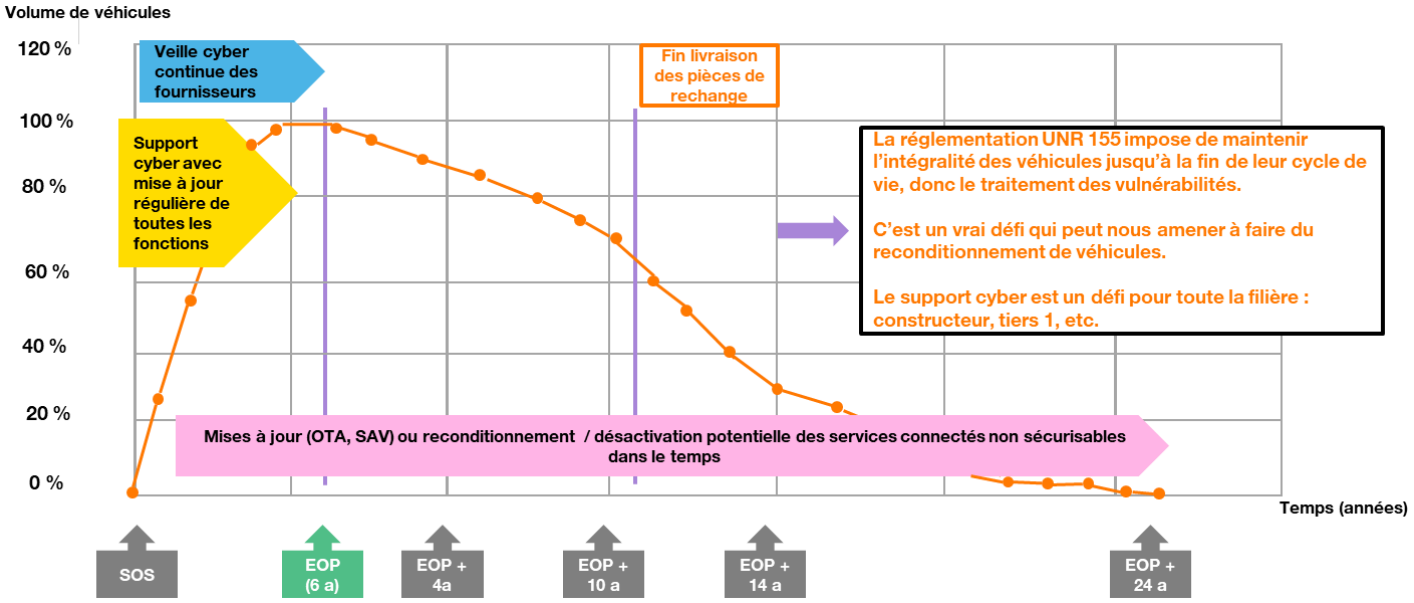
Le pack conformité aide à :

1. Déterminer qui est le responsable de traitement (le fournisseur de services, le constructeur) ;
2. Imposer la maîtrise concernant les paramétrages de protection des données et diverses mesures comme une possible anonymisation du chiffrement des canaux de transfert des données.

En résumé, ces lignes directrices soulignent plusieurs catégories de risques qui menacent les voitures connectées : la collecte excessive de données personnelles ainsi que leurs réutilisations, la difficulté de définir le responsable de traitement et la sécurité des données personnelles en général.

[4] Atelier du 21 Avril 2023, club conformité « Véhicule connecté et mobilité », CNIL

Figure 2 : évolution du support cybersécurité du véhicule[5]



[5] Source : les enjeux de la cybersécurité dans le domaine automobile (SIA : société des ingénieurs dans l'automobile)

Le cadre de la Loi d'orientation des Mobilités (2019)

Cette loi transforme en profondeur la politique des mobilités, avec un objectif simple : des transports du quotidien à la fois plus faciles, moins coûteux et plus propres. Le cadre de la LOM envisage l'hypothèse de la donnée appartenant au titulaire du certificat d'immatriculation, qui n'est pas toujours le conducteur. La loi vise le consommateur. Par consommateur, il est question de l'acheteur, qui est généralement le titulaire du certificat d'immatriculation et pas nécessairement le conducteur. Par exemple, lorsqu'on prête sa voiture à son conjoint, la loi vise la personne qui est propriétaire du véhicule et pas le conducteur qui l'utilise tous les jours.

En outre, il semble que les experts auto soient assez oubliés par la LOM. En effet, il y a toujours une différence entre les assureurs et les experts auto. Pour rappel, l'expert automobile est la seule personne autorisée à déterminer et chiffrer l'origine et le montant du dommage. (Articles R326 du code de la route).

L'article 32 de la LOM tempère cela puisqu'il donne à l'assureur un accès direct aux données du véhicule mais seulement aux fins d'indemnisation de la victime, les données devant déterminer qui (le conducteur) ou quoi (le système) avait la charge de la conduite du véhicule au moment de l'accident. Le consentement du propriétaire du véhicule, du conducteur ou du gardien du véhicule n'est pas demandé.

En revanche, l'expert auto doit avoir un accès non discriminatoire et le constructeur ne doit pas lui opposer un refus. En réalité, il n'est pas possible d'opposer un refus mais le processus peut être lourd et complexe. Par exemple, l'accès aux données peut être payant ou la demande de consentement assez longue à effectuer. En définitive, le cadre de la LOM fait entrave à la mission des experts automobile en alourdissant la procédure alors qu'il semblait possible de l'alléger.

Etat des lieux des réglementations existant au niveau international et national

		
Régulation du marché américain	**Union européenne**	**UN/WP 29 Forum mondial pour l'harmonisation des réglementations pour les véhicules**
NHTSA Lignes directrices, adaptées par auto-certification (basées sur la directive UN-R155)	UN-R155 Application du texte via la directive GSR2 (sécurité générale). Les pays membres appliquent la directive EU WTA NIS2 : protection de l'activité	Directive UN-R 155 sur la cybersécurité
		
Chine	**ISO TC 22/SC32/WG11- Cybersécurité**	**Niveau national, dans le monde**
Alignement avec l'Europe via la transposition de la directive UBT cyber	Norme ISO/SAE 21434	Royaume-Uni : adoptions des règles de l'UE Japon : adoption de la règle UN-R155 Corée : adoption de la règle UN-R155 pour l'auto-certification

Chapitre 3

La voiture connectée, une route pavée de défis et de risques

Chapitre 3 :

La voiture connectée, une route pavée de défis et de risques

Le véhicule connecté est confronté aux enjeux historiques du secteur de l'automobile mais aussi aux nouveaux défis liés à la connectivité des véhicules et à leur digitalisation.

3.1 Les différents risques : entre réalité et science-fiction

Flux de données

Ces véritables objets connectés demandent une sécurité accrue des flux de données émis et fournis. C'est pourquoi, il est nécessaire de sécuriser la gestion centralisée en base de données d'un véhicule connecté, le partage d'informations et potentiellement les unités de bord de route qui glanent les informations des objets en mouvement. Pour cela, il existe des clés de chiffrement et tout un système sécurisé. Ainsi, assurer son authentification permet de publier sa position, son état et le partager dans le cloud.

Protection des données

L'utilisation des données n'est pas sans poser quelques problèmes. Tout d'abord, il existe une réelle couverture de confidentialité. La protection des données au travers du RGPD est indispensable : il n'est pas possible de collecter des données sans consentement.

Données personnelles

En outre, il convient de rappeler que la donnée du véhicule, même purement technique (par exemple le numéro de série de la plaquette de frein) constitue de la donnée personnelle lorsqu'elle permet d'identifier a minima le titulaire du certificat d'immatriculation.

Tout ou presque peut être considéré comme de la donnée personnelle. La donnée personnelle est celle qui permet d'identifier ou de rendre identifiable directement ou indirectement une personne physique.
Ainsi, si on couple le numéro de série de la plaquette de frein avec d'autres informations et qu'il est possible de retrouver le titulaire du certificat d'immatriculation, alors cela pose un problème juridique.
Le propriétaire du véhicule n'est pas nécessairement celui qui conduit.

Protection du conducteur non-propriétaire

Mais qu'en est-il de la protection des données du conducteur non-propriétaire du véhicule ? En droit, la question du propriétaire des données personnelles n'est pas tranchée au niveau national, européen et international. Ces risques avérés sont liés au RGPD mais aussi aux risques de vol de

ces données. En revanche, des risques de voiture téléguidée reflètent pour le moment, davantage un film de science-fiction qu'une situation réelle.

3.2 L'augmentation des surfaces d'attaques

La surface d'attaque d'un véhicule est en train de se développer de manière exponentielle. Cela englobe non seulement le véhicule lui-même, mais aussi toutes les interactions qui l'entourent. Demain, les véhicules vont établir une communication avec leur environnement (V2X). Les cyberattaques peuvent également cibler le cloud, mettant ainsi en péril les données à long terme. Le véhicule devient un réservoir de données personnelles.

Data

La data augmente la surface de risques cyber, notamment en ce qui concerne la vie privée. Le développement des applications entraine plus de codage et donc plus de vulnérabilités. Plus complexes, les systèmes ultra-connectés deviennent plus difficiles à maîtriser. Pour atténuer ces risques, les fabricants doivent procéder à des mises à jour régulières. Auparavant, les véhicules étaient rappelés. Désormais, ils sont mis à jour à distance. De plus, l'identification précoce des scénarios et de leur occurrence et la détection des attaques connues peut contribuer à renforcer la sécurité des systèmes. La mise en place de bonnes pratiques d'hygiène en matière de sécurité peut également rendre plus difficiles les attaques basiques et freiner les attaques plus complexes.

Véhicule

L'accès physique au véhicule constitue une surface d'attaque complexe, potentiellement la plus dommageable. Il est essentiel de sécuriser tous les aspects du véhicule, en mettant l'accent sur les API, les applications et l'extérieur du véhicule. Les fabricants doivent prendre des mesures pour protéger leurs systèmes d'information afin de prévenir les attaques potentielles sur l'ensemble de leur parc de véhicules.

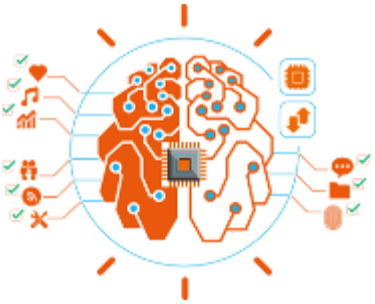
Face à l'explosion du nombre de surfaces d'attaques, le constructeur a la responsabilité de la sécurisation du véhicule et de ses composants électroniques et informatiques. Les assureurs ne se retournent pas nécessairement contre les constructeurs. Historiquement, il existe des exemples où les assureurs ont refusé d'assurer des véhicules, les estimant trop vulnérables. Cela est arrivé en Angleterre avec les Land Rover Evoque.

Législation

La législation va dans ce sens. La responsabilité n'est pas préétablie pour le moment. Il peut y avoir une co-responsabilité parmi les différents acteurs (fournisseur de software, constructeur automobile, fabricant…). Pour aller plus loin, dans le cadre d'un véhicule connecté, si celui-ci est piraté, alors la logique liminaire pourrait être de se retourner contre le constructeur. Quand le véhicule sera de plus en plus autonomisé, il y aura une bascule de responsabilité. La question de l'assurance sera soulevée. Il est possible d'envisager des défaillances d'un automatisme.

Groupes de réflexion

En outre, les constructeurs s'organisent. Il existe plusieurs groupes de travail de constructeurs dans le cadre de la PFA (Plateforme Automobile). Cela permet de travailler sur les aspects réglementaires et l'objectif est de partager des informations qui concernent le domaine de la cybersécurité et la réflexion autour de la responsabilité des acteurs du monde de l'auto.



Intelligence Artificielle

L'Intelligence Artificielle n'est pas exclue des risques de cyberattaques. Comme toute forme de code, l'IA est potentiellement attaquable. L'ajout de code supplémentaire peut créer une nouvelle surface d'attaque. Cependant, il est important de noter que cette surface d'attaque peut être spécifique et plus complexe à attaquer en raison de la structure de l'IA. Il est donc essentiel de mettre en place des mesures de sécurité appropriées pour protéger les systèmes d'IA contre les cyber menaces.

3.3 Améliorer la conformité et la sécurité des véhicules connectés

Le risque de la cyberattaque dans le véhicule connecté ne se limite pas seulement aux données du véhicule lui-même, mais s'étend à tout ce qui est connecté à celui-ci, y compris les données bancaires et les informations d'accès des smartphones, par exemple. Il est donc essentiel d'améliorer en permanence la conformité et la sécurité des véhicules connectés. Cela peut inclure des mesures telles que le cryptage des données, l'authentification forte, la surveillance en temps réel des systèmes et la mise à jour régulière des logiciels pour atténuer les risques de cyberattaque. La sécurité des véhicules connectés doit être une priorité pour garantir la protection des données sensibles et la confidentialité des utilisateurs.

La software République, dont Orange est un membre fondateur, mène une réflexion approfondie sur la sécurisation des véhicules connectés face aux cyberattaques. L'objectif de renseignement sur la menace est crucial pour anticiper et contrer les attaques potentielles. L'analyse des données générées par les véhicules peut fournir des informations précieuses pour détecter les signes de cyberattaques et prendre des mesures appropriées pour y faire face. Cette approche proactive est essentielle pour renforcer la sécurité des véhicules connectés et protéger les utilisateurs contre les menaces cybernétiques.

3.4 Un écosystème qui se développe

Le développement de l'écosystème des véhicules connectés entraîne des partenariats entre fournisseurs de services et constructeurs et la cybersécurité joue un rôle de plus en plus important dans le secteur automobile. La cybersécurité a un double rôle :

- D'une part, protéger tout au long de la chaîne de valeur ;
- D'autre part, permettre d'exploiter le potentiel offert par la connectivité. Elle est d'abord liée à la sécurité du véhicule connecté lui-même, puis elle vise à protéger le conducteur et les utilisateurs du véhicule.

La cybersécurité garantit la protection des données personnelles, améliore l'expérience utilisateur et établit un cadre de confiance. Il est essentiel de mettre en place des mesures de cybersécurité robustes pour prévenir les cyberattaques et assurer la sécurité et la confidentialité des utilisateurs dans l'écosystème des véhicules connectés.

La réduction de la vulnérabilité des véhicules est un défi constant pour les constructeurs. La connectivité et la digitalisation accrue des véhicules ont introduit de nouveaux risques, mais il est essentiel de minimiser ces vulnérabilités pour éviter toute exploitation par des pirates potentiels. La vulnérabilité d'un véhicule connecté est directement liée à la vulnérabilité du conducteur et du propriétaire. Par exemple, les capteurs, les données collectées et les applications tierces peuvent contenir des informations sensibles telles que les données bancaires, l'identité ou la religion du conducteur. Il est donc primordial de mettre en place des mesures de sécurité robustes pour protéger ces informations et garantir la confidentialité et la sécurité des utilisateurs dans l'écosystème des véhicules connectés.

L'étude récente de la fondation Mozilla[6] met en évidence des préoccupations légitimes concernant la confidentialité des données collectées et exploitées par les voitures connectées. Il est préoccupant de constater qu'aucun des 25 modèles de véhicules étudiés ne répond aux enjeux de confidentialité définis par la fondation Mozilla. La collecte d'informations sur les utilisateurs de véhicules connectés par les constructeurs automobiles soulève des questions sur la protection de la vie privée. La possibilité de partager des informations avec des fournisseurs de services, des courtiers en données et autres, ainsi que la vente de données personnelles par certains constructeurs, soulèvent des inquiétudes quant à l'utilisation et à la sécurité de ces informations sensibles, telles que l'origine ethnique, les croyances religieuses ou l'orientation sexuelle. Les utilisateurs ont la possibilité de se désengager de la collecte de données, mais il est préoccupant de constater que cela peut avoir des conséquences sur leur expérience utilisateur, voire rendre le véhicule inopérant, comme mentionné dans l'exemple cité.

Il est essentiel que les constructeurs automobiles prennent des mesures pour garantir la confidentialité des données personnelles des utilisateurs, respecter leur vie privée et offrir des options claires et transparentes en matière de collecte et d'utilisation des données. La protection de la vie privée des utilisateurs doit être une priorité absolue dans le développement et l'utilisation des véhicules connectés.

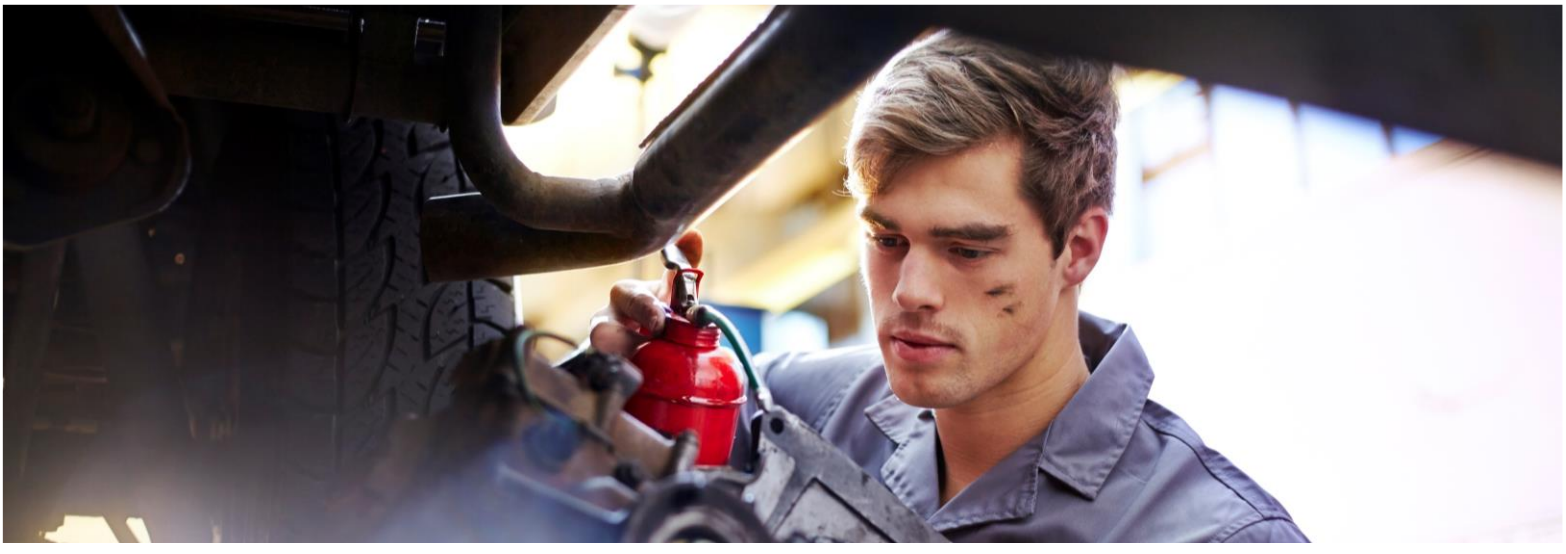
X 7

Multiplication du nombre de cyber incidents ciblant le parc automobile entre 2026 et 2019. (Upstream Security Global Automotive Cybersecurity Report)

[6] Source : Constructeurs automobiles : arrêtez de recueillir massivement nos données ! (mozilla.org)

Chapitre 4

Une connectivité accrue : quels impacts sur l’écosystème auto ?



Chapitre 4 :

Une connectivité accrue, quels impacts sur l'écosystème auto ?

L'arrivée de nouvelles technologies et problématiques technologiques a poussé et poussera le secteur auto à faire évoluer son fonctionnement et sa stratégie commerciale. Les risques cyber amenés à être de plus en plus présents dans ce secteur peuvent modifier les pratiques.

4. 1 Les constructeurs automobiles s'emparent du sujet

Les organisations de constructeurs ont progressivement mis en place des gouvernances cyber pour faire face aux risques. Elles permettent de développer des pratiques de sécurité évolutives et de mener de nouvelles analyses de risques pour anticiper les menaces. Il est également important de prendre en compte les différents profils d'attaquants potentiels, tels que les voleurs de voitures et les réseaux criminels. Les utilisateurs eux-mêmes peuvent devenir des attaquants potentiels, notamment lorsqu'ils cherchent à modifier leur voiture pour éviter de se rendre dans un garage. Cette évolution des profils d'attaquants nécessite une réflexion approfondie sur la sécurité des véhicules et la manière de prévenir les manipulations non autorisées tout en respectant les besoins et les préférences des utilisateurs.

100 Millions

Nombre de lignes de code dans un véhicule connecté

1 milliard

Nombre de lignes de code à l'horizon 2030 selon les constructeurs

Selon l'INRIA [7], d'ici quelques années, le logiciel représentera plus de la moitié des coûts de développement du véhicule et le logiciel embarqué comptera sans doute pour la majeure partie de sa valeur ajoutée. Grâce aux masses de données collectées via les véhicules connectés, les constructeurs pourront améliorer la conception des voitures et développer de nouvelles activités en créant de nouveaux services.

[7] Source : véhicules autonomes et connectés : les défis actuels et les voies de recherche, INRIA

Dans un autre domaine, au niveau Européen, la recherche de responsabilité en accidentologie ou plus généralement pour exercer des recours revêt une importance grandissante. Un autre type de mission confié à l'expert en automobile concerne la vérification de la nature du risque, afin d'aider l'assureur à bien l'appréhender. Dans le même esprit, dans le cadre d'un dossier de protection juridique ou de panne mécanique, l'expert en automobile devra identifier la source du dysfonctionnement et déterminer s'il s'agit d'une cyberattaque. Néanmoins, l'émergence de ces marchés dépend de la structuration d'une nouvelle offre assurantielle en parallèle de la technologie (l'assurance de données véhicule) et de l'évolution réglementaire (niveau d'autonomie des véhicules autonomes autorisé, accès à la boîte noire).

Dans l'Union européenne, la nouvelle réglementation sur la cybersécurité (UNECE WP 29/R 155) adoptée dès juin 2020, est obligatoire pour tous les nouveaux types de véhicules à partir de juillet 2022 et deviendra obligatoire pour tous les nouveaux véhicules produits à partir de juillet 2024. Elle impose aux constructeurs et équipementiers automobiles d'intégrer des activités de cyber sécurité tout au long de la chaîne de valeur, dès la conception et jusqu'au recyclage. L'expert en automobile de demain devra s'intégrer à ce nouvel écosystème sous peine d'être décroché techniquement par manque d'accès à la connaissance.

A la suite de la transposition dans le droit français du règlement Européen 2019 / 2144, les pouvoirs publics vont être amenés à agréer des centres qui auront un accès aux données des boîtes noires embarquées dans les véhicules. Au-delà des opportunités d'être intégrés dans la filière de par leur rôle reconnu de tiers de confiance, la connaissance de ces technologies et l'accès sécurisé aux données des boîtes noires sont des conditions sine qua non au maintien du statut de l'expert en automobile.

4. 2 Les assureurs face aux cyberattaques des véhicules connectés : leur vision, leur posture et leur rôle

La vision du risque cyber des assureurs

1. **Opportunités liées à la révolution numérique**

La révolution numérique est porteuse de vastes opportunités mais aussi de risques, voire de menaces. Dès 2015, le cyber risque figure au 1er rang des risques technologiques identifiés dans le Panorama 2016 des risques globaux du Forum de Davos. Il est question d'un risque dont la présence, la fréquence en termes d'actes de malveillance et la complexité ne cessent de croître au fil des avancées technologiques, de l'interconnexion progressive des réseaux et maintenant des objets. Les entreprises tout comme les citoyens dépendent donc de la sécurité et de l'efficacité de leur système informatique.

2. **Risque cyber**

Lorsqu'on aborde le risque cyber, la malveillance apparaît comme le premier élément qui est pris en compte par les assureurs. Par malveillance, on peut évoquer le détournement d'un véhicule de son usage, sa prise de contrôle et son utilisation à mauvais escient dans le cadre d'une voiture bélier ou d'un attentat par exemple. La prise de contrôle d'un véhicule peut permettre de réclamer des rançons. Si cela doit se produire, il y a une grande probabilité pour que cela se fasse au travers du serveur du constructeur afin d'impacter plusieurs véhicules.

3. Prise en charge des rançons

La prise en charge des rançons varie en fonction des assureurs et des politiques très variées sur cette question. Chez certains assureurs, la prise en charge peut se faire jusqu'à 2 millions d'euros. La recommandation de l'Autorité de contrôle prudentiel et de résolution était de ne plus prendre en charge afin de ne pas encourager le phénomène. En effet, la France était l'un des pays les plus rançonnés car les individus payaient dans la plupart des cas. Ces cyber extorsions sont donc aujourd'hui une réalité. Il existe également le vandalisme ou le vol avec le risque d'immobilisation d'une flotte de véhicules. De nombreux scénarios sont imaginables.

Le risque cyber est déjà présent mais n'apparaît comme étant un sujet prioritaire car il n'a pas encore directement impacté les assureurs. Il est concevable de supputer des aléas et des risques mais ce n'est pas encore d'actualité pour la plupart des assureurs. Toutefois, il s'agit d'un sujet d'actualité fort qui s'ancre dans un temps long.

Néanmoins, il convient de souligner que de nombreuses administrations publiques et entreprises sont attaquées. Cela a pour conséquences des dommages matériels importants et des impacts sur la survie de certaines entreprises. Le besoin est donc réel et important. De plus, la difficulté réside dans la manière dont l'assureur agit. Il peut y avoir une volonté de l'assureur de protéger contre ces évènements mais cela peut avoir un impact majeur pour lui (risques ne pouvant être assurables par exemple). Les acteurs du marché sont donc encore très hésitants.

4. Pistes de solutions

Dès lors, il existe deux pistes de solutions. En effet, il est possible de considérer le risque d'un point de vue indemnitaire mais aussi d'un point de vue prévention et accompagnement. De nombreux acteurs se lancent dans des logiques de prévention avec des cadres de souscription qui demandent des règles basiques de bonne gestion informatique des parcs avant de pouvoir avoir accès à des garanties d'indemnités.

Aujourd'hui, il n'existe pas de sinistres couverts directement liés à la connectivité et sécurité des véhicules. Néanmoins, il est possible de demander des protections supplémentaires. L'offre cyber reste liée aux entreprises de type TPE/PME. Ces offres sur les risques cyber sont complètement indépendantes de l'automobile. De surcroît, pour certains assureurs, il existe un risque IT plutôt qu'un risque centré sur le véhicule. Le véhicule apparaît ainsi comme un objet comme un autre dans l'IoT.

En outre, le risque via l'intelligence artificielle apparaît comme lointain. Pour le moment, il n'est pas identifié. Les risques liés à l'intelligence artificielle arriveront avec le véhicule autonome. Lorsque les constructeurs auront avancé sur le sujet, que la législation et les infrastructures en Europe permettront de faire circuler les véhicules autonomes, les premiers accidents arriveront. C'est à ce moment que la question sera posée et qu'un travail sera effectué sur l'identification de ce risque.

Enfin, la réaction en cas de crise est très importante. Il y a un effort d'accompagnement juridique et technique pour sécuriser les entreprises et ensuite un volet indemnitaire et de réparations. Une contre mesure est nécessaire pour s'opposer à ces réseaux criminels étant

donné que les voitures disparaissent assez vite. Par exemple, dans les heures qui suivent un vol, les plaques d'immatriculation et caractéristiques sont changées. Les réseaux peuvent donc être redoutablement efficaces dans le but de maquiller, faire disparaître des voitures volées. En lanceurs d'alertes, en remontant la récurrence des modèles les plus « vulnérables » ou « convoités », les assureurs peuvent échanger avec les constructeurs automobiles afin de repérer ce qui est le plus fréquemment volé.

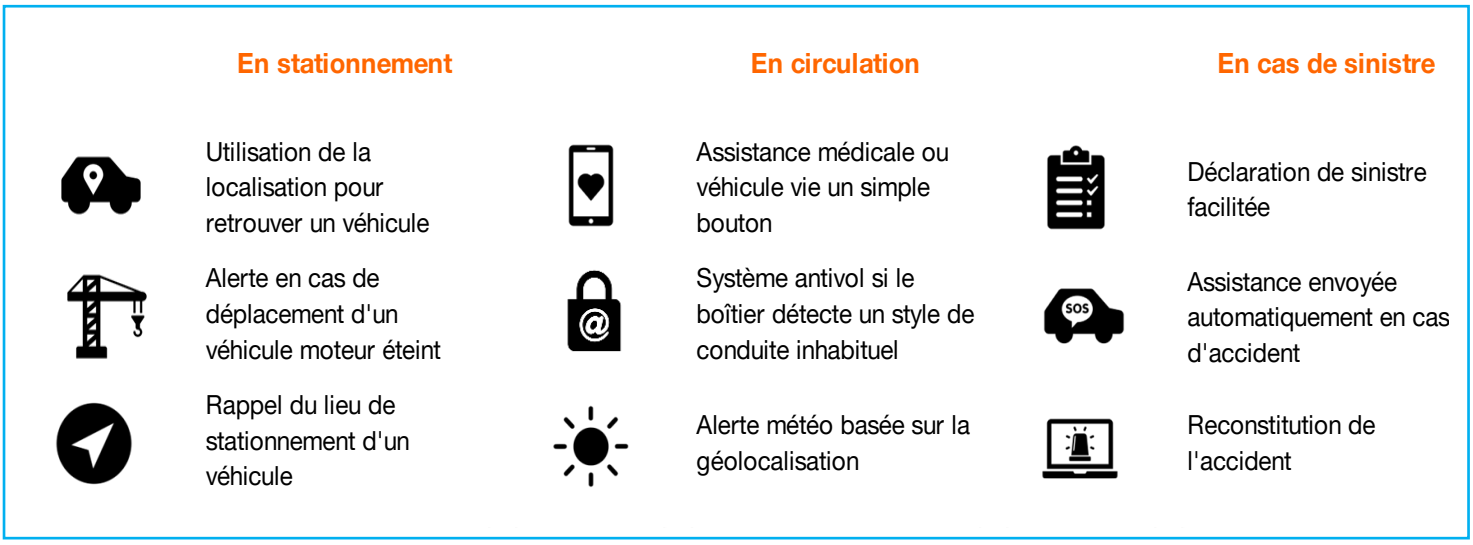
Encore une fois, se prémunir de tous les risques n'est pas possible mais une réaction efficace permet de pouvoir sécuriser au mieux les véhicules connectés. Certains sujets liés aux cyber-attaques sont regardés de très loin par la profession. De nombreux acteurs attendent d'avoir subi une attaque cyber pour pivoter et agir.

Ici, la question n'est pas de savoir si l'on va être piraté mais quand on va être piraté.

Les nouveaux services permis par les véhicules connectés : vers un nouveau rôle pour l'assureur ?

A la suite du développement continu de la connectivité des véhicules, les assureurs jouent un nouveau rôle et ne se limitent plus à payer les sinistres. Ils deviennent au fur et à mesure des partenaires de mobilité. Ils proposent de plus en plus des services comme l'amélioration de la prévention (à travers les données collectées par la voiture connectée), la mise en place d'un système d'alerte sur l'état du véhicule, une assistance médicale.

Figure 3 : quelques services possibles avec la connectivité des véhicules



La donnée : collecte, accès et partage

Les assureurs ne peuvent pas récolter les données des véhicules connectés sans consentement. Le consentement du client est nécessaire au même titre que la finalité d'utilisation des données. Ce consentement est explicité au moment de la souscription du contrat et le client peut le retirer à tout moment.

La donnée est l'élément clé et son accès au cœur des préoccupations des différents acteurs de l'écosystème. Comme nous l'avons vu précédemment, les obligations du RGPD s'appliquent aux véhicules connectés.

France Assureurs définit huit principes essentiels pour le traitement de la donnée

1. L'ensemble des données, quelle que soit leur nature et sous réserve du consentement de l'utilisateur, doit être accessible de façon équitable à toutes les parties prenantes. Cela implique une transparence complète sur les données disponibles.

2. Les choix des utilisateurs du véhicule doivent être rendus réellement effectifs grâce à des modalités fluides et réversibles du recueil de leur consentement.

3. Plusieurs modalités d'accès doivent être prévues afin de préserver la neutralité technologique et d'éviter les verrouillages démarchés.

4. Ces accès doivent s'opérer dans les conditions techniques et économiques identiques pour tous les acteurs, du constructeur à l'opérateur indépendant.

5. L'accès aux données et aux ressources du véhicule doit être direct et, si nécessaire en temps réel.

6. Les parties prenantes doivent, dans le cadre d'un besoin métier, pouvoir accéder aux données essentielles contenues au niveau même des calculateurs.

7. Une approche intersectorielle et coopérative doit permettre de concourir à un objectif partagé de sécurité et cybersécurité des véhicules.

8. Une réglementation européenne est primordiale, notamment en termes de standards, afin d'asseoir ces principes et une gouvernance neutre.

Il y a un enjeu à rendre les données accessibles et lisibles. Les prises OBD ont facilité les choses. L'interprétation des données est informative. C'est l'appréciation des données qui peut poser un problème.

Les données sont caractérisées par une réelle ambivalence, dans le sens où elles présentent à la fois des risques mais aussi des opportunités. Dès lors, le premier risque des données est économique, c'est-à-dire qu'elles soient un instrument de captation de la valeur au profit de ceux qui les détiennent et les gèrent (les constructeurs par exemple). Les constructeurs qui complexifient l'accès à la prise OBD au profit du passage obligé par les passerelles de sécurité (Gateway) imposant dès lors leur système de consultation des données uniquement à distance, sont hors la loi européenne. Les assureurs, équipementiers et d'autres acteurs considèrent que l'utilisation de la donnée doit être la plus fluide possible et ne pas être captée.

4.3 L'évolution du métier de réparateur à l'ère du numérique

L'ère du numérique représente une opportunité de développement pour les métiers de l'automobile. Le réparateur ne peut plus reconnecter les clés et réparer le véhicule comme avant. Il va y avoir de nouveaux métiers qui vont arriver dans les concessions autour de l'IA, de l'IT, de la data science. Tout le travail de mise en avant du véhicule comporte une série de données techniques qu'il est nécessaire d'expliquer au client final.

Plus il va y avoir de technologie, plus il va y avoir de l'attente au niveau humain.

Cette évolution passera par une formation des acteurs du secteur auto. Il s'agit de sujets de profils, de personnes dans les entreprises aptes à former et informer sur les nouvelles méthodes d'utilisation et de consommation de ces nouveaux véhicules. De plus, les risques évoluent avec les cyberattaques et de nouvelles pratiques de vols. Par exemple, lors d'un vol il n'y a plus de traces matérielles d'effractions.

Dès lors, il est nécessaire d'être doté d'outils spécifiques pour vérifier côté expertise. Pour définir s'il s'agit d'un vrai ou faux vol, il faut réaliser une expertise plus approfondie. La plupart des experts n'est pas formée à cette révolution qui change leur métier.

De nouvelles compétences nécessaires pour la réparation du véhicule électrique[8]

La réparation des batteries nécessite de mettre en place un processus, des conditions d'intervention et des formations totalement inédites pour les ateliers dédiés à la réparation. Il existe plusieurs activités techniques relatives à la maintenance préventive et corrective des batteries de véhicules électriques dont :

- La mise en sécurité du véhicule et de l'environnement de travail ;
- La vérification de l'intégrité physique et de la traçabilité de la batterie ;
- La mise en sécurité de la batterie ;
- Le développement d'opérations de diagnostic et de remplacement sur les composants électroniques et électriques ;
- Le calibrage des composants électroniques et électriques de la batterie d'un véhicule.

L'ensemble de ces activités illustre les évolutions pour les métiers du secteur auto en termes de bonne capacité d'interprétation de grandeurs physiques et dans la maîtrise de l'utilisation des équipements et des modes de diagnostic.

La transition digitale au cœur du secteur automobile et l'apparition de nouveaux risques comme les cyberattaques, apparaît comme étant synonyme de stratégie collaborative. Il est envisageable d'engager de nouveaux corps de métiers pour compléter les équipes et former davantage. Il est également possible de s'associer avec des entreprises d'autres domaines afin de proposer des prestations spécifiques.

Le développement de la connectivité et plus largement des nouvelles technologies, bien qu'elles bouleversent le cadre préexistant du secteur auto, permet aux acteurs automobiles de se diversifier, de développer de nouvelles offres, de se différencier dans un secteur très concurrentiel.

[8] Source : études de l'observatoire des métiers des services de l'automobile, Autofocus, octobre 2023

4.4 Les défis pour l'expert de demain

Face à tous ces enjeux, le métier de l'expert en automobile va être profondément transformé dans les années à venir, nécessitant de nouvelles compétences et de nouveaux outils. Les vulnérabilités logicielles déjà rencontrées illustrent les risques liés à cette avancée technologique des véhicules. Dans ce contexte, le rôle et les compétences de l'expert en automobile d'aujourd'hui tendent à être altérés bien que son positionnement reste le même.

La profession de l'expertise automobile est face à l'enjeu majeur de faire évoluer la qualification des experts, leur formation, les moyens numériques et techniques à leur disposition.
Par ailleurs, les compétences spécifiques en cybersécurité, data, analyse de logs et IA et la création d'outils d'analyse constituent des barrières à l'entrée et un défi de mise à niveau pour les experts en automobile.

1 vol sur 5 dans les voitures de nouvelle génération se fait avec une cyberattaque.

L'enjeu majeur pour les experts en automobile de demain est de parvenir à démontrer techniquement la réalité du vol, s'il s'agit bien d'une cyberattaque dit aussi, « vol à la souris ». Tracer une cyberattaque est actuellement une vraie difficulté technique, tant les constructeurs verrouillent l'accès aux données. Certaines marques vont même jusqu'à retirer les accès aux données à leur réseau de distribution à cause des normes RGPD. Avec une clé ou une carte de démarrage, il est possible d'avoir accès selon le modèle du véhicule, à de nombreuses données personnelles et circonstancielles.

Depuis le E-call, toutes les voitures sont équipées de carte Sim, vulnérables en cas de cyberattaques. Un autre défi concerne la remise en circulation des véhicules au terme d'une procédure « Véhicule endommagé », l'expert en automobile devant attester in fine que le véhicule est en état de circuler dans des conditions normales de sécurité au terme de l'article R327-2 du Code de la Route. Toute erreur dans un code source ou dans un logiciel devant être identifiée, pour qu'il soit en mesure de s'assurer notamment que l'ensemble des systèmes embarqués est bien opérationnel.

En bref

1. Le risque cyber existe aujourd'hui pour le secteur automobile mais deviendra un sujet incontournable dans les années à venir. C'est pourquoi la cybersécurité devient une priorité pour les industriels du transport et les acteurs du secteur.

2. Les solutions de cybersécurité existent mais devront être intégrées au processus de développement des véhicules. Que cela soit par des fonctions de firewall dans les interfaces avec les réseaux extérieurs, par la sécurisation des communications internes (entre les véhicules et les SI) par chiffrement et signature, par la sécurisation des calculateurs embarqués, de nombreuses solutions sont nécessaires tout au long du développement du véhicule.

3. Comme nous l'avons évoqué, cela ne se limite pas au véhicule mais à tout son environnement comportant des objets et infrastructures de plus en plus connectés.

4. Désormais, la voiture ne s'appuie plus seulement sur ses propres capteurs, mais étend sa perception à tous les éléments communicants de son environnement. Un écosystème autour de la connectivité 5G des véhicules est en train de se construire.

5. La généralisation de la conduite autonome n'est pas encore une réalité et nécessitera un réseau robuste et étendu. La 5G représente de manière substantielle l'avenir des véhicules autonomes. De nombreux acteurs, dont les assureurs, devront s'adapter à l'arrivée des véhicules autonomes et certains nouveaux risques pourraient avoir besoin d'être couverts tel que le piratage informatique des ordinateurs de bord ou le cyberterrorisme.

6. Néanmoins, le véhicule totalement autonome peut apparaître comme étant un fantasme et la crainte de l'absence de contrôle éloignée de toute réalité.

7. L'intelligence artificielle est de plus en plus présente dans la vie quotidienne et le secteur automobile ne fait pas exception. Le développement et l'autonomisation des véhicules connectés témoignent d'une certaine évolution de l'automobile. Cela va au-delà d'une simple intégration d'écrans tactiles dans l'habitacle du véhicule, l'industrie auto repense complètement sa conception des voitures. Elles ne seraient plus l'objet final en tant que tel mais plutôt de simples "terminaux" faisant partie d'un écosystème global d'appareils mobiles. De nouveaux services seront proposés, s'inscrivant dans la continuité des usages mobiles et s'éloignant progressivement de l'utilité initiale du véhicule.

+ 23 %

Estimation de la progression de la taille du marché des voitures autonomes entre 2024 et 2029, selon Mordor Intelligence.

Le marché devrait passer de 41 milliards de dollars à 114 milliards de dollars.

Glossaire

- **EDR**

Event Data Recorder. Dispositifs d'enregistrement installés sur les voitures. L'EDR permet de reconstituer ce qui s'est passé 5 secondes avant un crash. Il enregistre, durant quelques secondes, certaines données qui entourent un accident, en vue d'en comprendre les circonstances.

- **Ecall**

Système embarqué d'aide automatique fondé sur le 112, le numéro d'appel d'urgence unique européen.

- **DSSAD**

Data Storage System for Automated Driving. Enregistreur de l'état de délégation de conduite sur une longue période.

- **IoT**

Réseau d'objets et de terminaux équipés de capteurs (et d'autres technologies) leur permettant de transmettre et de recevoir des données entre eux et avec d'autres systèmes.

- **ISO (International Organization for Standardization)**

Organisation internationale de normalisation. L'AFNOR y représente la France.

- **OBD (prise)**

La prise diagnostic OBD permet d'accéder à un ensemble de données et est utilisée pour surveiller et diagnostiquer le fonctionnement du véhicule.

- **PFA**

Plateforme automobile qui rassemble la filière automobile en France. Elle définit et met en œuvre au nom de l'ensemble des partenaires (constructeurs, sous-traitants et acteurs de la mobilité), la stratégie de la filière en matière d'innovation, de compétitivité, d'emploi et compétences.

- **RGPD**

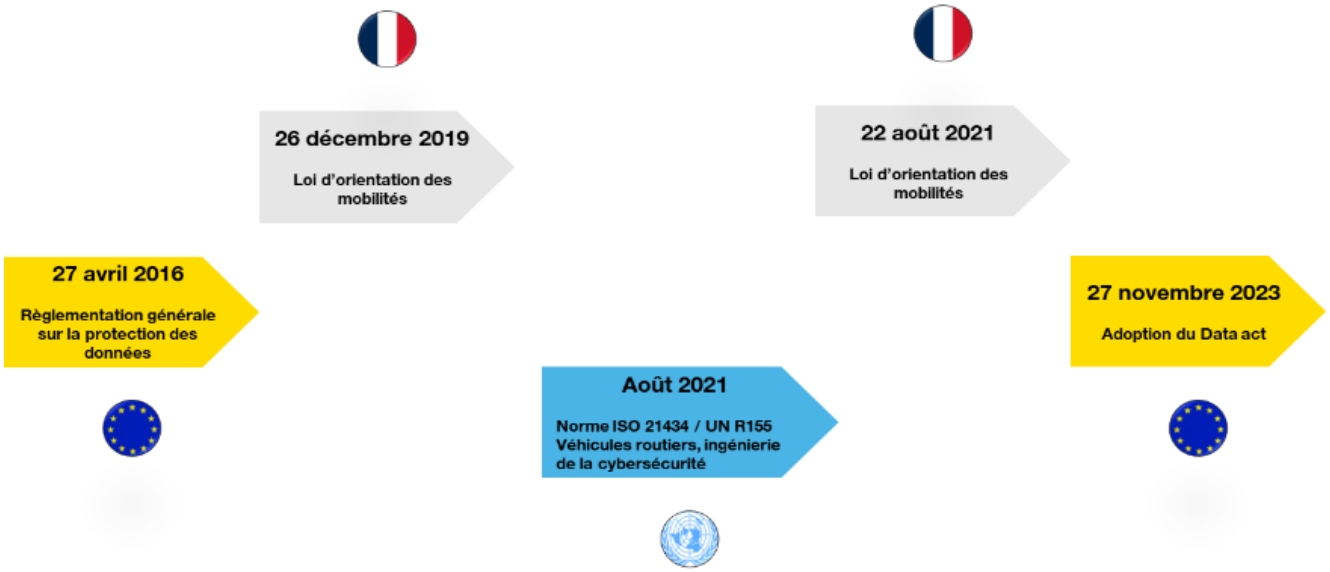
Le règlement sur la protection des données encadre le traitement des données personnelles sur le territoire de l'Union européenne.

- **VAC**

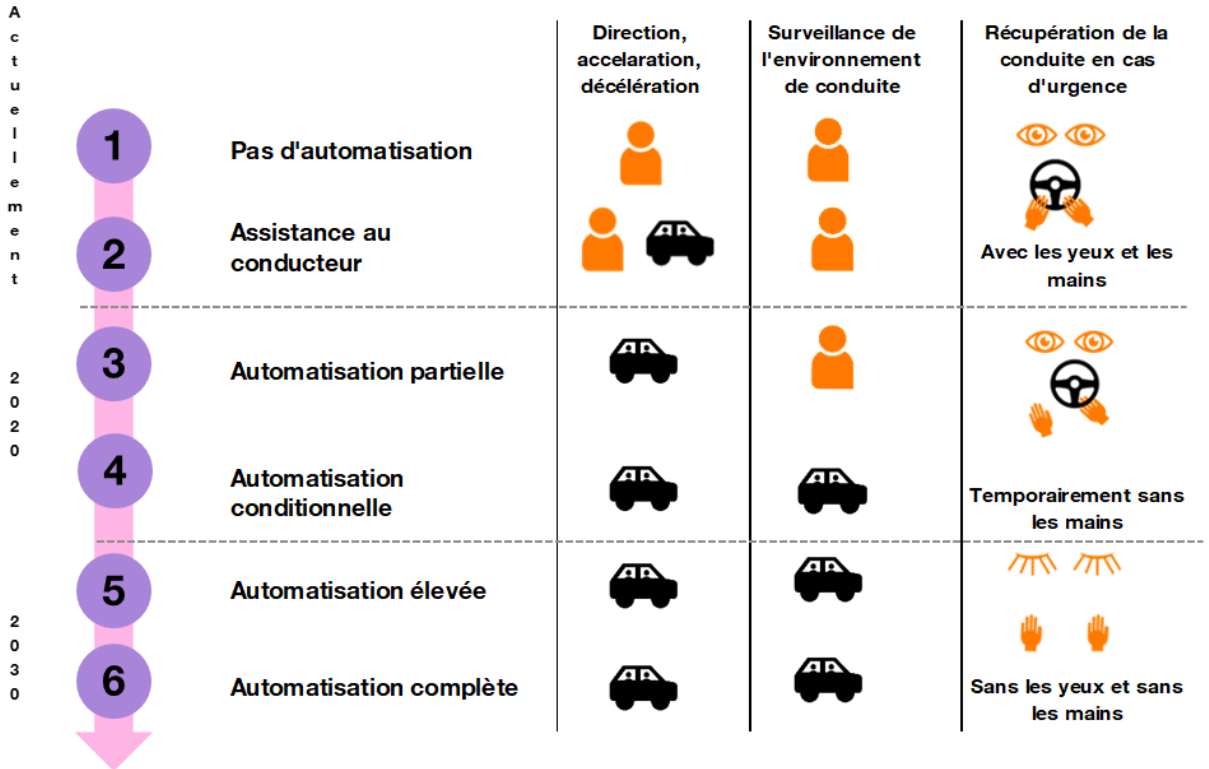
Véhicule se déplaçant de partiellement ou totalement autonome et connecté au sein de son environnement.

Lois et réglementations sur les voitures connectées

Dernières lois et réglementations sur les véhicules connectés



Les degrés d'autonomisation du véhicule[9]



Le 21 juillet 2022 un décret autorise la circulation des véhicules comportant un niveau 3 d'automatisation au 1er septembre 2022 en précisant que la responsabilité du constructeur sera engagée lorsque le mode conduite autonome est activé.

[9] Source : service de recherche du Parlement européen, Commission Européenne

Remerciements et contacts

Ce Livre Blanc est réalisé sous la direction d'Antoine Jove (BCA Expertise) et de David Kernanec (Orange Consulting).

Nos remerciements particuliers pour leur participation, leurs encouragements et précieux commentaires :

Juliette Berger, Directrice Achats Assurantiels, Axa France
Mickael Beurrier, Responsable opérationnel, Argos
Nuno Borges, Expert Conseil National, Generali
Eric Dequi, Expert Architecture électrique et Cybersécurité, Stellantis
Alexis de Schonen, Head of Partnerships, Axa France
Brice Duprieu, Directeur Innovation, Orange Cyberdefense
Florence Gagnepain, Industry and Connected Transport, Orange Innovation
Xavier Horent, Délégué Général, Mobilians
Patrick Jeanbart, Head of Connected Car, Orange Business
Benoît Leclair, Managing Director, Argos
Jean-Jacques Morisset, Manager Equipe Professional Services, OCEAN, Orange Business
Christophe Petrynka, Directeur, CESVI France
David Thévenot, Responsable Pôle Réseaux Auto, Groupe Covéa
Jacques Trassoudaine, Président de la FIEA
Barbara Tron, Directrice marketing et communication OCEAN, Orange Business

Nous tenons à remercier chaleureusement l'ensemble des collaborateurs et contributeurs de BCA Expertise et du Groupe Orange, dont :

Miriam Bouchebouba, Head of Operational Performance, BCA Expertise
Maimouna Diambang, Consultante Accélération Digitale, Orange Consulting
Daniel Gonçalves, Directeur Retail, Orange Consulting
Hélène Fétizon, Content Manager, Orange Business
Marie de Labeau, Brand Manager, Orange Cyberdefense
Julien Jouvrot, Directeur de l'expertise, BCA Expertise
Olivier Robert, Directeur de Territoire Sud, BCA Expertise

Antoine Jove, Directeur général adjoint, stratégie et développement, BCA Expertise Antoine.JOVE@bca.fr
David Kernanec, Senior Manager Smart Cities & Industries, Orange Consulting david.kernanec@orange.com
Guillaume Martin, Consultant Secteur Public, Orange Consulting guillaume4.martin@orange.com
Saïd Zerdoumi, Spécialiste national nouvelles technologies et recherche de responsabilités, BCA Expertise said.zerdoumi@bca.fr

BCA EXPERTISE S.A.S. au capital de 24 458 700 Euros - R.C.S Nanterre 489 139 436-
Siège Social : 14, rue Sarah Bernhardt - CS 60005 - 92665 - Asnières sur Seine Cedex

Orange Business Services SA - Société anonyme au capital de 1 063 592 809,20 Euro
1 place des droits de l'Homme 93210 SAINT DENIS - 345039416 RCS BOBIGNY - TVA FR26345039416

Mai 2024