Université de technologie d'Haïti

(UNITECH)

GROUPE FIREWALL

Nom & Prénom : DIEUVEUILLE Ruth

Nom & Prénom : COMPERE Kendy Morandi

Nom & prénom : DUPPOUX Jefferson Andy

Proposé par : Ismaël Saint Amour

Thème : La cybersécurité dans les systèmes de voitures connectées : enjeux et solutions.

Le 11 Mars 2025

Préfaces

Ce document conçu par le groupe firewall composé de 3 étudiants en sciences informatiques présente le rôle de la cybersécurité dans les systèmes de voitures connectées : ses enjeux et solutions apportées. Les étudiants expliquent :

1) Ce que c'est la cybersécurité (sa définition, son origine, ses rôles etc.)
2) Ce que c'est un système de voiture connectée (définition, historique, avantages etc.)
3) Les enjeux rencontrés dans ces systèmes et les solutions apportées.
4) La cybersécurité et la voiture connectée.

Objectifs des différents chapitres :

Chap1 : définir la cybersécurité.

Comprendre son origine et ses rôles.

Chap2 : définir un système de voiture connectée.

Comprendre son historique et les avantages de ce type de système.

Différencier une voiture autonome d'une voiture connectée.

Chap3 : Expliquer les problèmes et enjeux rencontrés dans ce système.

Chap4 : faire le lien entre cybersécurité et voiture connectée.

Table des Matières

Chap1. Qu'est-ce que la cybersécurité ? ----------4

1.1 Définition de la Cybersécurité----------4

1.2 Origine de la Cybersécurité ----------4

1.3 Rôle de la Cybersécurité ----------4

1.4 Technologie utilisée dans la cybersécurité----------5

Chap2. Qu'est-ce qu'un système de voitures connectée ? ----------6

2.1 Définition d'un système de voiture connectée----------6

2.2 Historique des voitures connectées. ----------6

2.3 Avantages des voitures connectées----------8

2.3 types de connectivité dans les voitures connectées ----------9

2.4 Différence entre voiture connectée et voiture autonome----------9

Chap3.Les enjeux dans les Systèmes de voiture connectées----------11

3.1 types de risques majeurs pour le véhicule----------11

3.2 Solutions pour renforcer la cybersécurité des véhicules connectés----------13

Chap4. Le rôle de la Cybersecurite dans les systèmes de voitures connectées ----------15

Définition de La cybersécurité

Le mot **cybersécurité** est un néologisme désignant le rôle de l'ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies qui peuvent être utilisés pour protéger les personnes et les actifs informatiques matériels et immatériels (connectés directement ou indirectement à un réseau) des États et des organisations (avec un objectif de disponibilité, intégrité et authenticité, confidentialité, preuve et non-répudiation).

Origine de la cybersécurité

Le terme cybersécurité est construit à partir du préfixe « cyber », d'origine grecque, réapparu au milieu du XX^{e} siècle avec le mot cybernétique, ce dernier concernant l'étude des processus de contrôle et de communication chez l'être vivant et la machine[2].

Ce préfixe « cyber » a donné avec le développement d'Internet et la généralisation du numérique un grand nombre de mots tels que cyberespace, cyberdéfense, cyberattaque, cybercrime, cybercafé, cyberculture, cyberdémocratie, cybermarché, cyber-réputation.

C'est par réaction contre les risques liés à l'omniprésence des technologies de l'information et de la communication et à leur capacité d'interconnexion et d'échange de données que la cybersécurité se constitue progressivement en tant que nouvelle discipline (spécialité) pleine et entière.

Le rôle de la cybersécurité

L'objectif principal de la cybersécurité est de protéger les systèmes, les réseaux et les programmes contre les menaces numériques, en veillant à ce que les informations restent confidentielles, intactes et accessibles. Cette protection est essentielle pour maintenir la confiance et la continuité opérationnelle dans le paysage numérique actuel.

Les technologies utilisées dans la cybersécurité

Des technologies adéquates sont en effet essentielles pour faire rempart contre les cyberattaques : IAM, threat intelligence, SIEM, pentest, SOC…

- *L'Identity and Access Management*
- *Cloud et gestion des identités*
- *La Threat Intelligence*
- *La gestion des évènements et des informations de sécurité (SIEM)*
- *Le pentest ou test d'intrusion*
- *Le SOC (Security Operation Center)*

Qu'est-ce qu'une voiture connectée ?

Une voiture connectée, également appelée voiture intelligente, est un véhicule équipé d'une technologie avancée qui lui permet de communiquer avec d'autres véhicules, Internet et des appareils externes. Logiciel de voiture connectée rend possible les fonctions de communication et de connectivité dans les voitures connectées. Cette connectivité ouvre un monde de possibilités, transforme l'expérience de conduite et offre de nombreux avantages aux conducteurs, aux passagers et aux constructeurs automobiles.

Historique des voitures connectées

1980 : La voiture connectée voit le jour en Formule 1, lorsque le premier ordinateur de bord est intégré aux voitures de course de l'équipe BMW.

1996 : C'est General Motors qui rend disponible au public la première voiture connectée, en équipant certains de ses modèles d'une fonction d'appel d'urgence. Le véhicule pouvait enregistrer un accident et appeler automatiquement les services d'urgences les plus proches.

2000 : Les signaux GPS, auparavant réservés aux militaires, sont mis à la disposition des entreprises et des particuliers par le président américain Bill Clinton, faisant ainsi avancer les systèmes de navigation.

2001 : Les diagnostics à distance sont installés pour la première fois dans les véhicules. Ils permettent aux constructeurs automobiles et aux propriétaires de flottes d'analyser le fonctionnement du système et d'identifier les problèmes plus rapidement. Certains véhicules bénéficient désormais de l'intelligence prédictive, qui permet aux gestionnaires de flotte de mieux organiser et entretenir leurs véhicules électriques ou thermiques.

2008 : La première voiture équipée d'une borne Wi-Fi est commercialisée, suivie de peu par des applications pour smartphone lui étant destinées, avec des fonctionnalités telles que le verrouillage et le déverrouillage des portes.

2014 : Audi et General Motors déploient en masse des points d'accès 4G LTE.

2016 : Toyota devient le premier constructeur à présenter des voitures équipées de V2X, vendues seulement au Japon.

2017 : Un fabricant européen annonce le déploiement de la technologie V2X.

2020 : 30 millions de nouveaux véhicules connectés sont vendus.

2021 : L'Allemagne endosse un rôle de premier plan et publie une loi sur la conduite autonome.

D'ici 2025 : Un véhicule sur deux circulant sur les routes de l'UE et des États-Unis devrait être connecté.
D'ici 2050 : Dans un scénario optimiste, la banque LBBW prévoit que la part des véhicules nouvellement immatriculés dotés d'un pilote automatique passera de 2,4 % en 2020 à 70 % en 2050.

Quels sont les avantages des véhicules connectés ?

Une fois les véhicules connectés, les données complexes du système GPS et de diagnostic embarqué (OBD) peuvent être traitées et présentées sur une plateforme de gestion de flotte en ligne. Les gestionnaires de flotte peuvent utiliser ces informations pour prendre d'importantes **décisions**, **mesurer** leur efficacité et **comparer** leurs performances avec celles de flottes similaires.

Voici quelques façons dont les flottes peuvent bénéficier de véhicules connectés :

- **Productivité :** En suivant les facteurs qui influencent la productivité de la flotte, tels que le temps de marche au ralenti ou de conduite, les arrêts clients ou les lieux d'allumage.

- **Sécurité :** En détectant les comportements de conduite à risque, tels que les freinages brusques, les excès de vitesse ou les virages serrés ; en mettant en place un système d'accompagnement ou d'assistance avancée du conducteur, ou en installant des solutions dash-cam pour accroître la visibilité des activités sur la route.

- **Maintenance :** En accédant aux données d'entretien du véhicule et en utilisant une plateforme de gestion de flotte connectée pour mettre en place une **maintenance prédictive**, afin de minimiser le risque de panne inattendue et potentiellement dangereuse des véhicules.

- **Durabilité :** En obtenant des données précises sur la consommation de carburant et les activités inefficaces, comme la marche au ralenti. Les flottes composées de VE, ou d'un mélange de VE et de véhicules conventionnels, peuvent surveiller les niveaux de charge, l'autonomie et la dégradation des batteries.

Types de connectivité dans les voitures

Les capacités des voitures connectées peuvent être regroupées en plusieurs catégories :

- **Télématique** : suivi en temps réel de la localisation et de l'activité du véhicule, comportement du conducteur, diagnostic de l'état de santé du moteur et de la batterie du VE. Permet aux organisations de voir les performances d'une grande flotte à partir d'une seule plateforme en ligne.
- **Véhicule-à-Tout** (V2X) : interaction avec tout objet se trouvant à proximité du véhicule. Cette communication peut être de type Véhicule-à-Véhicule (V2V), Véhicule-à-Piéton (V2P), Véhicule-à-Réseau (V2N) ou Véhicule-à-Infrastructure (V2I).
- **Système d'infodivertissement embarqué** : interaction avec les occupants du véhicule. Comprend des systèmes de divertissement audio et vidéo, ainsi que de navigation.

Quelle est la différence entre les voitures connectées et les voitures autonomes ?

Une voiture connectée fait référence à sa **connectivité Internet**, tandis qu'une voiture autonome est une voiture sans conducteur. Elle contrôle son propre mouvement. Un véhicule entièrement automatisé ou un véhicule à conduite autonome doté d'une intelligence artificielle (IA) ne nécessite aucune intervention du conducteur pour se rendre à destination.

Les véhicules hautement **automatisés** doivent encore faire l'objet d'années de tests, avant d'être largement disponibles pour un usage public. Toutefois, de nombreux conducteurs peuvent bénéficier dès aujourd'hui de la connectivité et d'une automatisation basique pour les aider dans des manœuvres comme les créneaux, ou avec le régulateur de vitesse adaptatif.

Voitures du futur

Les véhicules connectés et les voitures intelligentes transforment l'ensemble du secteur automobile. Les équipementiers et les startups investissent massivement dans la recherche autonome et le développement des véhicules de demain. La voiture de demain sera une automobile connectée, intelligente, voire complètement autonome. Grâce à des capteurs tels que lidars et radars, ainsi que des algorithmes d'assistance à la conduite toujours plus sophistiqués, le véhicule du futur pourra **analyser son environnement** en temps réel, anticiper les embouteillages, détecter les piétons, et **prendre des décisions** pour optimiser la sécurité des véhicules et des autres usagers de la route, et la fluidité des mobilités. Les voitures sans conducteur et les véhicules automatisés promettent une révolution dans les **transports intelligents** avec des nouveaux services. Cette transformation soulève également des questions cruciales en matière de cybersécurité, de législation et d'acceptabilité sociale, qui devront être résolues pour que la voiture du futur devienne une réalité. Les assureurs sont aussi concernés par les changements à venir dans le secteur de la **technologie** automobile et de la **conduite intelligente** qui impacteront les risques et les responsabilités en matière de sécurité des véhicules.

Les enjeux dans les systèmes de voitures connectées

Chaque véhicule connecté est relié à un réseau doté d'une mine de précieuses informations privées. Pour optimiser les avantages des véhicules connectés et assurer la sécurité des conducteurs et des passagers, il est capital de mettre en place des dispositifs de sécurité adaptés.

Tout constructeur de véhicule connecté et toute partie prenante doivent prendre en considération les éléments suivants :

- Plus que jamais, la collaboration entre opérateurs de télécommunications et constructeurs automobiles s'impose

- La voiture connectée offrant toujours plus de fonctionnalités connectées au réseau, les mises à jour de logiciels et les téléchargements reposant toujours davantage sur la connectivité du réseau, l'interdépendance de ces deux plateformes ne pourra que s'accroître.

La collaboration entre les opérateurs de télécommunications et les constructeurs automobiles doit se faire dans la même mesure que le développement de cette relation. Cette évolution est nécessaire pour assurer une meilleure sécurité de la plateforme, une amélioration de la sécurité de bout en bout et surtout, une meilleure sécurité des passagers du véhicule et de leur environnement.

Il existe quatre types de risques majeurs pour le véhicule

L'Administration nationale de la sécurité routière (NHTSA) américaine a identifié des cybermenaces sur quatre types de données ou de contrôle :
1. Protection des données personnelles et sécurité
2. Transactions commerciales non souhaitées ou non autorisées
3. Interférence opérationnelle ne relevant pas de la sécurité
4. Interférence opérationnelle relevant de la sécurité

La multiplicité de ces risques exige une sécurité de bout en bout entre les plateformes véhicules et télécommunications. Pour ce faire, il faut des voies de communication hautement sécurisées, tant à l'extérieur du véhicule qu'au sein de

l’environnement qui constitue sa plateforme interne.
1. Une sécurité de bout en bout à l’extérieur du véhicule : connecter la voiture, dans la mesure où elle communique avec le Cloud, au moyen de serveurs dédiés ou de personnes.
2. Une sécurité de bout en bout à l’intérieur du véhicule : entre les constructeurs automobiles et leurs fournisseurs – dont ceux de logiciels et de matériel – sur les données cruciales et les voies de communication au sein du véhicule.

Aux cyberattaques dirigées contre le véhicule peuvent venir s’ajouter celles dirigées contre les plateformes dans le cloud qui offrent des services en matière de véhicule connecté. Si ces services sont compromis, le hacker peut alors exploiter les interfaces de la flotte de véhicules, ainsi que les interfaces commerciales et d’affaires externes avec les entreprises partenaires.

Ces services étant susceptibles de contenir des données financières sur les utilisateurs, ils représentent des cibles idéales qui pourraient au final s’étendre et contaminer l’intégralité du système.

Solutions pour renforcer la cybersécurité des véhicules connectés

Face à cette menace ciblant l'industrie automobile, la mise en place de solutions et mesures de sécurité robustes pour les véhicules connectés est devenue une priorité. Le secteur automobile répond par l'adoption de normes et réglementations strictes, ainsi que par le déploiement de technologies avancées pour protéger les utilisateurs et leurs données.

Plusieurs normes et réglementations structurent désormais la cybersécurité dans le secteur automobile. Ces dernières se positionnent sur toutes les phases du cycle de vie des véhicules, de leur conception à leur maintenance pour être le plus efficace possible.

- Par exemple, la norme ISO/SAE 21434, issue d'une collaboration entre l'Organisation Internationale de Normalisation (ISO) et la Society of Automotive Engineers (SAE), définit des directives cruciales pour la gestion de la sécurité des informations. **Elle promeut une analyse approfondie des risques et l'adoption de mesures de protection adaptées.**

- La National Highway Traffic Safety Administration (NHTSA), l'agence fédérale américaine chargée de la sécurité routière, et la norme SAE J3061, spécifique à la cybersécurité dans l'automobile, proposent quant à elles des orientations pour **identifier et gérer les risques liés à la cybersécurité,** en insistant sur l'importance de rester proactif face aux menaces numériques.

- Une autre approche consiste à compartimenter le réseau des véhicules. Séparer les systèmes critiques (freinage et direction par exemple) des systèmes moins critiques (comme l'info divertissement) permet en effet de réduire le risque que des cybercriminels accèdent à des fonctions essentielles du véhicule en passant par des systèmes moins protégés.

- Les constructeurs orientent également leurs investissements R&D sur l'intelligence artificielle et l'apprentissage automatique. Ces technologies facilitent le développement de systèmes de sécurité capables d'apprendre et de s'adapter pour réagir aux nouveaux types d'attaques. L'analyse de grandes quantités de données permet d'identifier plus rapidement les schémas inhabituels et donc les possibles menaces pour la sécurité.

- Ces efforts sont complétés par les recommandations du WP.29, le forum mondial pour l'harmonisation des réglementations des véhicules des Nations Unies, qui établit **des principes pour la sécurité des véhicules connectés et pour les mises à jour logicielles effectuées à distance (Over-The-Air, OTA)**. Ces mises à jour OTA sont cruciales pour corriger rapidement les vulnérabilités. En parallèle, les meilleures pratiques de l'Automotive Information Sharing and Analysis Center (Auto-ISAC) aident les constructeurs et fournisseurs à renforcer leurs défenses contre les cyberattaques en favorisant le partage d'informations et la collaboration en matière de cybersécurité automobile.

  Ces cadres et directives jouent un rôle vital dans la prévention des cyberattaques et la protection des utilisateurs dans un paysage technologique en constante évolution.

La Cybersécurité et la voiture connectée

Les véhicules connectés sont de plus en plus nombreux sur les routes, offrant aux conducteurs un confort de conduite et une dynamique sans pareil. Mais pour pouvoir fonctionner comme ils sont censés le faire, ils ont besoin d'une solide connectivité permanente. Ce qui ne va pas sans poser un certain nombre de défis, notamment pour garantir la sécurité des véhicules et de leurs occupants.
Christine Caviglioli, vice-présidente Thales Automotive, et Jean-Marie Letort, vice-président Consulting & Opérations de cybersécurité, nous expliquent comment le Groupe relève les défis actuels et se prépare à faire face aux enjeux futurs.
On parle beaucoup des véhicules connectés. Pour beaucoup de personnes, cela signifie essentiellement accéder à leur playlist favorite via le cloud ou pouvoir utiliser les voies de télépéage sur l'autoroute. Je suppose que cela ne se limite pas à ces deux fonctions ?
Christine Caviglioli (CC) : Ce ne sont en effet que deux aspects familiers de la connectivité interne et externe du véhicule. En réalité, elle couvre un champ beaucoup plus large que le simple confort et le divertissement du conducteur, et devrait s'étendre encore avec l'augmentation du nombre de voitures électriques qui circulent sur les routes.
Les enjeux dans ce domaine – en particulier en zone urbaine – sont considérables : non seulement les véhicules sont censés amener le conducteur et ses passagers d'un point A à un point B, mais ils doivent en outre consommer moins d'énergie, s'intégrer parfaitement dans les nouvelles villes intelligentes et offrir toutes les garanties de sécurité pour les conducteurs et les piétons.

Plusieurs initiatives ont été prises pour renforcer la sécurité, en particulier le déploiement à l'échelle européenne du système eCall qui permet d'appeler automatiquement les secours en cas d'accident. Selon les estimations, ce système pourrait réduire de l'ordre de 40-50 % les délais d'intervention des secours.
Tout cela semble très positif. Mais quels sont les sujets de préoccupation ?
CC : C'est effectivement très positif. Mais l'intégration et la fiabilité requièrent plus de connectivité et cela a un prix. La voiture d'aujourd'hui est un ordinateur sur roues – les modèles de luxe comptent jusqu'à 100 millions de lignes de code – connecté à de multiples systèmes et réseaux qui lui permettent de fonctionner efficacement en toute sécurité. Toutes ces communications et connexions sont sans fil, avec un risque accru d'exposition aux cyberattaques visant les systèmes du véhicule, les infrastructures routières ou les données personnelles du conducteur. On assiste depuis quelques années à une véritable flambée de ce type d'attaques : les cyber-incidents ciblant le parc automobile ont été multipliés par sept entre 2016 et 2019[1].

C’est dans ce domaine que la cybersécurité joue un rôle crucial, pas seulement en termes de protection tout au long de la chaîne de valeur, mais en permettant d’exploiter pleinement le potentiel offert par la connectivité. Elle est essentielle à la fois pour les constructeurs automobiles, par exemple dans le domaine de la télématique (gestion du véhicule), et pour l’utilisateur final, qui bénéficie de nombreux services, notamment l’accès à divers contenus multimédias et à des informations en temps réel sur les conditions de circulation. Elle facilite en outre grandement l’autopartage, grâce à la communication, via le smartphone du conducteur, de la clé qui lui donne accès au véhicule.

Devant les nombreux pays et constructeurs /équipementiers concernés par les questions de cybersécurité, une réglementation semble inéluctable…
Jean-Marie Letort (JML) : On voit apparaître des directives et des règlements pour contrer ces cybermenaces et protéger les utilisateurs. Adopté en juin 2020, le règlement WP29 de la Commission économique pour l’Europe (ONU) relatif à l’homologation des véhicules, qui couvre le déploiement des systèmes de gestion de la cybersécurité, impose aux constructeurs et équipementiers automobiles d’intégrer des activités de cybersécurité tout au long de la chaîne de valeur.
Ces règlements, dont Thales a suivi l’élaboration, seront obligatoires pour les véhicules neufs dès 2022 et s’appliqueront à tous les véhicules d’ici 2024. Si le règlement WP29 est clair sur le Quoi – la mise en œuvre de la cybersécurité par les constructeurs – il l’est nettement moins sur le Comment. C’est là que Thales intervient : nous nous employons à aider nos clients à comprendre ces règlements et à concevoir et construire des solutions de cybersécurité innovantes conformes à ces règles, afin de protéger tous les équipements automobiles critiques contre les cybermenaces. Notre expérience de la sécurité sur des marchés très divers nous permet de déployer des services connectés sécurisés qui minimisent les risques et protègent l’utilisateur du véhicule.
La cybersécurité semble désormais aussi importante que la sécurité routière proprement dite...
CC : Dans le véhicule connecté, la cybersécurité est inséparable de la sécurité du véhicule et de la protection de l’utilisateur : elle est la meilleure garantie de succès de la voiture connectée et de la confiance des utilisateurs.

© 123RF/Nopphon Pattanasri

Cette confiance est également primordiale pour les constructeurs automobiles et les équipementiers de premier niveau. Ils ont besoin d’être sûrs que Thales est capable de gérer les défis posés par cette montée en puissance de la connectivité et de leur permettre de protéger la voiture et ses multiples interactions avec les éléments de

l'écosystème externe : les autres véhicules, les infrastructures routières ou, plus généralement, la ville intelligente.

Comment vous y prenez-vous pour relever un défi aussi complexe ?
JML : Ce qu'il faut, c'est une solide architecture de cybersécurité qui couvre la totalité de l'écosystème. L'utilisateur doit avoir l'assurance que les informations communiquées par la voiture et par les réseaux extérieurs sont dignes de confiance, et qu'il est protégé tout au long du chemin, depuis le moment où il accède au véhicule grâce un code numérique sécurisé, jusqu'à celui où le système de navigation du véhicule l'amène sain et sauf à sa destination finale.
Dans ce domaine, Thales agit depuis 2013 aux côtés des constructeurs automobiles et des équipementiers de premier niveau en mettant à profit son expertise en cybersécurité, depuis l'usine jusqu'à la mise en circulation. Dans le contexte de la conformité aux règlements que je viens d'évoquer, nous prenons en charge l'analyse du risque, la conception de l'architecture de cybersécurité et – par l'intermédiaire de notre Trusted Key Manager – la gestion des identifiants tout au long du cycle de vie du véhicule.
Nous disposons en outre – et c'est l'une des composantes majeures de l'architecture de cybersécurité de bout-en-bout de Thales – de plusieurs Centres opérationnels de sécurité (SOC) dans le monde, qui aident les constructeurs automobiles à surveiller la situation internationale et à protéger les véhicules contre les cyberattaques émergentes.
S'agit-il de solutions qui s'installent sur des véhicules finis ?
CC : Pour les véhicules déjà en circulation, c'est le cas. Mais les solutions de cybersécurité sont nettement plus efficaces si on les intègre dans les véhicules dès la construction. C'est la raison pour laquelle nous avons travaillé avec les grands constructeurs et équipementiers sur une approche de « sécurité par conception » de l'architecture, qui prend en compte les différentes fonctions interconnectées et les réseaux avec lesquels la voiture entre en relation. Plus nous anticipons les problèmes potentiels loin en amont – et la phase de conception est l'ultime phase amont –, plus la protection du véhicule sera efficace.
Vous avez évoqué les défis que vous rencontrez actuellement. Qu'en sera-t-il dans le futur ?
JML : C'est une bonne question. L'industrie automobile évolue à un rythme extrêmement rapide, ce qui fait de la gestion du cycle de vie un facteur clé. Lors du développement de nos solutions et de notre architecture de cybersécurité, nous concevons des composants intégrés évolutifs, capables de s'adapter aux nouveaux environnements futurs pour continuer à assurer la cybersécurité des véhicules de bout-en-bout.

La volonté de Thales de mettre son expertise à profit dans ces environnements trouve une illustration dans notre participation à l'initiative Mobena et à l'écosystème ouvert « Software République » pour une mobilité intelligente et durable. Le but est de créer un service innovant et sécurisé, basé sur le système Plug & Charge qui vise à simplifier la recharge des voitures électriques. L'acquisition de Gemalto en 2019 nous a permis d'assurer l'adaptabilité nécessaire dans ces environnements dynamiques et d'élaborer une gamme complète de solutions de cybersécurité qui couvrent la protection du véhicule et des échanges de données, la gestion du cycle de vie des fonctions de sécurité de la voiture, avec service de mises à jour à long terme, la détection et la réponse aux nouvelles menaces et attaques contre la cybersécurité.

En un mot, une expérience de la conduite automobile qui inspire confiance.

Conclusion

Pour conclure, ce document permet de constater l'importance de la cybersécurité dans les systèmes de voitures connectées en se basant sur ce que c'est d'abord la cybersécurité et ses rôles ensuite sur ce que c'est une voiture connectée et la problématique de ce système et enfin les solutions futures.

Pour rapporter les propos de Romain LAFITTE Managing Director chez Via ID

« La cybersécurité automobile ne se limite pas à un enjeu de protection ; elle représente une opportunité d'innovation et de différenciation dans un secteur en constante évolution. Les sociétés qui se sont développées dans ce domaine au cours des dernières années, en particulier en Israël, leader reconnu dans l'innovation de la cybersécurité, illustrent la dynamique et le potentiel de croissance de ce marché.

Pour finir, l'investissement dans la cybersécurité automobile s'annonce comme une démarche stratégique pour anticiper les besoins futurs de la mobilité connectée et assurer une avance technologique dans le domaine. La capacité à protéger efficacement les données et les systèmes sera un facteur clé du succès dans l'ère de la mobilité intelligente et connectée, offrant des opportunités sans précédent pour les investisseurs visionnaires prêts à contribuer à façonner l'avenir de la mobilité. »

Références

1. def. cybersecurite source Wikipedia
2. Source article « Au carrefour de la technologie et de la cybersécurité : quels sont les enjeux de la mobilité connectée ? » écrit par Romain LAFITTE Managing Director chez Via ID.
3. Source: Upstream Security 2020 Global Automotive Cybersecurity Report