Deloitte.

RIVA
CONNECTÉ. AUTOMATISÉ.

Ontario

Cybersécurité pour les véhicules connectés et autonomes

Considérations et possibilités de développement

Septembre 2019

Ontario Centres of Excellence

APMA
LEAD. REACH. CONNECT.

Sommaire

Contexte

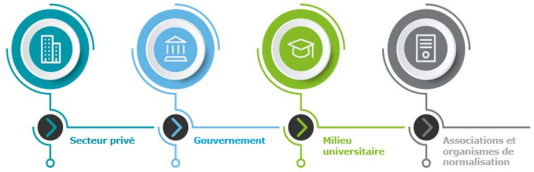
Les véhicules connectés et autonomes (VCA) séduisent les consommateurs, l'industrie et les gouvernements du monde entier. Bien que les VCA soient conçus avec des capacités et des caractéristiques qui ont le potentiel d'offrir une sécurité accrue, une plus grande satisfaction, un meilleur confort et plus de commodité, les VAC présentent également des défis émergents concernant la sécurité et la vie privée, combinés à des dangers physiques et numériques.

Le rapport *La cybersécurité pour les véhicules connectés et autonomes: éléments à considérer et possibilités de croissance* a été commandé par le Réseau d'innovation pour les véhicules autonomes (RIVA) et la Automotive Parts Manufacturers' Association (APMA) afin de donner un aperçu général de l'ensemble des menaces à la cybersécurité auxquelles font face les VCA, et de mettre en évidence à la fois les possibilités et les risques associés aux technologies émergentes des VCA, avec un accent sur les stratégies, les normes, les solutions envisagées et les opportunités sur le marché pour l'Ontario.

Objectif et méthodologie

Dans un contexte des menaces croissantes qui pèsent envers la cybersécurité, compte tenu des préoccupations relatives à la sûreté, à la sécurité, à l'efficacité et à la confidentialité des données, ce rapport vise à identifier les éléments essentiels à prendre en considération et les pistes pour la croissance et le développement. Alors que le marché des VCA en Ontario fait face à de plus en plus de défis, il est capable d'identifier et de capitaliser sur les possibilités d'accroître notre compréhension des menaces à la cybersécurité que présentent les VCA et il nous permet de continuer à innover dans ce domaine pour devenir un leader du marché mondial.

Ce rapport résume les observations qui peuvent se dégager d'un écosystème complexe pour les VCA à l'aide d'une approche hiérarchisée de recherche primaire et secondaire. Les méthodes de recherche primaire comprenaient l'administration de sondages, la conduite d'une série d'entrevues et de discussions pour valider l'information auprès des principaux intervenants et des experts en la matière en Ontario et dans d'autres juridictions majeures.



Les intervenants en cybersécurité des VCA couvrent de nombreux secteurs

Considérations et possibilités

Notre recherche à travers le monde et les réponses des intervenants dans le secteur des VCA ont souligné que l'authentification et la confiance seront des défis essentiels à relever à travers l'écosystème des VCA et que l'ensemble de la question de la sécurité doit être considéré, avec un accent sur la sécurité de l'infonuagique, la sécurité à bord des véhicules et la sécurité du réseau. Les éléments à considérer en matière de normalisation, de collaboration, de formation et de confiance, ajoutent de la complexité quand vient le temps d'être en mesure de répondre et de gérer les risques à la cybersécurité des VCA.

Les intervenants du secteur des VCA à travers le monde identifie la cybersécurité comme étant un élément essentiel pour assurer la sécurité et la sûreté de l'avenir de la mobilité, et ils ont identifié des possibilités de collaboration entre le gouvernement et l'industrie. Parmi ces possibilités, mentionnons les suivantes:

- Normalisation, certification et législation
- Croissance et rétention des talents qualifiés
- Collaboration et partenariats entre les industries
- Innovation en matière de confiance et d'authentification
- Mise sur le marché des FEO et de l'innovation technologique
- Tests de convergence de sécurité
- Protection de la vie privée et sécurité dès la conception ; cadres éthiques

Les intervenants du secteur des VCA en Ontario en matière de cybersécurité nous disent qu'il y a encore un chemin à parcourir sur les questions de la clarté des exigences, des partenariats et du soutien nécessaires à la cybersécurité des VCA. Il y a toutefois beaucoup de possibilités de continuer à établir l'Ontario comme le marché de référence pour cette composante centrale pour le succès et l'adoption des VCA à travers le monde.

À propos de nous

Le **RIVA** est une initiative du Gouvernement de l'Ontario administrée par les Centres d'excellence de l'Ontario (CEO). Le RIVA veille à ce que l'Ontario saisisse les possibilités économiques offertes par la technologie des VCA et les solutions de mobilité qui créent des emplois dans notre province, tout en veillant à ce que l'Ontario soit en tête en matière de préparation, d'adoption et de déploiement. Le RIVA soutient le développement et la démonstration de technologies des VCA, y compris les technologies d'infrastructure, les technologies commercialement prêtes à être appliquées aux véhicules légers et lourds (y compris les voitures, les véhicules commerciaux, les camions, les autobus et les véhicules récréatifs), les systèmes de transport intelligents (STI) et les technologies qui soutiennent le transport.

APMA s'est associée au RIVA pour exploiter une zone de démonstration technologique du RIVA située à Stratford, en Ontario. L'APMA est l'association nationale du Canada qui représente les fabricants FEO de pièces, d'équipement, d'outils, de fournitures, de technologies de pointe et de services pour l'industrie automobile mondiale. L'Association a été fondée en 1952 et ses membres représentent 90 % de la production indépendante de pièces au Canada. En 2018, les expéditions de pièces automobiles ont dépassé les 35 milliards de dollars et l'industrie employait plus de 100 000 personnes.

Les pratiques de **Deloitte** sur l'avenir de la mobilité servent l'ensemble de l'écosystème des entreprises qui travaillent en matière de mobilité. L'ensemble de nos déplacements d'un point A à un point B est en train de changer. Cette transformation crée un nouvel écosystème de mobilité personnelle, dont les effets ne concernent pas seulement l'industrie automobile. Les services cyber-risques de Deloitte aident les entreprises à résoudre des problèmes complexes et à améliorer leur rendement, afin qu'elles puissent se bâtir un avenir en confiance, un avenir meilleur pour les affaires, pour les gens et pour la planète. Grâce à la perspicacité humaine, à l'innovation technologique et à des solutions cybernétiques complètes, Deloitte gère le cyberespace partout dans le monde pour que la société puisse aller n'importe où.

Table des matières

Introduction

Introduction

Les véhicules connectés et autonomes (VCA) séduisent les consommateurs, l'industrie et les gouvernements du monde entier. Bien que les VCA sont conçus avec des capacités et des caractéristiques qui ont le potentiel d'offrir une sécurité accrue, la satisfaction, le confort et la commodité, les VCA apportent également des défis émergents à la sécurité et la vie privée – avec une combinaison de menaces physiques et numériques.

Le véhicule connecté et autonome défini

Transports Canada définit les véhicules connectés comme étant « des véhicules utilisant différents types de technologies de communication sans fil pour communiquer avec leur environnement ». [1] Un véhicule autonome ou automatisé est décrit comme un « ensemble de capteurs, de contrôleurs et d'ordinateurs de bord, associé à un logiciel sophistiqué, permettant au véhicule de contrôler au moins certaines fonctions de conduite, à la place d'un conducteur humain ». Alors que nous nous dirigeons vers des véhicules de plus en plus connectés et autonomes, la complexité de la gestion des menaces qui pèsent sur ces véhicules – et leurs passagers – augmente également.

Les avantages et les risques de la connectivité et de l'automatisation des véhicules

La sécurité est l'un des principaux moteurs de l'automatisation, d'autant plus que la grande majorité des accidents graves sont dus à des erreurs humaines. Les VCA ont le potentiel de réduire les blessures et de sauver des vies. Les VCA peuvent accroître l'efficacité de la mobilité en réduisant la congestion routière et peuvent apporter des avantages économiques en augmentant la productivité et en offrant de nouvelles possibilités de mobilité. Tout comme les ordinateurs portables et les téléphones mobiles ont augmenté les capacités humaines, les VCA s'efforcent de créer une expérience de conduite et un écosystème plus habilités, engagés et intégrés.

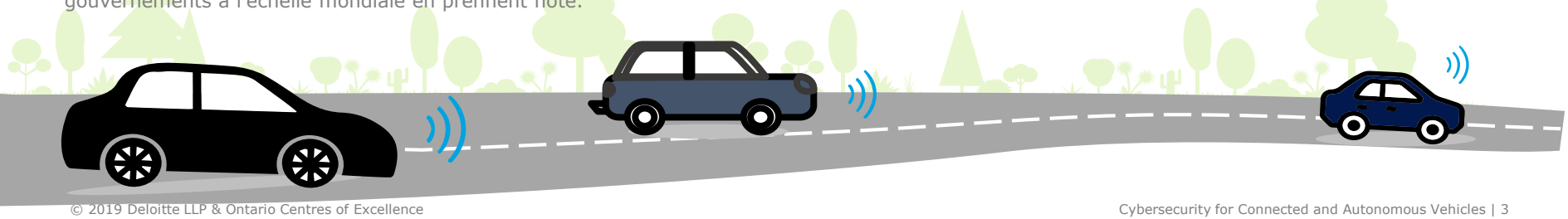
L'écosystème VCA est en pleine croissance et s'étend de l'infrastructure, aux constructeurs automobiles, aux fournisseurs de services, aux clients. Les risques et les répercussions augmentent en même temps que la demande des consommateurs en matière de disponibilité, et l'industrie et les gouvernements à l'échelle mondiale en prennent note.

Au Canada, il y a eu un certain nombre de rapports récents soulignant l'impact de la cybersécurité sur les VCA.[2] En 2018, le Comité sénatorial permanent des transports et des communications a publié un rapport intitulé « Driving Change: Technology and the future of the automated vehicle », qui a fait ressortir d'importantes préoccupations en matière de sécurité et de protection de la vie privée. Cette année, Transports Canada a publié un outil d'évaluation de la sécurité qui tient compte de la cybersécurité. Le Groupe de travail sur les véhicules automatisés et connectés du Comité d'appui aux politiques et à la planification (SPPC) a élaboré un cadre stratégique pour les VCA qui recommande de sensibiliser le public aux vulnérabilités en matière de cybersécurité. Innovation, Sciences et Développement économique Canada (ISED) a déclaré publiquement qu'il appuiera une modification à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) afin d'améliorer l'applicabilité des lois sur la protection des renseignements personnels. L'ISED a en outre souligné l'émergence des véhicules autonomes comme une raison importante de la refonte des mécanismes de protection de la vie privée dans l'annonce de la Charte numérique de 2019.[2]

Dans le contexte des incidents cybernétiques majeurs ayant un impact sur les véhicules dans le monde entier, le Global Risks Report[3]2019 du Forum économique mondial (WEF) a souligné une tendance clé avec des impacts importants sur l'écosystème VCA :

> Une cyberdépendance croissante due à l'interconnexion numérique croissante des personnes, des choses et des organisations, avec des impacts potentiels sur les infrastructures et les investissements clés.

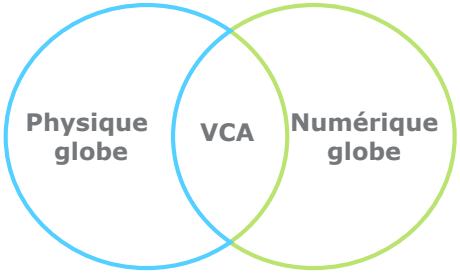
Le marché des VCA de l'Ontario fait de plus en plus face à ces considérations, mais il voit aussi des possibilités intéressantes d'accroître notre compréhension de la cybersécurité VCA et d'innover dans ce domaine pour devenir un leader du marché mondial.



Méthodologie

Les besoins pour un cadre de cybersécurité VCA.

Les risques de cybersécurité sont particulièrement complexes pour les VCA, car ils opèrent à la fois dans le monde physique et numérique, et à la fois consommer et créer des données, tout en communiquant avec l'écosystème environnant.



Les risques pour les VCA impliquent des menaces liées à :

- Le véhicule,
- L'écosystème VCA, et
- Les données recueillies.

Selon le National Institute of Standards and Technology (NIST), l'atténuation des risques pour les dispositifs complexes de l'Internet des objets (IdO) doit porter sur la protection de la sécurité des dispositifs, la sécurité des données et la vie privée des personnes[4] - ce qui est précisément le cas des VCA. Cet écosystème VCA complexe nécessite un cadre qui prend en compte la convergence de la sécurité (la combinaison de la sécurité physique et de la cybersécurité) et le concept de confidentialité par la conception

Le Cadre de cyberstratégie (CSF) de Deloitte, appuyé par notre cadre de protection de la vie privée dès la conception et notre méthodologie de convergence de la sécurité, permet l'analyse des capacités clés nécessaires pour atténuer les menaces émergentes pour les VCA. Le CSF de Deloitte couvre la nécessité d'une **gouvernance** de la cybersécurité, ainsi que de capacités **sûres**, **vigilantes**, et **résistantes**.

L'application de tout cadre de cybersécurité à l'environnement VCA doit tenir compte de l'ensemble de l'écosystème et chaque partie prenante doit comprendre l'éventail des risques et des possibilités.

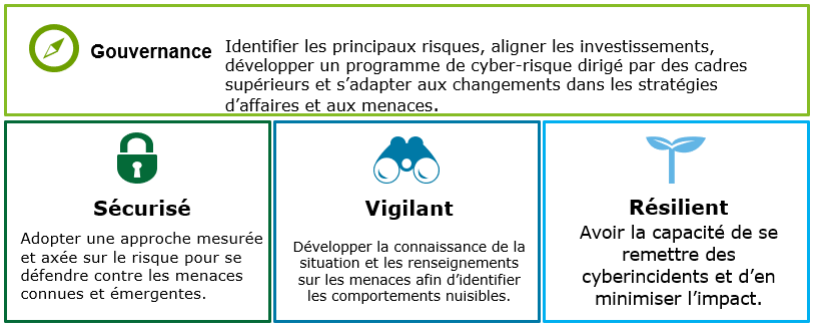
Voir l'annexe pour plus de détails sur les cadres de conception Convergence de la sécurité et Confidentialité.

Objectif et méthodologie

Le Réseau d'innovation pour les véhicules autonomes (RIVA) est une initiative du gouvernement de l'Ontario mise en œuvre par les Centres d'excellence de l'Ontario (CEO). Le RIVAs assure que l'Ontario saisit les opportunités économiques présentées par la technologie VCA et les solutions de mobilité pour créer des emplois dans notre province, tout en s'assurant que l'Ontario occupe la première place dans la préparation, l'adoption et le déploiement. Le RIVAs appuie le développement et la démonstration des technologies VCA, y compris les technologies d'infrastructure, les technologies commercialement prêtes à être appliquées aux véhicules légers et lourds (y compris les voitures, les véhicules commerciaux, les camions, les autobus et les véhicules récréatifs), les systèmes de transport intelligents (STI) et les technologies favorisant le transport en commun.

Dans le contexte des menaces croissantes à la cybersécurité, des préoccupations au sujet de la collecte de données sur les véhicules, ainsi que des opportunités de VCA en Ontario, le présent rapport vise à cerner les principaux domaines à considérer et les pistes de croissance et de développement. En utilisant une approche stratifiée de la recherche secondaire et primaire, ce rapport résume les aperçus à travers un écosystème VCA complexe. Les principales méthodes de recherche comprenaient un sondage et une série d'entrevues et de discussions de validation avec des intervenants clés et des experts en la matière en Ontario et d'autres administrations importantes.

Les quatre piliers du CSF de Deloitte



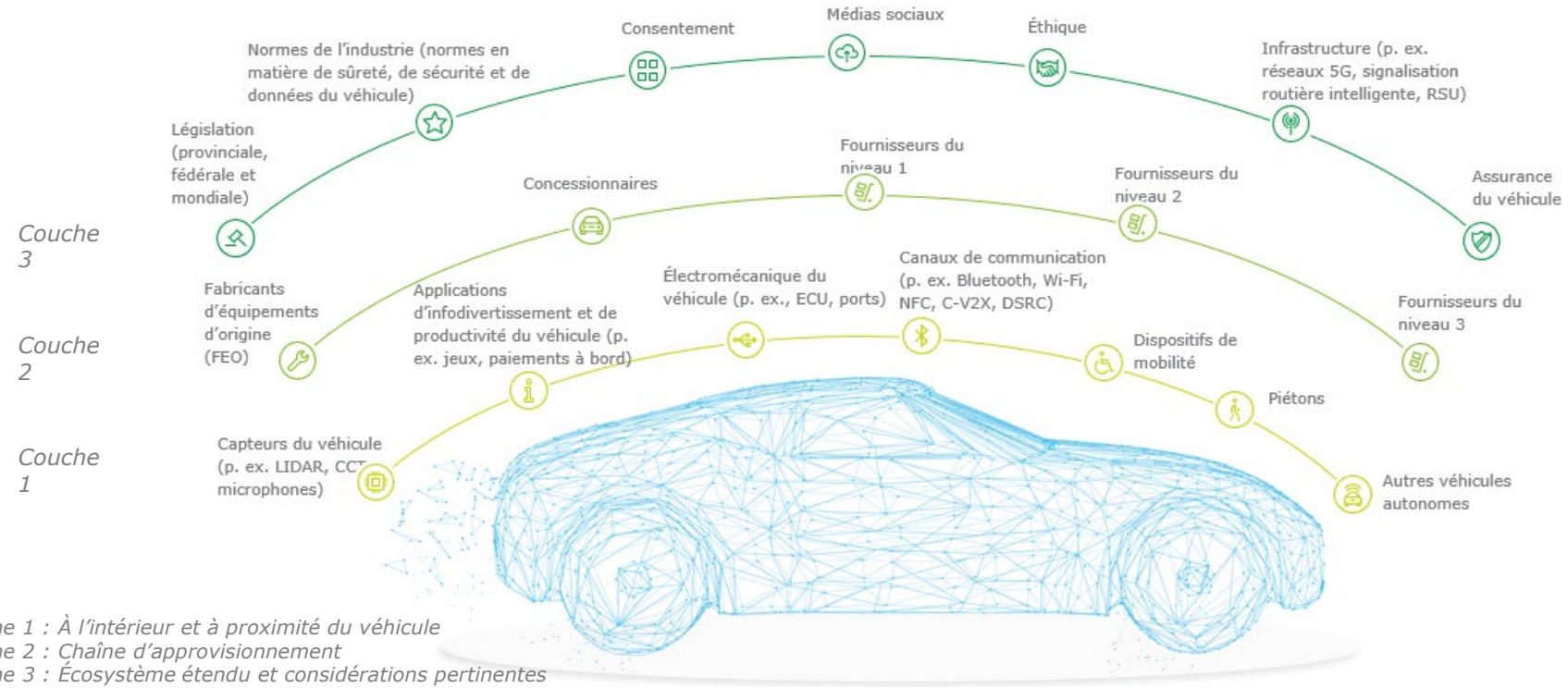
En savoir plus sur le véhicule connecté et autonome

Connectivité VCA, caractéristiques et attributs

Le véhicule connecté et autonome peut être considéré comme une combinaison de divers dispositifs IdO ayant la capacité de communiquer avec son environnement physique et numérique environnant. Selon les caractéristiques installées, un véhicule connecté peut être capable de communiquer avec les éléments suivants :

- Ses occupants, les autres véhicules (de véhicule à véhicule ou V2V), les autres dispositifs connectés (par exemple, les téléphones mobiles) et les usagers de la route
- Applications basées sur Internet
- Un système de gestion des justificatifs de sécurité (SCMS)
- L'infrastructure physique de transport environnante, comme les contrôleurs de feux de circulation, les unités routières (RSU) et l'infrastructure numérique, comme les réseaux de communication et les systèmes en nuage - collectivement appelés véhicule à infrastructure ou V2I.

L'image ci-dessous fournit des exemples d'attributs associés à un VCA - de la connectivité à l'intérieur ou à proximité du véhicule, à des tiers clés, à l'environnement et aux considérations.



Couche 1 : À l'intérieur et à proximité du véhicule
Couche 2 : Chaîne d'approvisionnement
Couche 3 : Écosystème étendu et considérations pertinentes

Les véhicules autonomes et l'avenir de la mobilité

Vers des véhicules autonomes

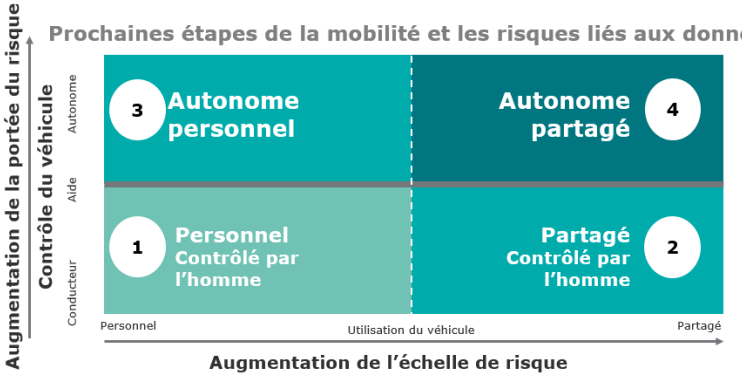
A chaque étape du développement d'un véhicule entièrement autonome, différentes étapes de développement et de complexité des systèmes avancés d'aide à la conduite (ADAS) sont utilisées pour établir les bases techniques. Différents capteurs autour de la voiture détectent les obstacles, aident à garder le véhicule sur la bonne voie et avertissent le conducteur en cas de danger. Les applications ADAS assurent non seulement un niveau de sécurité plus élevé pour le conducteur en fournissant plus d'informations sur l'environnement du véhicule, mais elles favorisent également le confort. Les différents états de la conduite autonome peuvent être décrites par niveaux, de 0 à 5, tels que définis par la Society of Automotive Engineers (SAE), adoptée et décrite par la National Highway Traffic Safety Association (NHTSA). 5 Le tableau ci-dessous fournit un résumé de ces niveaux, avec des exemples de caractéristiques de SAE.

Pas d'automatisation de la conduite	Aide au conducteur	Automatisation partielle de la conduite	Automatisation conditionnelle de la conduite	Automatisation élevée de la conduite	Automatisation totale de la conduite
Niveau 0	**Niveau 1**	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Il n'y a pas d'automatisation à ce niveau. Toutes les tâches de conduite sont effectuées par le conducteur, même lorsqu'elles sont améliorées par des solutions de sécurité actives.	Le véhicule est commandé par le conducteur, mais le véhicule dispose également de quelques fonctions d'aide à la conduite qui peuvent fournir, par exemple, une aide à la direction OU au freinage/à l'accélération.	Le véhicule est doté de fonctions automatisées combinant, par exemple, l'assistance à la direction ET au freinage/à l'accélération simultanément, mais le conducteur doit rester engagé dans la tâche de conduite et surveiller l'environnement à tout moment.	Le véhicule est équipé d'un système de conduite automatisé capable de contrôler entièrement la tâche de conduite; cependant, un conducteur est toujours nécessaire. Le conducteur doit répondre aux demandes d'intervention et être prêt à prendre le contrôle du véhicule en tout temps.	Le véhicule est conçu pour exécuter toutes les fonctions de conduite dans certaines conditions. À ce stade de l'automatisation, le conducteur peut contrôler le véhicule dans des conditions limitées.	Le véhicule est conçu pour exécuter toutes les fonctions de conduite dans toutes les conditions. Le contrôle du véhicule par un conducteur peut être facultatif à ce stade de l'automatisation.
• Avertissement d'angle mort • Avertissement de changement de voie	• Centrage de voie OU • Régulateur de vitesse adaptatif (pas simultanément)	• Centrage de voie ET • Régulateur de vitesse adaptatif (simultanément)	• Conducteur en bouchon	• Taxi local sans conducteur • Les pédales/le volant peuvent être installés ou non.	• Identique au niveau 4, mais la fonction peut conduire partout dans toutes les conditions.

Pour atteindre des niveaux plus élevés d'automatisation, les OEM, les fournisseurs, les éditeurs de logiciels, les régulateurs et les autres parties prenantes doivent relever un certain nombre de défis, allant du développement de fonctionnalités de conduite fiables au règlement des problèmes juridiques qui subsistent tout en garantissant la sécurité, la sûreté et la confidentialité des consommateurs.

L'émergence de véhicules connectés, électriques et autonomes et l'évolution des attitudes à l'égard de la mobilité sont susceptibles de modifier profondément la manière dont les personnes et les marchandises se déplacent et dont elles attendent que leurs données soient sécurisées dans ce contexte. Au fur et à mesure que ces tendances se développent, quatre « **états futurs** » concurrents pourraient émerger dans un nouvel écosystème de mobilité, émanant de l'intersection des propriétaires du véhicule et de ceux qui les exploitaient.[6] défis uniques en matière de cybersécurité liés aux données.

Prochaines étapes de la mobilité et les risques liés aux données



Bien que l'utilisation de véhicules partagés augmente rapidement, parallèlement au renforcement du degré d'automatisation du véhicule, il est probable que des voitures appartenant à des particuliers et à des personnes contrôlées par l'homme coexisteront avec ces futurs États - des véhicules contrôlés par le conducteur et des véhicules autonomes partageant la route. Chaque futur état présente de nouveaux risques ou une augmentation d'un potentiel impact.

Futur état 1 | Les véhicules personnels contrôlés par l'homme continueront de dominer le système de mobilité, car les propriétaires ne se sépareront pas volontairement de leurs véhicules et n'investiront pas dans de nouvelles technologies autonomes aux rendements incertains. La connectivité accrue et les nouvelles fonctionnalités centrées sur les données étant disponibles pour ces véhicules, des capacités de sécurité accrues seront nécessaires.

Futur état 2 | Les véhicules partagés sous contrôle humain connaissent une croissance continue, les passagers appréciant la commodité du transport point à point et les avantages économiques démontrés de la voiture à grande capacité et du covoiturage. L'utilisation d'applications mobiles, la connectivité aux médias sociaux et l'intégration aux systèmes de paiement augmentent les menaces pour ces véhicules et leurs usagers.

Futur état 3 | Les véhicules autonomes appartenant à des particuliers commenceront à s'avérer sûrs, pratiques, économiques et viables, tandis que les consommateurs conserveront une préférence pour la propriété privée. Un nouveau niveau de confiance dans les communications est nécessaire non seulement à l'intérieur ou directement autour du véhicule, mais aussi dans l'infrastructure environnante et dans l'ensemble de la chaîne logistique.

Futur état 4 | Les véhicules autonomes en commun deviennent une réalité à la convergence d'une technologie autonome supérieure et de la croissance continue de la mobilité partagée. Les menaces qui pèsent sur les futurs états 1 à 3 sont multipliées par un ordre de grandeur en raison de l'ampleur des dommages potentiels.

Essai global, législation et normes pilotes VCA

L'évolution de la législation en matière des essais VCA à travers le monde est en marche vers des normes améliorées et une législation plus claire. Comme en Ontario, il y a d'autres juridictions dans le monde entier qui adoptent ou examinent de nouvelles législations en matière d'essai et d'innovation VCA :

Allemagne

Le projet de loi sur les véhicules autonomes a été promulgué en juin 2017, modifiant la loi sur la circulation routière en vigueur qui définit les exigences relatives aux véhicules hautement et entièrement automatisés, ainsi qu'aux droits du conducteur.[7]

Australie

En mai 2017, les ministres australiens des transports ont approuvé les Directives pour les essais de véhicules automatisés en Australie. Les lignes directrices fournissent une approche claire et cohérente à l'échelle nationale dans le but d'équilibrer la sécurité et l'innovation.[8]

Pays-Bas

En novembre 2017, la Chambre des représentants a reçu un projet de loi régissant l'utilisation expérimentale de véhicules automoteurs sur la voie publique avec des conducteurs éloignés. Le projet de loi a finalement été adopté.[9] Les entreprises qui souhaitent tester des véhicules automoteurs doivent d'abord démontrer que les tests seront effectués en toute sécurité par le biais d'une procédure d'admission gérée par l'Autorité néerlandaise chargée du contrôle des véhicules Le gouvernement néerlandais a récemment annoncé la délivrance d'un nouveau permis de conduire pour les véhicules automoteurs dans le but de certifier de nouveaux modèles autonomes et d'encadrer sa législation.[10]

Inde

Les lois (p. ex. la Loi de 1988 sur les véhicules à moteur des Indiens) et les règles régissant la conduite des véhicules exigent qu'un conducteur humain ait en tout temps le contrôle effectif du véhicule. Le projet de loi proposé sur les véhicules à moteur (amendement), 2017, contient des dispositions visant à promouvoir les technologies de remplacement et l'innovation tout en favorisant la sécurité sur les routes.[11]

Chine

Janvier 2019, plus de 101 plaques d'immatriculation ont été délivrées pour les véhicules autonomes/automoteurs. Le gouvernement de Pékin a délivré un permis pour tester des véhicules autonomes sur la voie publique, avec un total de 123 kilomètres pour ce test. En dehors de Pékin, des tests sont effectués dans d'autres villes de Chine, y compris dans les provinces. On s'attend à ce que 50 % des véhicules vendus en 2020 aient des fonctions autonomes.[12]

Japon

En décembre 2018, l'Agence nationale de la police a dévoilé un projet de loi qui permettrait aux véhicules dotés d'un haut niveau d'autonomie de circuler sur la voie publique. En mai 2019, le Japon a publié un projet de loi permettant aux conducteurs d'utiliser leur smartphone pendant que leur voiture roule de façon autonome dans certaines circonstances et s'ils sont capables de passer immédiatement à la conduite manuelle en cas d'urgence.[13]

Programme pilote de véhicules automatisés de l'Ontario

En 2016, l'Ontario a lancé un programme pilote de dix ans pour permettre l'essai de véhicules automatisés sur les routes de l'Ontario.[14] En réponse aux progrès de la technologie VCA, le programme a été mis à jour le 1er janvier 2019 pour permettre l'essai et la vente de technologies plus innovantes. Ces mises à jour comprenaient :

- Mise à jour aux restrictions pilotes : Les VA équipés de la technologie de niveau 3 de la Society of Automotive Engineers (SAE) qui sont admissibles et disponibles pour achat au public au Canada peuvent maintenant rouler sur les routes de l'Ontario. Ces véhicules ne sont plus réservés aux participants inscrits au programme pilote. Les véhicules dotés de la technologie SAE de niveau 3 du marché des pièces de rechange (technologie qui a été ajoutée à un véhicule après sa vente, et non par un équipementier) demeurent limités au programme pilote et ne sont pas autorisés pour un usage public. Quiconque conduit un véhicule, quel que soit son niveau d'automatisation, doit être attentif en tout temps et respecter toutes les lois en vigueur sur la conduite, y compris la distraction et la conduite avec facultés affaiblies. Les participants au projet pilote peuvent faire l'essai de véhicules sans conducteur sur les routes de l'Ontario, dans des conditions strictes qui garantiront que les essais sont effectués dans des environnements sûrs et contrôlés.
- **Programme pilote coopératif de remorquage des camions de l'Ontario** : L'Ontario a lancé un programme pilote d'une durée de huit ans pour mettre à l'essai une technologie de « remorquage » connecté, dans le cadre duquel les gros camions sont équipés de systèmes de soutien et de communications de véhicule à véhicule qui leur permettent de voyager en étroite collaboration en tant que groupe.[15] Pour assurer la sécurité des essais, certaines des exigences comprennent une cote de sécurité élevée pour les transporteurs, la présence d'un conducteur formé et expérimenté dans chaque véhicule, le maintien d'un espace sécuritaire entre les véhicules et le respect des exigences de signalisation des véhicules.

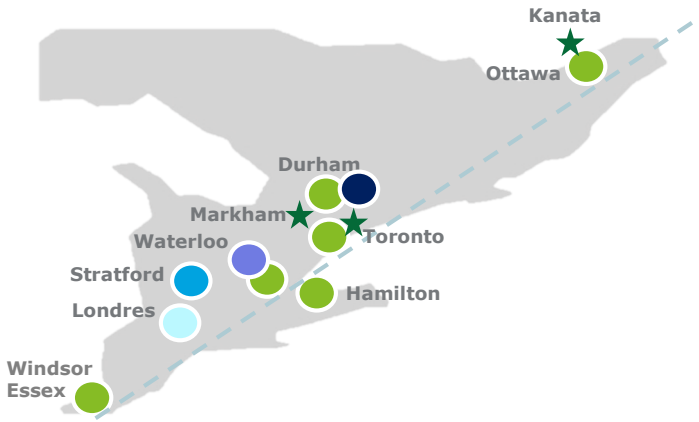
Dans le cadre des processus de demande des deux programmes pilotes, les candidats doivent déclarer les mesures, les choix de conception et les mesures qu'ils ont prises pour s'assurer que les véhicules qu'ils prévoient tester ont tenu compte des risques de cybersécurité qui peuvent avoir une incidence sur la sécurité routière.

Écosystème de l'innovation VCA de l'Ontario

Essai VCA et plan de démonstration

L'innovation VCA de l'Ontario est située le long d'un corridor similaire à l'ensemble de l'innovation de l'Ontario en matière de cybersécurité, regroupés à proximité des centres universitaires, mais avec beaucoup plus de variation à travers l'Ontario et se répand dans les juridictions voisines.

Groupes d'essais et de démonstration VCA



Légende : Groupes d'essais et de démonstration VCA

- Sites régionaux de développement de technologies (SRDT) du RIVA
- Zone pilote RIVA
- Centre d'excellence automobile (CEA) de l'Université technique de l'Ontario
- Espace du Conseil national de recherches Canada pour la fabrication et l'innovation automobile
- Waterloo Centre for Automotive Research (WatCAR)
- ★ Recherche et initiatives/pilotes de l'industrie : GM (Markham), Ford (Kanata), Uber (Toronto), groupe Kanata Autonomous Vehicle dirigé par BlackBerry QNX (Kanata)

Le rapport Deloitte Essex de 2016 sur l'innovation en matière de cybersécurité, intitulé « exploiter les possibilités de croissance en matière de cybersécurité », révèle que les groupes naturels d'innovation en matière de cybersécurité en Ontario sont concentrés dans la région du Grand Toronto, la région de la capitale nationale et Kitchener-Waterloo.[16]

L'une des principales conclusions du rapport de 2016 sur l'innovation en matière de cybersécurité était la répartition géographique des cyberPME qui indiquait le regroupement naturel en fonction de la population, ainsi que : Confluence du milieu universitaire et des grandes industries dans la RGT

- Importantes plaques tournantes militaires, de l'intelligence sécuritaire et technologiques dans la RCN
- Les établissements universitaires axés sur la technologie (p. ex. Institute for Quantum Computing) et organismes piliers (p. ex. BlackBerry) à Kitchener-Waterloo.

Groupes d'innovation en matière de cybersécurité en Ontario

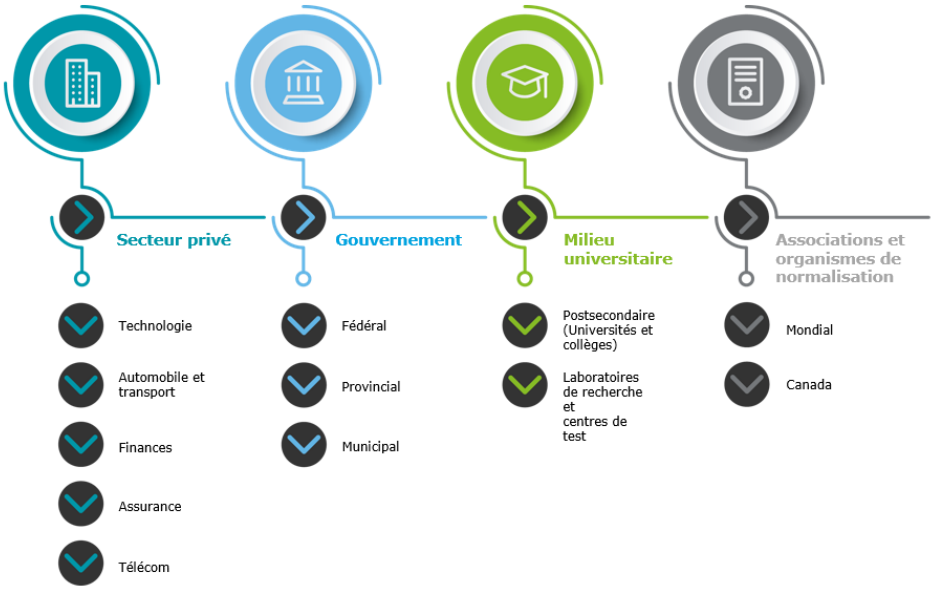
L'innovation VCA en matière de cybersécurité se produit non seulement dans le milieu universitaire et de la recherche, mais au sein et en partenariat avec des organisations du secteur privé des pilotes de premier plan et des groupes technologiques dans plusieurs centres d'innovation et les villes de l'Ontario.

Paysage des parties prenantes en matière de cybersécurité VCA

Écosystème complexe des parties prenantes

L'écosystème VCA est composé d'une variété des parties prenantes interconnectées, y compris les entreprises de pièces automobiles et de logiciels, les établissements universitaires, les organismes de normalisation, les associations industrielles et les institutions financières

Les parties prenantes VCA en matière de cybersécurité ont des interactions uniques avec les organismes en charge de la réglementation, les décideurs et les organisations de développement économique à travers le secteur VCA. Les parties prenantes inclues dans le présent rapport couvrent plusieurs secteurs et sous-secteurs, et de nombreuses parties prenantes ont des rôles multiples.



Dans l'Ontario, tandis que le plus grand nombre de parties prenantes VCA en matière de cybersécurité sont des organisations du secteur privé, beaucoup notent l'importance des partenariats avec les villes (par exemple, la Ville d'Ottawa), la province (par exemple, AVIN), et le gouvernement fédéral par des subventions, des groupes technologiques et des corridors, et l'élaboration de normes et des orientations.

Les partenariats interprovinciaux et transfrontaliers ont également été soulignés comme importants pour le succès du marché VCA, avec un accent sur le rôle que le gouvernement fédéral devrait jouer dans cette industrie.

L'écosystème de cybersécurité VCA - Exemples clés entre les catégories de secteur

Secteur privé : Comprend les fournisseurs de technologie (tels que l'infodivertissement, les capteurs, le développement de logiciels et les services de cybersécurité automobile), la finance, l'assurance, l'automobile (y compris les équipementiers, les fournisseurs de niveau 1-3 et la gestion de la flotte).

Gouvernement : Comprend tous les ordres de gouvernement et les organismes de réglementation au Canada, y compris la police et la justice, les ministères, les organismes du secteur public, etc.

Milieu universitaire : Comprend les établissements postsecondaires (universités et collèges), les laboratoires de recherche et les centres d'examen.

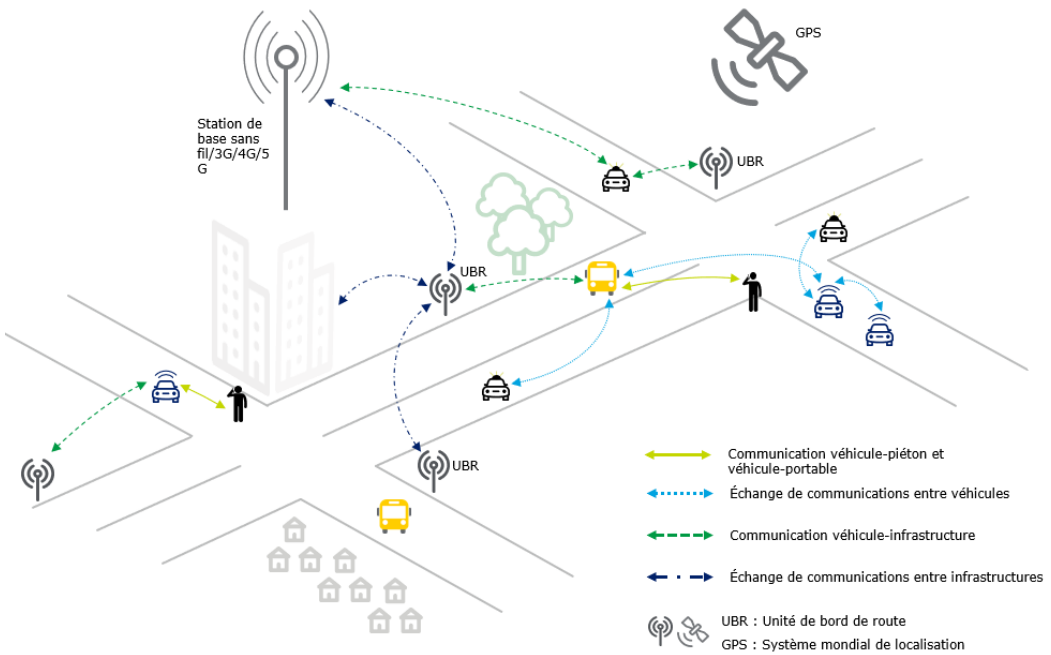
Associations et organismes de normalisation comprend les standards organismes de normalisation et d'accréditation tels que la National Institute of Standards and Technology (NIST), la Society of Automotive Engineers (SAE), et l'Organisation internationale de normalisation (ISO). Il est à noter que certains organismes de normalisation font partie d'organismes du secteur public ou sont financés par lui, tandis que d'autres sont dirigés et gérés par l'industrie.

Paysage de la menace de cybersécurité: VCA Vecteurs d'attaque

Attaques émergentes sur les VCA - Augmentation des attaques à distance et des canaux de communication

Avec l'augmentation du nombre et de la vitesse des canaux de communication avec les véhicules, il y a eu, ces dernières années, une augmentation des attaques malveillantes sur les véhicules. Le nombre d'attaques cybercriminelles (« Black Hat ») a maintenant dépassé le nombre d'attaques fondées sur la recherche (« White Hat ») dans ce domaine, le nombre d'attaques à distance surpassant les attaques physiques sur les véhicules - provenant de distances de plus en plus longues[17]. Il en résulte une augmentation des risques pour les dispositifs, la collecte et le partage des données, ainsi que la sécurité et la protection de la vie privée des personnes concernées par les données.

Canaux de communication VCA



Les VCA font face à une combinaison de problèmes lés à la cybersécurité, la sécurité physique et la protection de la vie privée constitués des composantes uniques à leur écosystème ou à plus grande échelle et impact - en raison du nombre de canaux de communication et du volume et de la sensibilité des données transmises.

Vecteurs d'attaque clés[17]

- les systèmes LIDAR et radar (p. ex. attaques d'usurpation d'identité ou de saturation)
- Serveurs
- Télédéverrouillage
- Port de diagnostic embarqué (OBD)
- Clé OBD
- Application mobile
- Infodivertissement
- Réseau à large bande (p. ex., cellulaire)
- Communication V2X
- Wi-Fi
- Capteurs
- Port USB
- Bluetooth
- Unité de contrôle télématique (TCU)

Les principaux vecteurs d'attaque en 2018, selon un rapport sur la sécurité en amont[17], étaient les attaques de serveurs distants (21 %) et les attaques par télédéverrouillage (19 %), où une personne entre dans une voiture sans utiliser une clé pour la porte ou le contact. Un autre 10 % des attaques ont été effectuées par le port OBD et 7 % par des applications mobiles ou des systèmes d'info-divertissement.

Les attaques de réseaux Wi-Fi et cellulaires ont représenté un peu plus de 4 % chacune, mais pourraient augmenter dans un contexte de connectivité accrue et de couverture 5G. Avec 41% des incidents Black Hat impliquant des serveurs dorsaux en 2019, y compris des serveurs Web OEM piratés, il est nécessaire non seulement d'assurer la sécurité et la sûreté des périphériques, mais aussi d'adopter une approche stratégique globale contre les menaces.

Paysage de la menace de cybersécurité VCA Vecteurs de risque

Risques organisationnels pour l'écosystème VCA

Un VCA est une combinaison d'appareils connectés dans un seul appareil en mouvement - avec un large paysage de menaces. L'écosystème complexe VCA comprend certains défis émergents qui ont un impact sur les organisations du secteur.

Le mélange des domaines de la sécurité physique et de la cybersécurité
Dans un environnement IdO dynamique et connecté, les plates-formes technologiques nouvelles et existantes peuvent exposer une organisation à des risques de sécurité de nature convergente.

Sécurité des données et vie privée
La protection des données des clients, des employés et de l'organisation exige des contrôles de sécurité avancés tout en veillant à ce que les exigences en matière d'intégrité et de confidentialité des données soient prises en compte et conçues dès le départ.

Sophistication des actes du criminel
Bien que la croissance rapide de l'intelligence artificielle (IA) ait aidé les organisations, elle a augmenté la capacité des acteurs de la menace, permettant ainsi une plus grande efficacité des attaques.

Collaboration
La sécurité physique devenant de plus en plus possible grâce à la technologie, une atmosphère de collaboration entre les équipes de sécurité peut optimiser la gestion des menaces.

Culture du risque
Disposer d'une culture du risque appropriée est l'un des principaux facteurs de réussite pour se préparer à de nouveaux risques et y faire face.

Talent
Recruter, former et retenir les meilleurs talents en cybersécurité.

Du point de vue de l'entreprise
Aborder les risques sous l'angle de l'entreprise permet d'avoir une vue d'ensemble des risques, ce qui est nécessaire pour faire face aux menaces émergentes d'aujourd'hui.

Réglementation et justice
Comprendre et mettre à jour le cadre de réglementation et de justice est nécessaire pour assurer un écosystème VCA sûr et sécurisé.

Principales menaces qui pèsent sur l'écosystème VCA

Menaces des initiés : Les initiés ont confiance, ont accès aux connaissances et aux joyaux de la couronne de l'organisation. Les motivations des initiés peuvent varier - ils peuvent voler des données, commettre des fraudes ou causer des dommages physiques ou du sabotage. Détecter des initiés qui se comportent normalement, mais avec des arrière-pensées, peut s' avérer difficile - comme en témoignent des affaires comme le procès secret commercial de Levandowski entre Waymo et Uber.[18]

Cyberattaques dans les communications V2X : Avec beaucoup plus de logiciels embarqués nécessitant des mises à jour régulières en matière de sécurité et de navigation, les véhicules autonomes du nouvel écosystème de la mobilité disposeront probablement de lignes de communication avec le fabricant pour la transmission instantanée des correctifs liés au logiciel. Les vulnérabilités des voies de communication pourraient faire en sorte qu'un acteur de la menace compromette la sécurité et la sûreté des véhicules.

Détournement de capteurs de véhicules et prise en charge des contrôles physiques : L'intersection des capteurs critiques et non critiques du véhicule et des bus sous-jacents peut permettre à un injecteur de messages de transmettre des données indésirables aux dispositifs du véhicule en exploitant le point le plus faible. Les progrès de l'informatique cognitive créent de nouvelles voies visant à exploiter les capteurs et les dispositifs IdO utilisés par les VCA, comme l'ont démontré les chercheurs en incitant les LIDAR des véhicules à faire des jugements imprécis, en utilisant l'usurpation d'identité et des attaques par saturation Cela peut conduire à des accidents physiques par VCA ou des vols des VCA.

Récupération des données dans les poubelles : Tout comme les enregistreurs de données de vol recueillent des informations sur ce qui se passe dans un poste de pilotage, les véhicules connectés enregistrent les détails sur ce que font leurs propriétaires et leurs passagers, ce qui peut servir de pot de miel aux acteurs malveillants : De plus, on a signalé des cas où des conducteurs d'applications de covoiturage ont enregistré secrètement leurs conversations avec leurs passagers, ce qui a des répercussions sur la vie privée.

Risques liés à la chaîne d'approvisionnement et aux tiers : L'écosystème VCA se compose d'une grande variété de fournisseurs de services et de solutions. La gestion des risques liés aux tiers tout au long de la chaîne de valeur s'est révélée difficile pour les entreprises en raison des différents niveaux de maturité des fournisseurs de services, du manque de visibilité et de contrôle des données et des difficultés à appliquer une norme commune en matière de contrôle de sécurité.

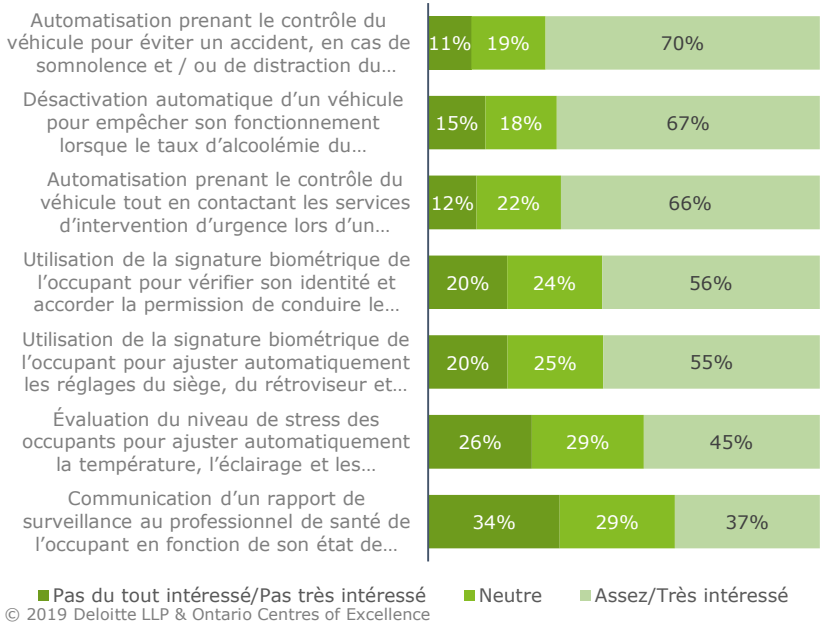
Paysage de la menace de cybersécurité VCA Collecte des données VCA

Confiance des consommateurs et collecte de données sur les véhicules

Les attentes croissantes des consommateurs à l'égard des services connectés et disponibles, tels que les fonctions de sécurité intelligentes et les services de localisation, s'accompagnent d'un manque constant de confiance des consommateurs dans la façon dont leurs données sont traitées une fois collectées par les véhicules.

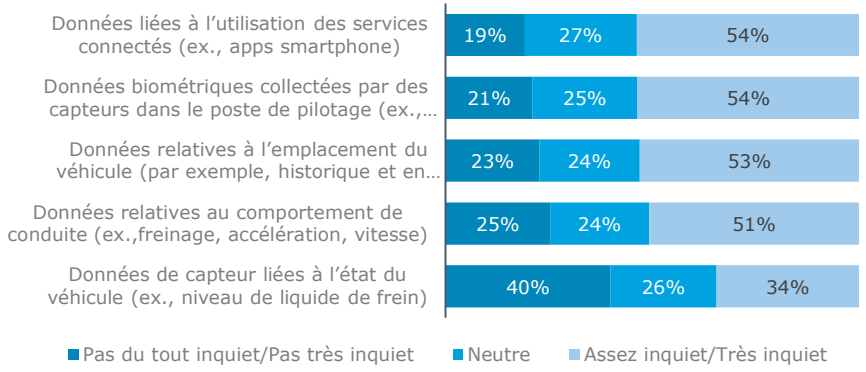
L'Enquête mondiale auprès des consommateurs du secteur automobile de 2019 de Deloitte - qui sonde chaque année 25 000 consommateurs dans 20 pays différents afin de cerner les tendances de l'industrie automobile dans tous les pays et toutes les générations – - révèle que **seulement 27 % des consommateurs canadiens font confiance aux OEM pour gérer les données produites dans un véhicule connecté**, mais que plus des deux tiers des consommateurs canadiens sont intéressés aux avantages proposés par des véhicules connectés.[19] Pour fournir ces avantages, les fournisseurs de services VCA ont besoin d'échanger un grand volume de données - des données potentiellement sensibles - avec le véhicule au fil du temps et à travers les zones géographiques.

Comme l'habitacle des véhicules est équipé de capteurs plus connectés et/ou d'une technologie de conduite autonome, dans quelle mesure êtes-vous intéressé par chacun des éléments suivants ?

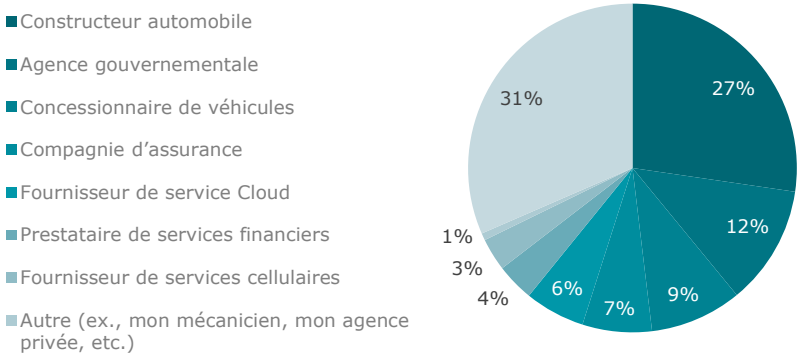


Dans le contexte où les utilisateurs trouvent plus d'avantages aux véhicules connectés d'une année sur l'autre, 45 % de ces consommateurs pensent qu'il est au moins quelque peu important d'avoir la même interface technologique entre plusieurs véhicules – **plus de la moitié des consommateurs ont fait part de leurs préoccupations concernant la collecte et le partage des données relatives aux applications, la biométrie et l'emplacement du véhicule**. Il y a de **réelles préoccupations au sujet des attaques de véhicules lorsqu'ils sont connectés via l'Internet sans fil** – qui sont demeurées constantes au cours des deux dernières années, en dépit de la valeur croissante perçue des véhicules connectés. Le niveau de confiance des consommateurs varie selon le type d'organisation qui traite leurs renseignements.

Dans quelle mesure seriez-vous préoccupé si les types de données suivants étaient partagés avec votre constructeur automobile, votre concessionnaire, votre compagnie d'assurance et/ou d'autres tiers ?



Laquelle des entités suivantes serait la plus à même de gérer les données générées et partagées ?



Paysage de la menace de cybersécurité VCA Tendances et impacts

Tendances dans la cybersécurité VCA et impacts sur les consommateurs et l'industrie

Étant donné que le nombre et la sophistication des menaces de cybersécurité augmentent dans le monde entier, ce qui a des impacts immédiats sur l'industrie croissante VCA : Les consommateurs sont à l'origine de la demande de services automobiles mieux connectés et intégrés, mais à mesure que des informations plus sensibles sur les véhicules et leurs occupants sont collectées et partagées dans un écosystème interconnecté de fournisseurs de services et de constructeurs, les véhicules deviennent une cible de plus en plus précieuse pour les acteurs de la menace. Le paysage de l'industrie est en train de changer en réponse aux demandes des consommateurs et aux cyberdemandes, mais les intervenants hésitent encore à coopérer dans un marché concurrentiel qui repose fortement sur le secret commercial. C'est dans ce contexte que le paysage de la cybermenace continue d'évoluer et de tirer parti des vulnérabilités VCA, y compris un manque de normalisation à travers la réglementation mondiale.

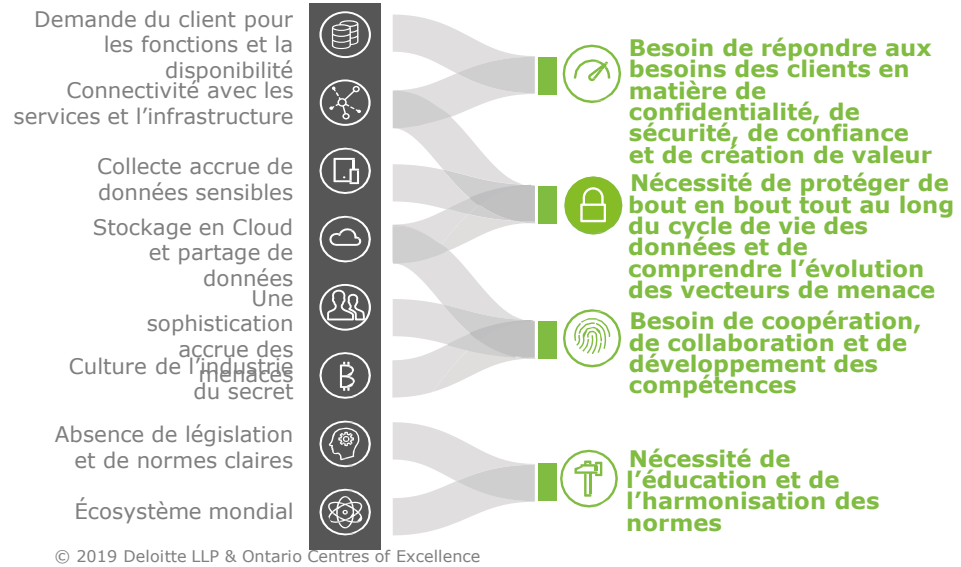
Demande des consommateurs

Compétitivité de l'industrie

Évolution du paysage des menaces

Absence de normalisation réglementaire

Les tendances cybernétiques des VCA ayant une incidence sur les risques existants et la création des besoins des écosystèmes



Influences et impacts de la menace sur les VCA en Ontario

Facteurs clés influençant le risque de cybersécurité dans les villes intelligentes (tiré du rapport de Deloitte intitulé *Making Smart Cities Cybersecure*[20]) :

- **Convergence** : Convergence des infrastructures des technologies de l'information (TI) et des technologies opérationnelles (TO), estompant ainsi le fossé entre le monde physique et le monde cybernétique
- **Interopérabilité** : Coexistence et interactions fréquentes entre les anciens et les nouveaux systèmes et plates-formes
- **Intégration** : Intégration et regroupement de services dans plusieurs domaines grâce à l'IdO et aux technologies numériques

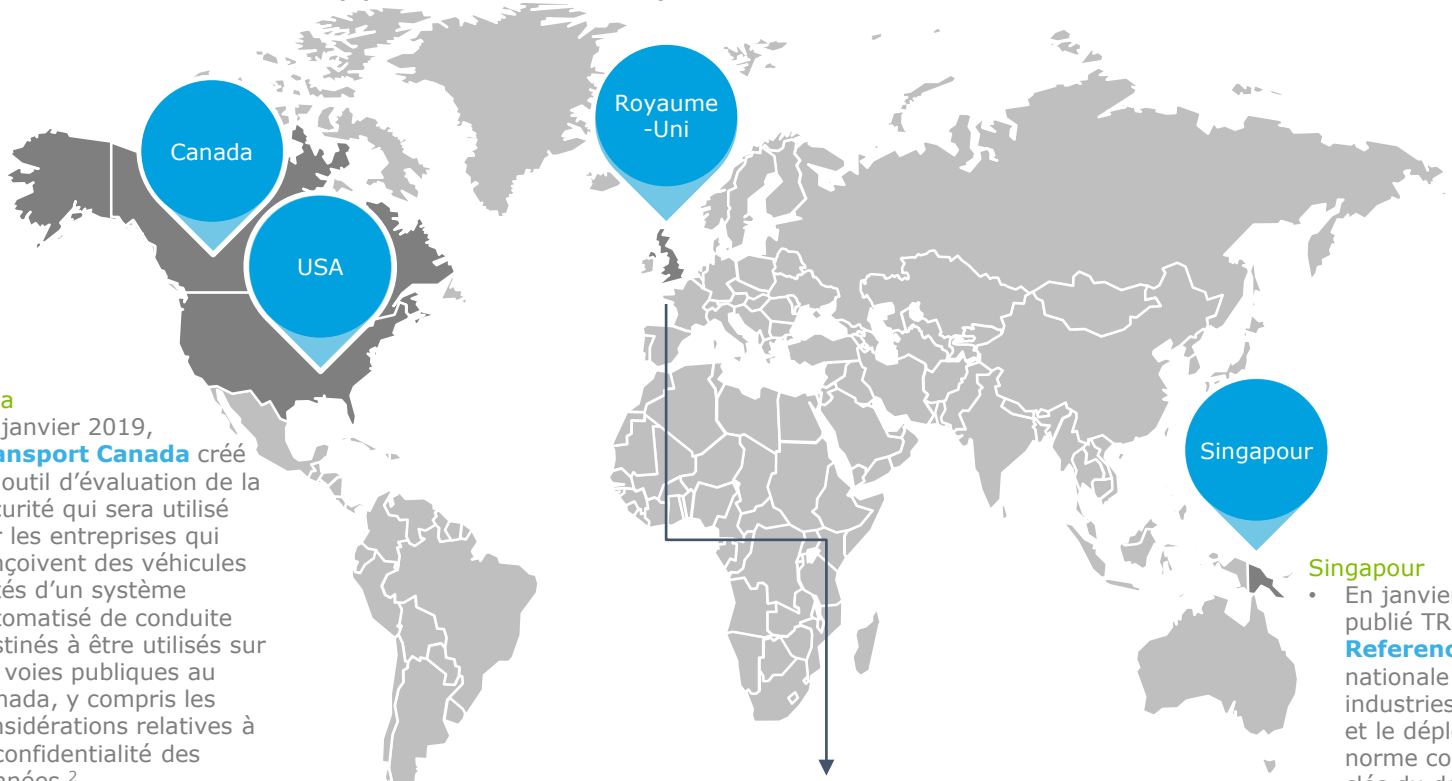
Principaux impacts des menaces qui pèsent sur les consommateurs utilisant des véhicules en réseau (tiré du rapport de Deloitte intitulé *Securing the Networked Vehicle*[21]) :

- **Vol de propriété** : Les acteurs malveillants peuvent voler des véhicules à des fins personnelles ou financières. Le vol de marchandises au Canada représente des pertes économiques de 5 milliards de dollars canadiens par année et il est facilité davantage si les agresseurs peuvent avoir accès à l'emplacement, à l'itinéraire ou au mot de passe d'un véhicule
- **Vol de données** : Les véhicules connectés peuvent saisir et stocker toute une gamme de renseignements personnels, y compris des renseignements sur les transactions et les paiements, les données d'identification des utilisateurs et les communications
- **Destruction physique et sabotage** : Si le contrôle à distance d'un véhicule ou l'accès à son emplacement et à son itinéraire est possible, un acteur malveillant peut gravement endommager le véhicule, ses passagers ou les biens environnants.
- **Atteinte à la vie privée** : Les renseignements personnels, les métadonnées, les adresses à domicile et au travail, et les communications par téléphone mobile pourraient être saisis par les VCA et accessibles sans permission
- **Fraude** : La fraude à l'assurance-automobile pourrait être un problème important, car les estimations de l'assurance reposent de plus en plus sur les données relatives aux véhicules et à mesure que la prévalence du covoiturage augmente

En 2019, les principales répercussions des cyberattaques sur les véhicules ont été **le contrôle non autorisé des systèmes automobiles, le vol de véhicules et les atteintes à la protection des données**.[17]Cela démontre que les cyberattaques ont des répercussions qui vont au-delà des attaques traditionnelles contre la sécurité des réseaux et qu'elles ont des répercussions réelles sur la vie humaine.

Les développements mondiaux de la cybersécurité dans le paysage VCA

Nous avons identifié la législation sur la cybersécurité et le développement d'exigences dans le monde entier en rapport avec l'écosystème VCA.



Canada

- En janvier 2019, **Transport Canada** créé un outil d'évaluation de la sécurité qui sera utilisé par les entreprises qui conçoivent des véhicules dotés d'un système automatisé de conduite destinés à être utilisés sur les voies publiques au Canada, y compris les considérations relatives à la confidentialité des données.[2]

USA

- En octobre 2018, le US Department of Transportation (DOT) a publié le « Automated Vehicles 3.0: **Préparer l'avenir des transports** ». Ce communiqué se concentre sur six principes d'automatisation identifiés par l'USDOT, et fournit également aux représentants du secteur privé des conseils, notamment sur « **L'adoption des meilleures pratiques en matière de cybersécurité** ».[22]

Royaume-Uni

- Les **Principes clés de la cybersécurité pour les véhicules connectés et autonomes** ont été élaborés par le ministère des Transports (DFT) en collaboration avec le Centre pour la protection des infrastructures nationales (CPNI) pour les entreprises impliquées dans la chaîne d'approvisionnement (comme la fabrication, la technologie, etc), vers le développement, l'essai et le déploiement des VCA.[23]
- **La norme PAS 1885:2018 du BSI** doit être lue conjointement avec les Principes clés.[24]

Singapour

- En janvier 2019, Singapour a publié TR68 (**Transport Reference 68**),[25] une norme nationale pour guider les industries dans le développement et le déploiement des VA. Cette norme couvre quatre domaines clés du développement audiovisuel, en mettant l'accent sur la cybersécurité et l'interopérabilité des données: **comportement du véhicule, sécurité fonctionnelle du véhicule, cybersécurité et formats de données**.

La cybersécurité intégrée dans les stratégies et la législation du VCA

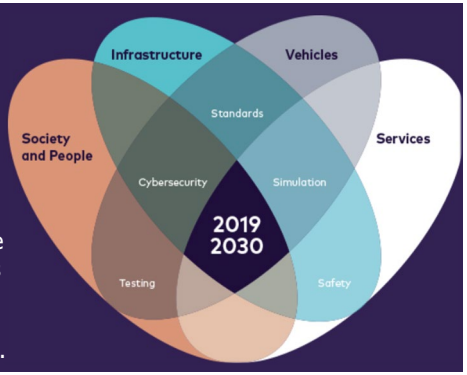
Au Canada et dans le monde, les gouvernements envisagent et intègrent de plus en plus la cybersécurité dans leurs stratégies, outils d'évaluation et lois VCA.

Tendances : Formaliser les meilleures pratiques

Un certain nombre de pays sont en train de rédiger des lois et de publier des directives et des cadres visant à améliorer la recherche, le développement et la mise à l'essai des VCA, et de plus en plus de pays commencent à considérer la cybersécurité comme un élément clé de ces lois, stratégies et directives - dont le Canada, les États-Unis et le Royaume-Uni.

La cybersécurité en tant que composante de base pour une feuille de route VCA – Pleins feux sur le Royaume-Uni

Zenzic (anciennement Meridian Mobility, développé par le gouvernement britannique) se concentrera sur les domaines clés des capacités britanniques dans le secteur mondial des VCA, y compris le développement avancé et la validation, les environnements connectés, les données, la cybersécurité et le développement de nouveaux services. En septembre 2019, ils lanceront leur feuille de route 2019-2030 : **La feuille de route du Royaume-Uni pour une mobilité connectée et automatisée d'ici 2030**, fait de la cybersécurité un pilier clé.



Canada

L'Ontario a coprésidé l'élaboration d'un cadre stratégique canadien pour les VCA, publié en janvier 2019[2], qui définit un ensemble de principes stratégiques que les organismes gouvernementaux canadiens à tous les niveaux peuvent utiliser comme guide pour promouvoir l'essai et le déploiement des VCA au Canada. Ce cadre a mis en lumière les vulnérabilités importantes que sont la cybersécurité et la protection de la vie privée, et a recommandé de sensibiliser davantage le public à ces considérations.

Transport Canada a créé un outil d'évaluation de la sécurité qui sera utilisé par les entreprises qui conçoivent des véhicules dotés d'un système automatisé de conduite destinés à être utilisés sur les voies publiques au Canada.[2] Les résultats de cet outil d'évaluation sont regroupés en trois sections qui comprennent la cybersécurité et la gestion des données, y compris les considérations relatives à la confidentialité des données.

Singapour

Le gouvernement singapourien a apporté une modification à sa *loi sur la circulation routière* qui autorise l'essai des voitures autotractées sur la voie publique en 2017.[26] Le ministère des Transports a publié en février 2017 une série de règles sur les véhicules autonomes (VA) pour permettre la conduite automobile autonome[27] . En outre, la norme nationale de Singapour pour les AV, TR68, a été créée pour promouvoir la sécurité dans le développement et le déploiement des AV à Singapour.[28]

Royaume-Uni

Le Royaume-Uni a créé un service gouvernemental, le Centre for Connected and Autonomous Vehicles, qui travaille sur une législation permettant les essais sur les autoroutes dans le pays. Il existe également des programmes d'essais dans des villes, dont Londres et Coventry, avec des organismes de recherche établis pour développer la technologie et les systèmes. **La feuille de route du Royaume-Uni pour une mobilité connectée et automatisée d'ici 2030** fait de la cybersécurité un pilier clé (voir l'encadré ci-dessus).[29]

États-Unis d'amérique

Depuis 2014, les États-Unis ont connu une forte augmentation de la législation dans l'ensemble de ses États en ce qui concerne les véhicules autonomes ou hautement autonomes. Il y a des villes où des véhicules autonomes ont déjà été déployés et fonctionnent actuellement (p. ex. Ann Arbor). L'élaboration de règles fédérales commence à inclure les exigences du plan de confidentialité et de cybersécurité (ex., la SELF DRIVE Act, pas encore adoptée par le Sénat),[30] et les dossiers montrent qu'en 2018, 15 États ont promulgué 18 projets de loi liés aux VCA.[31]

Normes et réglementations en matière de cybersécurité axées sur l'industrie

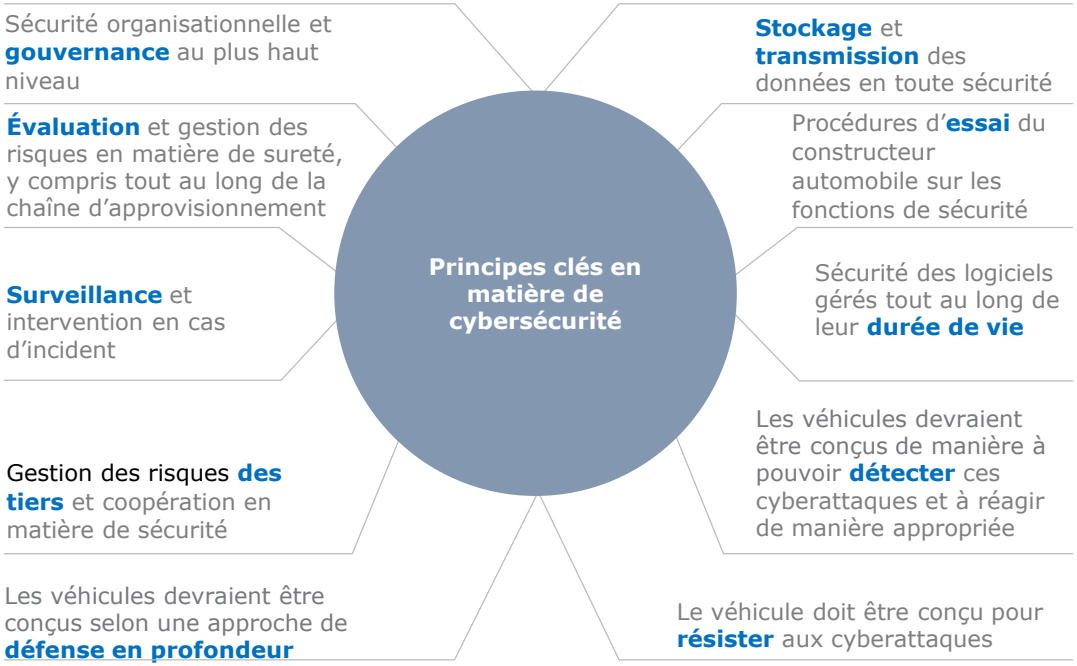
Formalisation des normes axées sur l'industrie

Les associations industrielles et les associations de normalisation du monde entier élaborent d'importantes lignes directrices en matière de cybersécurité qui s'appliquent directement aux VCA:

- **ISO et SAE** développent actuellement une nouvelle norme commune « ISO/SAE 21434 Véhicules routiers - Ingénierie de la cybersécurité ». Cette norme est actuellement en cours d'élaboration.
- **Le Comité des normes de fabrication du Singapore Standards Council (SSC)**, la Land Transport Authority, et la Singapore Manufacturing Federation-Standards Development Organisation (SMF-SDO) ont appuyé l'élaboration des normes techniques de référence 68 (TR68) pour les véhicules autonomes.
- **La British Standards Institution PAS 1885:2018** est destinée à être lue conjointement avec les Principes clés de cybersécurité pour les véhicules connectés et autonomes du Royaume-Uni.[23]
- **Programme de cybersécurité pour l'Internet des objets (IdO) du NIST** « Considerations for a Core IoT Cybersecurity Capabilities Baseline » a été publié en février 2019. Dans le cadre du suivi de l'initiative NIST IR 8228, cette initiative impliquera une collaboration entre le NIST et les parties prenantes afin d'élaborer une base de référence en matière de cybersécurité - un ensemble de capacités de base qui peuvent être largement applicables à de nombreux ou tous les dispositifs IdO avant sa commercialisation.[4]

Pleins feux sur la proposition de règlement des Nations Unies sur la cybersécurité VCA

À l'appui du mandat du Groupe de travail des véhicules automatisés/autonomes et connectés du Forum mondial de l'harmonisation des Règlements concernant les véhicules (WP29) de la Commission économique des Nations Unies pour l'Europe (CEE), les experts de l'Équipe spéciale de la cybersécurité et des questions relatives à la navigation aérienne ont présenté un nouveau projet de règlement sur la cybersécurité en novembre 2018.[32]



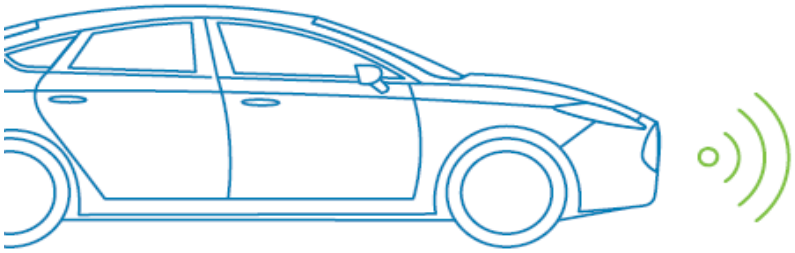
La proposition de règlement des Nations unies élabore des dispositions uniformes concernant l'homologation de la cybersécurité et prévoit l'obligation pour ces parties contractantes de faire évaluer et délivrer par une autorité d'homologation ou un service technique les « certificats de conformité du système de gestion de la cybersécurité ».

Les développements de solutions dans le paysage VCA

Les partenariats et la collaboration entre les parties prenantes VCA sont destinés à faire avancer l'innovation VCA, face aux risques émergents.

L'innovation VCA et le mantra de la coopération

La recherche sur l'intelligence et la logique des VCA a commencé dès les années 1970. Les bases de l'ère de la mobilité en réseau ont été jetées par le projet PROMETHEUS lancé en 1986 par Mercedes-Benz et EUREKA (une organisation intergouvernementale paneuropéenne de coopération internationale en matière d'innovation) et ont ouvert la voie à des technologies comme le régulateur de vitesse et les communications V2X.[33]



Au cours des dernières années, il y a eu de plus en plus de partenariats entre des organisations mondiales alors que les entreprises se précipitent vers la ligne d'arrivée pour lancer des véhicules aux capacités autonomes croissantes et partager les coûts de développement. Voici une liste illustrative de quelques-uns des partenariats récents et majeurs dans l'espace VCA :

- En octobre 2018, Honda s'est engagée à investir 2,75 milliards de dollars dans l'unité autonome Cruise de GM pour développer conjointement une flotte d'auto-propulseurs.[34]
- Waymo (anciennement Google Self-Driving Car Project) s'est associé à Fiat Chrysler début 2018 pour ajouter jusqu'à 62 000 fourgonnettes Chrysler au parc de Waymo ainsi que 20 000 voitures de Jaguar Land Rover[35].
- S'appuyant sur des investissements antérieurs, Toyota a dirigé un financement de 1 milliard de dollars en avril 2019 dans le groupe des technologies de pointe d'Uber pour accélérer la commercialisation des services de covoiturage automatisés.[36]
- En février 2019, BMW et Daimler ont annoncé une coopération sur la technologie sans conducteur complétée par un investissement de 1 milliard de dollars dans une coentreprise pour développer des services de mobilité.[37]

Risques et solutions technologiques émergents pour les VCA

L'utilisation de technologies émergentes telles que la chaîne de blocs, l'impression 5G et 3-D apporte avec eux des défis et des opportunités pour la cybersécurité des VCA.

Par exemple, les solutions de chaîne de blocs peuvent être utilisées pour partager des données entre les VCA, les OEM et les fournisseurs de services, ce qui permet une gestion décentralisée de l'information et l'obtention d'informations précieuses grâce à l'intelligence artificielle et l'apprentissage machine (ML). Dans le même temps, la chaîne de blocs présente des défis traditionnels en matière de cybersécurité, tels que la mise en œuvre de pratiques de gestion clés efficaces, ainsi que des défis technologiques spécifiques tels que le risque de collusion, qu'il convient de surveiller et de prévenir.

Les réseaux 5G, avec leur latence ultra-faible et leurs vitesses accrues, sont prêts à agir comme un facilitateur pour les communications CAV et V2X hyper connectées. Au fur et à mesure que le volume de données collectées et traitées augmente, les défis qu'il pose en matière de protection de la vie privée des utilisateurs doivent être relevés avec soin et une diligence raisonnable doit être exercée pour assurer la sécurité de l'infrastructure et de l'architecture 5G.

La fabrication d'additifs, également connue sous le nom d'impression 3D, permet de créer des composants automobiles plus efficaces en termes de processus et d'énergie. Les chercheurs ont démontré qu'en manipulant malicieusement le code du logiciel 3D blueprint, il est possible d'induire des défaillances mécaniques dans les objets imprimés en 3D.[38] À mesure que l'adoption généralisée de ces technologies augmente, les fournisseurs devraient veiller à ce que les principes de sécurité dès la conception soient intégrés à toutes les étapes de la fabrication.

Implications à la cybersécurité des VCA

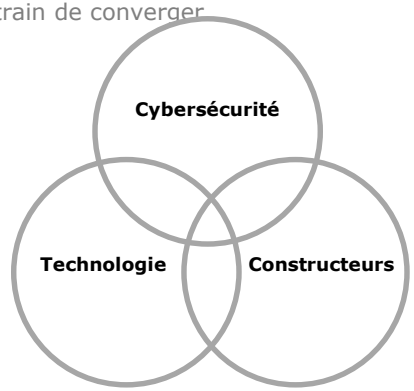
Une collaboration accrue et l'adoption de la sécurité et de la vie privée par les principes de conception entre les acteurs permettra le transfert de connaissances, l'accélération du développement technologique, et aider la cause de l'amélioration de la situation de cybersécurité des VCA.

Modèles d'innovation en matière de cybersécurité des écosystèmes VCA

Tendances clés des innovateurs VCA – domaines d'intérêt et des synergies émergentes entre les industries précédemment en vase clos.

Une approche collaborative à l'innovation liée à la cybersécurité VCA

Dans l'ensemble de la communauté des entreprises en démarrage et en développement, l'innovation dans les domaines de la cybersécurité, de la technologie et de la fabrication, qui se faisait traditionnellement en vase clos, est en train de converger.



Approche collaborative

Les jeunes entreprises cybernétiques offrent leur expertise aux fabricants et travaillent avec les jeunes entreprises technologiques pour mettre au point des technologies qui répondent efficacement aux cybermenaces (ex., intégration des technologies d'IA).

Tendances dans la cybersécurité VCA et innovation en matière de protection de la vie privée

Afin de développer des solutions de cybersécurité adaptées à l'écosystème VCA, les entreprises de technologie et de cybersécurité développent des partenariats innovants avec les fabricants à travers la chaîne d'approvisionnement. Dans certains cas, ces cybersolutions ne nécessitent pas de connexion Internet, réduisent les vecteurs de menaces possibles et utilisent les technologies de l'intelligence artificielle et de la chaîne de blocage pour fournir des solutions de cybersécurité plus efficaces.

Les tendances dans l'écosystème de l'innovation en matière de cybersécurité VCA comprennent :

Partenariats et preuves de concepts (PDC) avec les fabricants

Dans certains cas, aucune connexion Internet n'est nécessaire pour assurer la cyberprotection.

Innovation dans le domaine de la cybersécurité grâce à l'intelligence artificielle et à la chaîne de blocage

Passer des idées, au développement, au marché

De nouvelles solutions dans l'écosystème VCA sont en train de passer des idées, au développement de produits et de services, et enfin à la commercialisation - itération à l'échelle clé et la mise en œuvre des défis.

Innovation des idées

Comprendre les besoins et obtenir la bonne orientation

Recherche et analyse de l'écosystème pour identifier les principaux risques et défis en matière de cybersécurité, et ce qui est nécessaire pour les atténuer avec succès.

Développement de solutions

Bien concevoir le concept

Transformer l'innovation en réalité par la recherche, les essais et le développement; chercher à se lancer sur le marché.

Innovation du marché

Mise à l'échelle de la solution

Une fois la solution affinée et prête à être commercialisée, innover pour répondre aux défis d'interopérabilité, d'échelle et de mise en œuvre.

Voir l'annexe pour une liste des développements d'une solution globale dans la cybersécurité VCA.

Considérations de cybersécurité VCA : Thèmes des principales parties prenantes

Thèmes clés des parties prenantes de l'écosystème élargi

Interrogés sur les risques VCA cybersécurité, par le biais d'entretiens et d'enquêtes, les organisations du secteur privé mettent en évidence les principaux risques à travers le périmètre de sécurité étendu - avec un accent sur la connectivité nuage, la communication de pair à pair, les systèmes d'infotainment, systèmes de sécurité et les données stockées dans les véhicules. La principale leçon tirée des parties prenantes VCA et de la recherche mondiale est que l'ensemble du périmètre de sécurité étendu doit être examiné, avec un accent sur le nuage, dans les véhicules, et la sécurité des réseaux.

L'authentification et la confiance sont quelques-unes des considérations clés

Bien que l'approche de défense en profondeur est bonne en principe, plusieurs intervenants du secteur VCA à travers l'écosystème étendu décrivent les défis autour de l'application de mesures de sécurité patchwork sur les systèmes et dispositifs existants. Cette question se pose particulièrement dans le contexte d'une chaîne d'approvisionnement complexe, où il est difficile de s'assurer que les produits et services tout au long de leur cycle de vie sont sûrs, qu'ils sont ce qu'ils prétendent être et que les communications entre les dispositifs sont authentiques.

Les thèmes clés identifiés par les intervenants dans les entrevues et les réponses à l'enquête sont catégorisés ci-dessous sous les piliers du CCA de Deloitte :

Thèmes clés

Gouvernance

- **Responsabilisation :** Divers rôles sont responsables du cyberespace et de la protection de la vie privée
- **Normes :** De multiples normes sont utilisées et il y a un manque d'harmonisation : L'ISO, le NIST, l'IMSI, l'IETF et l'ETSI ont été notés :
- **Éthique** : Absence de cadres éthiques dans les organisations
- **Maintien en poste et recrutement** : Offre insuffisante et forte demande en matière de cybersécurité; il existe un déficit de compétences.

« Manque de certification, manque de coordination avec d'autres juridictions. Il y a beaucoup de directives et de normes, mais rien à certifier, donc tout est subjectif ». *[Partie prenante]*

Sécurité

- **Authentification et confiance :** La gestion des identités et des accès est un défi majeur dans l'écosystème complexe du VCA
- **Assurance :** Difficultés liées à l'assurance de la chaîne d'approvisionnement; on utilise actuellement la certification, les rapports de vérification et les PDC pour évaluer les fournisseurs.
- **Patching :** correctifs ou des corrections de bogues sont effectués, mais tous les correctifs ne sont pas centralisés ou automatisés
- **Tests d'intrusion :** Des tests d'intrusion (ou piratage éthique) sont effectués pour déceler les vulnérabilités en matière de sécurité, mais le moment choisi dépend de l'organisation

Vigilant

- **Hameçonnage** : Les attaques d'hameçonnage constituent un risque majeur pour toutes les organisations
- **Intelligence de la menace** : La plupart s'abonnent à des fils de nouvelles ou partagent avec des groupes de l'industrie, mais tous n'ont pas un dépôt central et ne prennent pas toutes des mesures en matière de renseignement
- **Mises à jour de sécurité :** Les mises à jour sont effectuées par les fournisseurs de logiciels ou par l'organisation, selon l'entente
- **Surveillance :** Les organisations surveillent les événements liés à la sécurité, mais toutes les activités de surveillance ne sont pas effectuées 24 heures sur 24, 7 jours sur 7 et 365 jours par an

Résilient

- **Gestion de la continuité des opérations (GCA) :** La plupart ont un plan de GCA, mais tous ne sont pas mis à l'essai et mis à jour
- **Intervention en cas d'incident (RI) :** Certains ont des plans de RI cybernétiques, mais ils sont rarement mis à l'essai et seules quelques organisations font des simulations
- **Tests de résistance des fournisseurs :** Les tests de stress ne sont pas toujours effectués ; ils dépendent d'accords avec les fournisseurs

« La protection du flux de trafic de bout en bout et la résilience contre les vecteurs d'attaques multiples » *est l'un des plus grands défis de cybersécurité VCA [partie prenante]*

- Systèmes d'infodivertissement
- Connectivité aux services cloud
- Communication entre pairs (V2V)
- Systèmes de sécurité et de contrôle
- Informations stockées sur le véhicule

Considérations clés mondiales pour la cybersécurité VCA

L'une des considérations clés pour VCA cybersécurité au niveau mondial est la normalisation et la coordination avec d'autres juridictions sur les exigences - les parties prenantes veulent avoir une norme claire et objective à certifier. Les parties prenantes de tous les secteurs et de toutes les administrations ont identifié des possibilités de collaboration entre le gouvernement et l'industrie afin de créer des normes harmonisées et de faire équipe avec une autorité de certification pour élaborer des normes de sécurité et délivrer des certifications, comme c'est actuellement le cas pour les exigences de sécurité fonctionnelle automobile.

Les parties prenantes à travers le paysage VCA sont en train d'identifier la cybersécurité comme un élément essentiel pour assurer la sécurité et la sûreté de l'avenir de la mobilité. Les autorités du gouvernement canadien ont signalé qu'elles pourraient devoir jouer un plus grand rôle dans l'application de la loi ou la vérification des exigences en matière de protection de la vie privée et de sécurité dans le contexte des nouvelles technologies comme les VCA[2], et ont invité les intervenants à travailler ensemble à l'élaboration de futurs cadres stratégiques et orientations.

Aujourd'hui plus que jamais, la cybersécurité est une priorité pour les constructeurs automobiles, car leurs voitures sont de plus en plus connectées au monde extérieur. Les véhicules d'aujourd'hui sont des ordinateurs sur roues – avec plus de 100 millions de lignes de logiciels par voiture. La technologie qu'ils contiennent nous protège, nous divertit et, à bien des égards, commence à nous motiver – pensez aux caractéristiques ADAS comme l'évitement des collisions, la surveillance de l'angle mort et les systèmes d'avertissement de changement de voie qui deviennent rapidement de rigueur chez les constructeurs automobiles avec un œil sur le futur.

Cependant, dans la course à l'auto-conduite, il est tout aussi important d'instaurer la confiance des consommateurs en matière de sécurité que de développer la technologie. Pour que le grand public accepte et, à terme, adopte massivement des véhicules autonomes, il faut avoir confiance dans les technologies, dans leurs avantages et, bien sûr, dans le fait que les entreprises qui les construisent (et qui en profitent) agiront de manière responsable.

***C'est un impératif moral pour ceux d'entre nous qui, au sein de l'industrie, font avancer ce futur qui approche à grands pas, de veiller à ce qu'il soit à la fois sûr et sécuritaire**.*

– Blackberry

Les plus grandes possibilités pour la cybersécurité VCA

Normalisation, certification et législation

Créer une image plus claire des normes et des lignes directrices à suivre, et élaborer un processus de certification et/ou une nouvelle législation pour vérifier et/ou appliquer les normes clés. Au Canada, d'importants travaux sont en cours à Transports Canada pour élaborer et adopter des normes pour de nombreux aspects des VCA ainsi que pour discuter de l'élaboration d'un processus de certification pour les opérations VCA. En collaboration avec ISED, Transports Canada a lancé un groupe de travail sur la cybersécurité des véhicules pour discuter de ces considérations et des solutions possibles avec les experts VCA.

Croissance et fidélisation des talents qualifiés

Avec des universités et des centres d'examen universitaires de premier plan, il est possible de mieux retenir les cyberdoués dans l'industrie automobile – par exemple grâce à des partenariats significatifs entre le milieu universitaire et l'industrie.

Collaboration et partenariats entre les industries

Collaboration de multiples acteurs de différents secteurs d'activité pour innover dans l'espace VCA – des entreprises de cybersécurité, aux OEMs, aux innovateurs de télécom et de paiement.

Mise sur le marché des OEM et de l'innovation technologique

présence et l'innovation existantes parmi les équipementiers et les entreprises technologiques actives au niveau mondial sont considérées comme un avantage significatif – et devraient être encouragées pour la croissance dans ce domaine. Le développement durable de la recherche et du développement sur la cybersécurité du CAV sur le marché devrait être une priorité.

Innovation en matière de niveau de confiance et d'authentification

Mettre au point des processus et outils de confiance et d'authentification en mettant à profit les architectures sécurisées dès leur conception (p.ex., tirer le meilleur parti des infrastructures sécuritaires préexistantes pour assurer l'authentification et l'intégrité).

Test de sécurité de convergence

Transformer et développer les anciens et nouveaux sites d'essais en des installations destinées aux essais de sécurité de convergence afin de veiller à ce que l'ensemble des menaces à la cybersécurité – à l'intérieur et à proximité du véhicule et les interactions avec les infrastructures environnantes – soient prises en compte avant la mise sur le marché d'un VCA.

Protection de la vie privée et sécurité assurées dès la conception; cadres éthiques

Veiller à doter les nouvelles solutions de fonctionnalités destinées à assurer la protection de la vie privée et la sécurité afin de contribuer à la gestion des risques liés à la vie privée et à la sécurité du nombre grandissant de véhicules connectés et autonomes. Élaborer et intégrer des cadres éthiques dans le cycle de vie du développement des solutions au sein des organismes. Par exemple, le Commissariat à la protection de la vie privée du Canada (CPVP) élabore un document d'orientation sur la protection de la vie privée des consommateurs de véhicules connectés et entend élaborer des directives destinées à l'ensemble de l'écosystème des VCA pour les prochaines années.

Principales opportunités pour la cybersécurité des VCA en Ontario

Considérations essentielles liées à la cybersécurité des VCA

L'écosystème des véhicules connectés connaît de l'expansion et l'importance de la cybersécurité dans les technologies novatrices liées au VCA et la croissance du marché se pose dans toute son acuité. Face aux nouvelles menaces, certaines considérations essentielles ajoutent à la complexité de la maîtrise et de la gestion des risques liés à la cybersécurité des VCA. Il s'agit notamment du manque de clarté autour des normes, des difficultés observées dans la formation et la rétention des ressources qualifiées dans ce secteur en Ontario, de la collaboration au sein d'une industrie hautement concurrentielle et de l'établissement et du maintien de la confiance – non seulement des consommateurs, mais à l'égard des produits eux-mêmes et de leurs interactions continues avec les personnes et les objets présents dans l'écosystème environnant.

Thématique propre à l'écosystème	Considérations essentielles
Normalisation et applicabilité	Absence d'exigences unifiées : • Existence de différentes normes internationales et locales • Aucune certification requise pour le moment au Canada • Absence d'un cadre réglementaire clair ainsi que de son application • Chaîne d'approvisionnement élargie et écosystème constitué de fournisseurs et de prestataires de services variés (p.ex., télécom., paiements) ayant des exigences diverses
Formation et développement	Difficulté à attirer et à retenir les talents en cybernétique : • Inadéquation entre la demande (forte) et l'offre (insuffisante) de talents en cybersécurité • Difficulté à retenir les talents dans l'industrie • Inadéquation entre le travail académique et l'occupation durable de postes dans l'industrie
Transparence et collaboration	Manque de transparence et de coopération relativement aux défis posés par la cybersécurité dans le secteur automobile : • Corrélation faible entre la recherche/le monde universitaire et l'industrie • Manque de partage d'expérience entre les différents FEO et les prestataires de services en raison de la concurrence • Manque de transparence à l'égard des principaux défis posés par la cybersécurité par crainte de vulnérabilité face à la concurrence ou aux acteurs malveillants
Confiance	Difficulté à garantir l'offre de produits et de services sur toute la chaîne d'approvisionnement ainsi que la confiance entre les prestataires et les communications, en raison de la complexité de l'environnement et des communications requises (p.ex., V2I, V2V) pour assurer la circulation d'un VCA et la réception de ses mises à jour.

Principales opportunités de promotion de la cybersécurité des VCA en Ontario

Sensibilisation des entreprises à la protection de la vie privée et à la sécurité et amélioration du niveau de maturité

Aider les entreprises ontariennes à mieux comprendre les risques et lacunes en matière de cybersécurité, leurs responsabilités et comment intégrer l'aspect protection de la vie privée et sécurité dans leurs produits ou services et structures, par le biais de la formation et de la sensibilisation. Par exemple, l'Ontario a coprésidé le groupe de travail sur l'élaboration du cadre stratégique des VCA du CSPP[2], mettant en exergue la nécessité de prise de conscience.

Partenariats transfrontaliers basés sur la cybersécurité des VCA

Promouvoir l'investissement stratégique et les partenariats opérationnels avec divers gouvernements, centres académiques, plateformes de cybersécurité et secteurs d'une frontière à l'autre.

Stages et placements axés sur la cybersécurité des VCA

Soutenir des partenariats industriels durables en vue de la formation et de la rétention des meilleurs talents en cybernétique dans l'industrie automobile. En Ontario, le gouvernement finance de multiples programmes, tels que le programme de développement des talents du RIVA, et a également manifesté son engagement à mobiliser et à développer les talents dans le secteur automobile par le truchement de son programme dédié au secteur automobile, *Piloter la prospérité*.[39]

Normalisation et un processus de certification inhérent à la cybersécurité des VCA

Collaborer à tous les niveaux du gouvernement afin de participer à l'élaboration de nouvelles lois et directives harmonisées visant à clarifier les normes et responsabilités nationales et à réduire les obstacles à l'innovation en encourageant un développement sécuritaire de produits et de services. Par exemple, les intervenants dans le secteur des VCA et les décideurs en Ontario continuent de faire partie des groupes de travail afin d'apporter leur expérience en vue de l'adoption de la meilleure stratégie de développement et d'établissement des cadres importants relatifs aux VCA.

Recherche, mise à l'essai et développement dans la filière de la cybersécurité des VCA

L'expansion de la capacité des laboratoires et des centres d'essais de véhicules existants visant à favoriser la mise à l'essai des technologies de cybersécurité contribuera à accélérer le progrès dans cette filière et à attirer des talents et les géants de l'industrie. Par exemple, par le biais du programme de financement du partenariat de R-D du RIVA de l'Ontario, les intervenants de la filière des VCA ont l'opportunité de s'associer et de collaborer afin de développer, de mettre à l'essai et de commercialiser les nouvelles technologies dans la filière. Le Centre d'excellence de l'automobile (CEA) logé à l'Institut universitaire de technologie de l'Ontario met la recherche en cybersécurité en pratique en commençant par l'intégration des tests de cybersécurité dans son installation. *Pour obtenir des renseignements complémentaires sur les opportunités de convergence dans les centres d'essai, veuillez vous reporter à l'Annexe.*

Conclusion

La cybersécurité des VCA nécessite la collaboration entre tous les intervenants de l'ensemble de l'écosystème des VCA

Conclusion

La technologie des véhicules connectés et autonomes a la capacité de renforcer la sécurité et l'efficacité de la mobilité. Pourtant, un certain nombre de nouvelles menaces à la cybersécurité plane sur l'industrie prospère des VCA - sur l'intégralité de la chaîne d'approvisionnement - ajouté à l'augmentation des points de service physiques et numériques.

Compte tenu des considérations complexes d'ordre technique, réglementaire et organisationnel, les intervenants de l'écosystème des VCA devront nouer des partenariats en vue de la gestion et de la lutte contre les menaces à la sécurité. Pour ce faire, la question de la cybersécurité dans l'écosystème des VCA requiert une attention collaborative harmonisée, plutôt que des initiatives de développement et de croissance autarciques.

La collaboration comprend l'établissement de partenariats avec divers secteurs et domaines de spécialité, la coopération avec et au sein des gouvernements par le biais de l'élaboration d'approches visant la normalisation et l'application de la réglementation dans les industries dédiées aux VCA et la collaboration avec le monde universitaire, afin de créer et de renforcer les centres d'essais, la recherche ainsi que le développement des talents afin de mieux comprendre les menaces physiques et cybernétiques qui pèsent sur la technologie des VCA.

Prochaines étapes pour l'Ontario

Les intervenants de la filière de la cybersécurité des VCA en Ontario nous révèlent qu'il reste du travail en ce qui a trait à la clarté des exigences, des partenariats et du soutien à la cybersécurité des VCA - mais que la province regorge également d'opportunités lui permettant de demeurer la plaque tournante dans cette filière essentielle au succès et à l'adoption des VCA à travers le monde.

Par exemple, grâce au RIVA, le gouvernement de l'Ontario a réalisé des progrès importants dans le développement de ces opportunités et la stimulation de la croissance en Ontario. À mesure que la cybersécurité des VCA poursuit sa trajectoire ascendante et suscite un intérêt croissant des gouvernements, des leaders de l'industrie et du monde universitaire, ainsi que du public, le RIVA entend intensifier ses efforts de mobilisation de l'ensemble de l'écosystème des VCA afin de garantir l'avancement de la cybersécurité des VCA en Ontario.

Notes de fin de document

1. *Véhicules automatisés et connectés 101 Transports Canada 2019*. Disponible à l'adresse suivante : https://www.tc.gc.ca/en/services/road/innovative-technologies/automated-connected-vehicles/av-cv-101.html

2. *Des évolutions récentes ont eu cours dans le système fédéral canadien, notamment :*

   - *Paver la voie : Technologie et le futur du véhicule automatisé.* Le Sénat du Canada 2018. Rapport du comité sénatorial permanent des transports et des communications. Le rapport est disponible à l'adresse suivante : https://sencanada.ca/en/info-page/parl-42-1/trcm-driving-change/
   - *Évaluation de la sécurité des systèmes de conduite automatisés au Canada. Transports Canada 2019*. Disponible à l'adresse suivante : https://www.tc.gc.ca/en/services/road/documents/tc_safety_assessment_for_ads-s.pdf (version française disponible)
   - *Cadre stratégique des véhicules automatisés et connectés pour le Canada.* Rapport du groupe de travail du CSPP sur les véhicules automatisés et connectés 2019. Disponible à l'adresse suivante : http://publications.gc.ca/collections/collection_2019/tc/T42-13-2019-eng.pdf (version française disponible)
   - *Statement by Minister Bains and Minister Gould on the Privacy Commissioner findings on Facebook privacy practices. ISDE Canada 2019*. Disponible à l'adresse suivante : https://www.canada.ca/en/innovation-science-economic-development/news/2019/04/statement-by-minister-bains-and-minister-gould-on-the-privacy-commissioner-findings-on-facebook-privacy-practices.html,
   - *Charte numérique du Canada en action.* Gouvernement du Canada 2019. Disponible à l'adresse suivante : https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html

3. *World Economic Forum Global Risks Report 2019. WEF 2019*. Disponible à l'adresse suivante : https://www.weforum.org/reports/the-global-risks-report-2019

4. *Consideration for managing IoT Cybersecurity and Privacy Risks. NIST 2018*. Disponible à l'adresse suivante : https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8228-draft.pdf. Pour en savoir plus, veuillez consulter les adresses suivantes : https://www.nist.gov/blogs/i-think-therefore-iam/dont-leave-us-our-own-devices-seeking-feedback-draft-nistir-iot, et https://www.nist.gov/blogs/i-think-therefore-iam/lets-talk-about-iot-device-security

5. *SAE International Releases Updated Visual Chart for Its "Levels of Driving Automation" Standard for Self-Driving Vehicles. The Society of Automotive Engineers (SAE) 2018.* Disponible à l'adresse suivante : https://www.sae.org/news/press-room/2018/12/sae-international-releases-updated-visual-chart-for-its-"levels-of-driving-automation"-standard-for-self-driving-vehicles. Pour examiner la taxonomie détaillée, veuillez consulter la ressource suivante : *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016_201806.* Disponible à l'adresse suivante : https://www.sae.org/standards/content/j3016_201806/. Pour obtenir un aperçu des niveaux d'automatisation de la conduite de la SAE, veuillez consulter la source : *Automated Vehicles for Safety – The Road to Full Automation. National Highway Traffic Safety Administration (NHTSA) 2019*. Disponible à l'adresse : https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety

6. *Securing the future of mobility. Deloitte 2017*. Disponible à l'adresse : https://www2.deloitte.com/insights/us/en/focus/future-of-mobility/cybersecurity-challenges-connected-car-security.html

7. *The state of autonomous legislation in Europe. Auto Vista Group 2019.* Disponible à l'adresse suivante : https://autovistagroup.com/news-and-insights/state-autonomous-legislation-Europe

8. *Australian trials and policy development. Gouvernement australien 2017*. Disponible à l'adresse suivante : https://www.austrade.gov.au/future-transport/connected-automated-vehicles/

9. *New legislation allows for testing of cars with remote drivers.* Gouvernement des Pays-Bas 2017. Disponible à l'adresse suivante : https://www.government.nl/latest/news/2017/11/22/new-legislation-allows-for-the-testing-of-cars-with-remote-drivers

10. *Bikes but spanner in works of Dutch driverless car schemes. The Guardian 2019*. https://www.theguardian.com/world/2019/feb/13/bikes-put-spanner-in-works-of-dutch-driverless-car-schemes

11. *Centre to reintroduce motor vehicle bill in-house. Hindustan Times 2019*. Disponible à l'adresse suivante https://www.hindustantimes.com/india-news/centre-to-reintroduce-motor-vehicle-bill-in-house/story-Jn6p2G7BGflapEglgSuiIL.html

12. *Autonomous vehicles gaining more ground. China Daily 2019*. Disponible à l'adresse suivante : http://www.chinadaily.com.cn/a/201901/15/WS5c3d2bb0a3106c65c34e46e2.html. Veuillez également consulter : *China Releases National Automatic Vehicle Road Testing Rules. The National Law Review 2018.* Disponible à l'adresse : https://www.natlawreview.com/article/iot-update-china-releases-national-automatic-vehicle-road-testing-rules

13. *Japan enacts bill to allow use of smartphones under some circumstances in self-driving cars. The Japan Times 2019*. Disponible à l'adresse : https://www.japantimes.co.jp/news/2019/05/29/national/japan-enacts-bill-allow-use-smartphones-circumstances-self-driving-cars/#.XR5b-ehKhPY. Veuillez également consulter : *Japan edges closer towards brave new world of self-driving cars but hard questions remain. South China Morning Post 2019*. Disponible à l'adresse : https://www.scmp.com/news/asia/east-asia/article/2180828/japan-edges-closer-towards-brave-new-world-self-driving-cars

14. *Ontario's Automated Vehicle Pilot Program. Ministère des Transports de l'Ontario 2019. Disponible à l'adresse suivante : www.mto.gov.on.ca/english/vehicles/automated-vehicles.shtml.*

15. *Programme pilote ontarien pour la circulation des camions en convoi automatisé.* Ministère des Transports de l'Ontario 2019. Disponible à l'adresse : http://www.mto.gov.on.ca/english/trucks/cooperative-truck-platooning.shtml (version française disponible)

16. *Harnessing the cybersecurity opportunity for growth. Ontario Centres of Excellence 2016*. Disponible à l'adresse suivante : https://www.oce-ontario.org/docs/default-source/publications/final_oce_tfsa_cyber-innovation-report_v6-2.pdf?sfvrsn=2

17. *Global Automotive Cybersecurity Report. Upstream Security 2019*. Disponible à l'adresse : https://industrytoday.com/wp-content/uploads/2018/12/Upstream-Security-Global-Automotive-Cybersecurity-Report-2019.pdf

18. *Uber and Waymo Settle Trade Secrets Suit Over Driverless Cars. The New York Times 2018*. Disponible à l'adresse suivante : https://www.nytimes.com/2018/02/09/technology/uber-waymo-lawsuit-driverless.html

Notes de fin de document

19. *Deloitte Global Automotive Consumer Survey (Canadian Data). Deloitte 2019*. Disponible à l'adresse : https://www2.deloitte.com/us/en/pages/manufacturing/articles/automotive-trends-millennials-consumer-study.html

20. *Making smart cities cybersecure: Ways to address distinct risks in an increasingly connected urban future. Deloitte 2019*. Disponible à l'adresse suivante : https://www2.deloitte.com/insights/us/en/focus/smart-city/making-smart-cities-cyber-secure.html

21. *Securing the networked vehicle: The Threat Landscape. Deloitte 2016*. Sommaire disponible (et rapport complet disponible sur demande) à l'adresse : https://www.linkedin.com/pulse/securing-networked-vehicle-nick-deshpande

22. *Preparing for the future of transportation. WSP 2018.* Disponible à l'adresse : http://www.wsp.com/-/media/Sector/US/Document/Summary-of-USDOTs-Automated-Vehicles-30.pdf

23. *The Key Principles of Cyber Security for Connected and Automated Vehicles. Gouvernement britannique 2018*. Disponible à l'adresse suivante : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/661135/cyber-security-connected-automated-vehicles-key-principles.pdf

24. *The fundamental principles of automotive cybersecurity. British Standards Institution (BSI) 2018*. Peut être acheté à l'adresse suivante : https://shop.bsigroup.com/ProductDetail/?pid=000000000030365446&_ga=2.267667464.704902458.1545217114-2008390051.1545217114

25. *How the Land Transport Authority's (LTA's) Technical Reference 68 fueled Singapore's autonomous vehicle agenda. Techwire Asia 2019*. Disponible à l'adresse suivante : *https://techwireasia.com/2019/03/how-the-ltas-tr68-fuelled-singapores-autonomous-vehicle-agenda*

26. *The Country Best Prepared for Autonomous Vehicles. Forbes 2018.* Disponible à l'adresse suivante https://www.forbes.com/sites/niallmccarthy/2018/10/23/the-countries-best-prepared-for-autonomous-vehicles-infographic/#1a68dc4c3df2

27. *How Singapore is driving the development of Autonomous Vehicles. CIO - IDG Communications 2019.* Disponible à l'adresse suivante : https://www.cio.com/article/3294207/how-singapore-is-driving-the-development-of-autonomous-vehicles.html

28. *Singapore develops provisional national standards to guide development of fully autonomous vehicles. Land Transport Authority 2019*. Disponible à l'adresse suivante : *https://www.lta.gov.sg/apps/news/page.aspx?c=2&id=8ea02b69-4505-45ff-8dca-7b094a7954f9*

29. *The UK Connected and Automated Mobility Roadmap to 2030. Zenzic UK* 2019. Disponible à l'adresse suivante : https://triangle.ifourhosting.co.uk/what-we-do/uk-connected-and-automated-mobility-roadmap

30. *H.R.3388 - SELF DRIVE Act, 115th Congress. 2017-2018. (Passed by the U.S. House of Representatives, not yet passed by the Senate. Latest Action: Received in the Senate; read twice and referred to the Committee on Commerce, Science, and Transportation).* Disponible à l'adresse suivante : https://www.congress.gov/bill/115th-congress/house-bill/3388/text.

31. *Autonomous vehicles | Self driving vehicles enacted legislations. National Conference of State Legislation 2019*. Disponible à l'adresse suivante : http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

32. *Draft proposal to introduce a Regulation on Cyber Security. United Nations Economic and Social Council 2018*. Disponible à l'adresse suivante : https://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29grva/ECE-TRANS-WP29-GRVA-2019-02e.pdf. Pour examiner le cadre, veuillez également consulter : *Framework document on automated/autonomous vehicles.* 2019. Disponible à l'adresse suivante : https://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29/WP29-177-19e.pdf

33. *The PROMETHEUS project launched in 1986: Pioneering autonomous driving. Daimler AG 2016.* Disponible à l'adresse suivante : https://media.daimler.com/marsMediaSite/en/instance/ko/The-PROMETHEUS-project-launched-in-1986-Pioneering-autonomous-driving.xhtml?oid=13744534

34. *Honda to invest $2.75 billion in GM's self-driving car unit. Reuters 2018.* Disponible à l'adresse suivante : https://www.reuters.com/article/us-gm-autonomous/honda-to-invest-2-75-billion-in-gms-self-driving-car-unit-idUSKCN1MD1GW

35. *Waymo expands autonomous driving partnership with Fiat Chrysler. TechCrunch 2018.* Disponible à l'adresse suivante : https://techcrunch.com/2018/05/31/waymo-expands-autonomous-driving-partnership-with-fiat-Chrysler

36. *Uber self-driving tech group receives $1B investment led by Toyota. CNET 2019.* Disponible à l'adresse suivante : https://www.cnet.com/roadshow/news/uber-1bn-investment-self-driving-cars-toyota-denso

37. *BMW and Daimler team up on cars of the future to fend off Silicon Valley. CNN 2019.* Disponible à l'adresse suivante : https://www.cnn.com/2019/02/28/business/bmw-daimler-driverless-cars/index.html

38. *The Threat 3-D Printing Could Pose To Global Security. Forbes 2018*. Disponible à l'adresse suivante : https://www.forbes.com/sites/jenniferjohnson/2018/05/29/does-3-d-printing-present-a-threat-to-global-security/#155eb4ad2535

39. *Piloter la prospérité : L'avenir du secteur de l'automobile de l'Ontario.* Gouvernement de l'Ontario 2019. Disponible à l'adresse suivante : https://news.ontario.ca/medg/en/2019/02/driving-prosperity-the-future-of-ontarios-automotive-sector.html (version française disponible)

40. *The London Office For Rapid Cybersecurity Advancement (LORCA) 2019.* Disponible à l'adresse : https://www.lorca.co.uk/what-we-do/

41. *Angoka 2019.* Disponible à l'adresse : http://angoka.io/

42. *Argus 2019.* Disonible à l'adresse : https://argus-sec.com/argus-solution-suites/

43. *Dellfer 2019*. Disponible à l'adresse : https://dellfer.com/

44. *ISARA 2019.* Disponible à l'adresse : https://www.isara.com/

Notes de fin de document

45. *Regional Technology Development Sites. Autonomous Vehicle Innovation Networks 2019.* Disponible à l'adresse suivante : https://www.avinhub.ca/regional-technology-development-sites/#el-531e46b1

46. *Ryerson University Announces $30 Million in Public and Private Support for Rogers Cybersecure Catalyst. Ryerson University 2019.* Disponible à l'adresse suivante : https://www.ryerson.ca/cybersecure-catalyst/news/rogers-cybersecure-catalyst/

47. *Autonomous Vehicle Innovation Centre (AVIC). Blackberry QNX 2019.* Disponible à l'adresse suivante : http://blackberry.qnx.com/en/blackberry-qnx-autonomous-vehicle-innovation-centre

48. *Blackberry QNX and Blackberry Certicom 2019.* Disponible à l'adresse suivante : https://blackberry.qnx.com/en and https://blackberry.certicom.com/

49. *CloudGRC Inc. 2019.* Disponible à l'adresse suivante : https://www.cloud-grc.com/automotive-industry/

50. *ESCRYPT 2019.* Disponible à l'adresse suivante : https://www.escrypt.com/en/industries/automotive-security and https://www.escrypt.com/en/news-events/transport-canada-contract

51. *EZFleet - Fleet management solutions for autonomous vehicles. Easymile 2019.* Disponible à l'adresse suivante : https://easymile.com/solutions-easymile/ezfleet-by-easymile

52. *Bigchaindb 2019.* Disponible à l'adresse suivante : https://www.bigchaindb.com/features/

53. *SAFERIDE technologies 2019.* Disponible à l'adresse suivante : https://saferide.io/

54. *Centri 2019.* Disponible à l'adresse suivante : https://www.centritechnology.com/company-about-centri/

55. *ARXAN 2019.* Disponible à l'adresse suivante : https://www.arxan.com/

56. *NVIDIA 2019.* Disponible à l'adresse suivante : https://www.nvidia.com/en-us/about-nvidia/

57. *Mitsubishi 2019.* Disponible à l'adresse suivante : https://www.mitsubishi-motors.com/en/index.html

58. *Trillium 2019.* Disponible à l'adresse suivante : https://trilliumsecure.com/solutions/

59. *AT&T Ventures into the Connected Car Industry in Mexico. The Fast Mode 2018.* Disponible à l'adresse suivante : https://www.thefastmode.com/services-and-innovations/13148-at-t-ventures-into-the-connected-car-industry-in-mexico

60. *Jooycar 2019.* Disponible à l'adresse suivante : https://jooycar.com/

61. *SOS LAB Secures $6M in Series A Funding Round. Business Wire 2018.* Disponible à l'adresse suivante : https://www.businesswire.com/news/home/20181005005114/en/SOS-LAB-Secures-6M-Series-Funding

62. *CUBE NEWS – Monthly Report March 2019. Cube Intelligence 2019.* Disponible à l'adresse suivante : https://blog.cubeint.io/2019/03/cube-news-monthly-report-march-2019.html

63. *Quantoz 2019*. Disponible à l'adresse suivante : https://quantoz.com/

Termes clés

- **VA** – Véhicule autonome ou véhicule automatisé
  - Les autres termes couramment utilisés pour désigner un VA comprennent : les voitures sans conducteurs, les véhicules hautement automatisés (VHA), les systèmes de conduite automatisés (SCA).
- Les réseaux de zombies - un type de logiciel malveillant qui prend le contrôle d'une machine hôte et l'utilise pour perpétrer des attaques, envoyer des pourriels, dérober les données, etc.
- **VCA** – Véhicule connecté et autonome
- **Déni de service distribué (DDOS) –** Un volume de requêtes Internet trop important, généralement envoyé par un réseau de zombies, visant à faire planter un système afin de rendre un site Web ou un réseau muet.
- **Menaces internes** – Un compte utilisateur interne d'une entité (employé, contractant, etc.) qui exécute une attaque, soit via le propriétaire du compte ou suite à la compromission du compte faisant l'objet d'une attaque d'un pirate externe.
- **IdO** – Internet des objets.
- **LIDAR** – Détection et télémétrie par ondes lumineuses; méthode de télédétection qui utilise la lumière pour mesurer les distances
- **Maliciel** – Tout type de logiciel malveillant.
- **Attaque de maliciels** – Présence massive de logiciels malveillants sur plusieurs ordinateurs ou système au sein d'une organisation.
- **FEO** – Fabricant d'équipement d'origine.
- **Hameçonnage** – Une attaque au cours de laquelle un individu malveillant essaie de convaincre un employé du fait qu'une communication (par courriel, appel téléphonique, etc.) provient d'une source licite afin de l'amener à suivre les instructions données.
- **Logiciel rançonneur**– Un type de programme malveillant qui chiffre les données d'un poste et invite la victime à verser une rançon pour obtenir la clé de déchiffrement.
- Unité de bord de route (UBR) - Les unités de bord de route assurent des communications sans fil entre des infrastructures situées à proximité des routes et des systèmes de véhicules connectés. Les UBR communiquent avec les mobimètres ou les systèmes de diagnostic embarqué (OBD) des véhicules afin d'obtenir des renseignements tels que le temps, la vitesse, l'emplacement afin de faciliter les interventions comme la prévention des collisions.
- **SAE** – Society of Automotive Engineers.
- **Convergence de sécurité** – L'association de la cybersécurité et de la sécurité physique.
- **Mystification** – Une forme d'attaque (qui s'opère généralement sur le réseau) au cours de laquelle un utilisateur, un système ou une connexion fait l'objet d'une duperie par la falsification des données avec pour objectif l'obtention d'un avantage illicite.
- **TCU** – Une unité de contrôle télématique est un système intégré à un véhicule qui transmet et interprète les données au sein de ce véhicule ou celles communiquées ou reçues par des serveurs situés à l'extérieur du véhicule, par exemple, des données provenant des FEO destinées à la réalisation des mises à jour logicielles par radiocommunication.
- **Panorama des menaces** – Identification des menaces en fonction des tendances observées sur l'ensemble de l'écosystème
- **V2I** – Communication véhicule-infrastructure.
- **V2V** – Communication entre véhicules.
- **V2X** – Communication entre un véhicule et toute chose.
- **FEM** – Forum économique mondial.

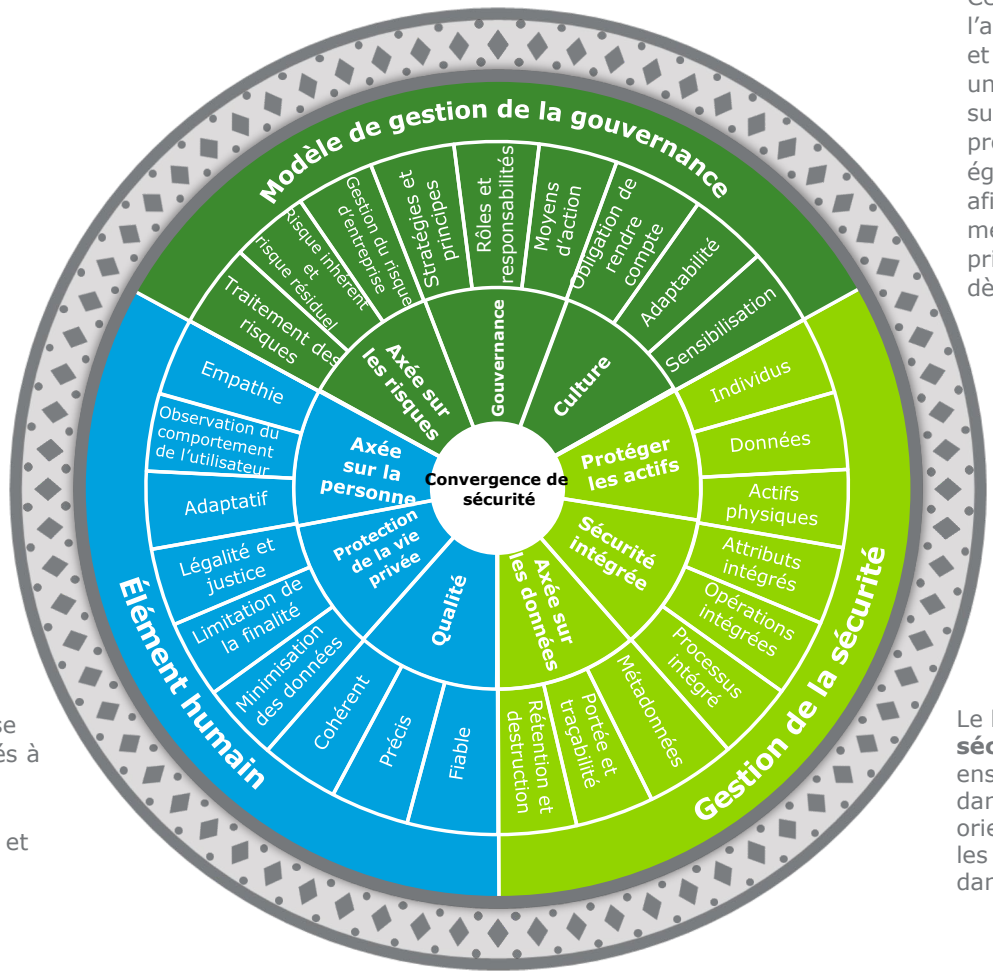
Annexe

Un cadre de convergence de sécurité pour l'écosystème des VCA

Le cadre global de Deloitte – convergence de sécurité, cybersécurité et protection de la vie privée dès la conception – peut être utilisé pour faciliter la compréhension des différents aspects de la sécurité physique, de la cybersécurité et de la protection de la vie privée dès la conception, dans l'ensemble de l'écosystème.

La nécessité d'un cadre de cybersécurité de convergence

La complexité de l'écosystème des VCA nécessite un cadre qui considère la **Convergence de sécurité** (l'association de la sécurité physique et de la cybersécurité) et la **Protection de la vie privée dès conception**, comme les principaux piliers du cadre stratégique robuste relatif à la cybersécurité (du style du CSC de Deloitte).



Ce cadre prend en compte l'association de la sécurité physique et de la sécurité numérique qui ont une incidence sur les VCA ainsi que sur la stratégie de cybersécurité propre à l'entité - laquelle nécessité également un cadre hautement fiable afin de veiller à ce que des mécanismes de protection de la vie privée et de sécurité soient conçus dès la phase initiale.

L'association de ces cadres favorise l'analyse des principaux risques liés à l'ensemble de la chaîne d'approvisionnement en VCA, aux multiples voies de communication et aux cycles de vie complexes des données.

Le **bouclier de Convergence de sécurité** de Deloitte offre un ensemble global de neuf principes dans trois domaines visant à orienter et à évaluer la maturité et les capacités d'une organisation dans sa quête de convergence.

Un cadre de convergence de sécurité pour l'écosystème des VCA

Une description détaillée des composants du cadre de Convergence de sécurité de Deloitte :

L'**élément humain** vise les prestataires et les consommateurs de services – les personnes, afin de veiller à ce que la conception soit centrée sur la personne, respecte sa vie privée et garantit le maintien de la qualité des données qui sont à la base de la prise de décisions.

Approche centrée sur la personne

Veiller à ce que les solutions, les conceptions et les processus offrent aux utilisateurs une interface intuitive et adaptative est crucial pour accroître la participation et l'adoption d'une approche efficace basée sur la convergence

Protection de la vie privée

Assurer la *Protection de la vie privée dès la conception* est indispensable pour obtenir et maintenir la confiance des personnes afin qu'elles partagent leurs données et pour satisfaire aux exigences réglementaires telles que le RGPD

Qualité

La qualité des décisions dépend de la qualité des données sur lesquelles celles-ci reposent et par conséquent, il est essentiel de veiller à ce que les données permettant d'implémenter les algorithmes soient cohérentes, fiables et précises.

La **Gestion de la sécurité** renvoie à la protection des meilleurs actifs de la société au moyen d'un système connecté et axé sur les données ainsi que d'une approche de sécurité intégrée.

Approche axée sur les données

Dans le but d'assurer l'exactitude des données et l'obtention de résultats pertinents, les données provenant des systèmes cybernétiques et physiques doivent être gérées de manière efficace pendant l'intégralité de leur cycle de vie en s'appuyant sur une gestion robuste des métadonnées.

Sécurité intégrée

S'assurer de l'intégration des différentes fonctions de sécurité et autres fonctions connexes, notamment les TI, la protection de la vie privée, les RH et les unités fonctionnelles, dans les ressources humaines, le processus et la technologie afin de garantir un flux continu d'informations

Protéger les actifs

Les entreprises doivent protéger leurs meilleurs actifs - les ressources humaines, les données et les biens - au moyen d'une architecture sécurisée, vigilante, robuste afin d'assurer la continuité des services et des opérations critiques

Le **Modèle de gestion de la gouvernance** propose des lignes directrices portant sur la mise en place d'une gouvernance collaborative basée sur l'appétence au risque et l'adoption d'une culture de convergence visant à transformer le domaine de la sécurité d'un centre de coûts en un centre de valeurs.

Culture

L'adoption d'une culture basée sur un environnement adaptatif dans lequel chaque individu a l'obligation de rendre compte et acquiert de l'autonomie à travers une formation et une sensibilisation appropriées

Gouvernance

La mise en place d'un modèle de gouvernance reposant sur une vision stratégique et des rôles et responsabilités bien définis permet à l'entité de gérer les risques liés à la convergence avec efficacité

Approche axée sur les risques

La priorisation de l'allocation des ressources et des actions en fonction du contexte de risque constitue le socle d'un programme de gestion efficace des risques d'entreprise

Cadre de protection de la vie privée dès la conception

Les 7 principes de protection de la vie privée dès la conception peuvent être intégrés dans la conception, le développement et le processus de déploiement des VCA afin de faire du respect de la vie privée une priorité dans la prise de décision relative à l'écosystème des VCA.

7 principes fondamentaux de la protection de la vie privée dès la conception

1	**Adopter une approche proactive et non réactive, préventive et non corrective**
2	**Définir la protection de la vie privée comme une priorité essentielle**
3	**Intégrer la protection de la vie privée dans la conception**
4	**Assurer une fonctionnalité intégrale, selon un paradigme à somme positive et non à somme nulle**
5	**Assurer la sécurité de bout en bout, notamment sur l'intégralité du cycle de vie**
6	**Assurer la visibilité et la transparence : maintenir l'accessibilité**
7	**Respecter la vie privée des utilisateurs : maintenir une approche centrée sur l'utilisateur**

Cadre harmonisé de contrôle de la confidentialité

Deloitte, en association avec le Privacy by Design Centre for Excellence de l'Université Ryerson, a mis en place un cadre de contrôle de la protection de la vie privée dès la conception qui repose sur les Principes généralement reconnus en matière de protection des renseignements personnels (PPRP) et qui englobe les obligations juridiques en matière de protection des renseignements personnels canadiens et internationaux (p. ex., la LPRPDE, le RGPD), les meilleures pratiques et normes sur la protection des renseignements personnels de l'industrie (Code type de la CSA, ISO/IEC 27001/2, ISO/IEC 27018, ENISA), et les lignes directrices réglementaires.

Opportunité de convergence de sécurité pour les sites de mise à l'essai des VCA

Capacités principales des centres d'essai de véhicules et inclusion potentielle des tests de cybersécurité dédiés aux VCA

1 | La durabilité de la structure

2 | Plusieurs analyses du cycle de vie
[Par exemple, la durée de vie d'un composant particulier du véhicule et les différents points de contrainte d'utilisation d'un composant]

3 | Les conditions climatiques

Dans la filière des véhicules connectés et autonomes, les risques cybernétiques s'ajoutent aux risques présents dans l'environnement physique. Renforcer les capacités existantes des centres d'essai des VCA en y ajoutant des exigences relatives à la cybersécurité peut déboucher sur la mise en place de centres destinés aux essais de sécurités de convergence - des installations qui peuvent être utilisées aux fins d'identification des vulnérabilités inhérentes aux aspects physiques et liés à la cybersécurité. Ci-après figurent quelques recommandations en matière d'activités liées aux tests de cybersécurité susceptibles d'être ajoutés aux composants des tests de sécurité physique réalisés dans les centres d'essai des VCA.

A | Logiciel
[En lien avec la « durabilité de la structure »]

La mémoire rémanente et le micrologiciel peuvent être extraits, analysés et modifiés. Des mécanismes de protection doivent être vérifiés afin de prévenir l'extraction.

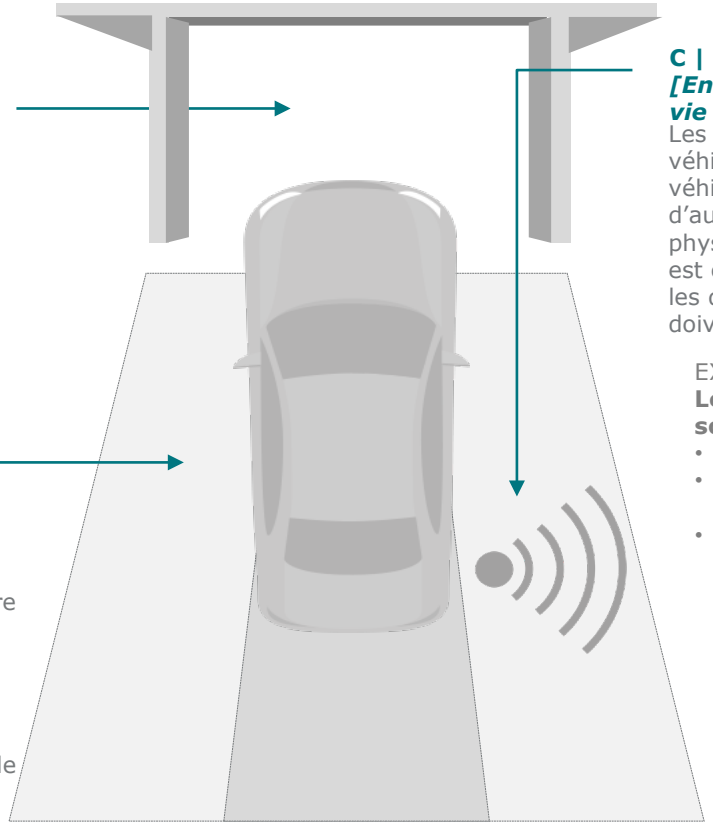
EXEMPLE | Mémoire embarquée

Le contenu de la mémoire rémanente peut généralement faire l'objet d'une extraction :

- Les contenus sont rarement chiffrés
- Peut stocker des justificatifs d'identité incorporés au programme
- Peut être modifiée (désactivation des fonctionnalités de sécurités)

B | Logiciel
[En lien avec « l'évaluation du cycle de vie »]

Le logiciel utilisé pour activer la fonctionnalité du VCA peut être vulnérable aux attaques et doit faire l'objet d'une évaluation face aux potentielles attaques cybernétiques - à distance, à proximité ou à l'intérieur de la voiture. Les fonctionnalités des VCA qui en facilitent l'usage (p.ex., le démarrage à distance) doivent être analysées du point de vue de leurs vulnérabilités susceptibles de favoriser des attaques cybernétiques telles que l'attaque de « l'homme du milieu ».



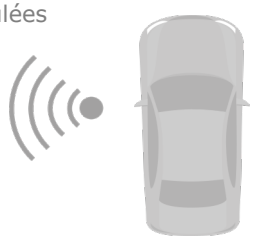
C | Communications du véhicule
[En lien avec « l'évaluation du cycle de vie »]

Les vulnérabilités des communications entre un véhicule et toute autre chose (p.ex. entre un véhicule et une infrastructure, une personne ou d'autres véhicules) doivent être évaluées. L'accès physique au bus de communication du véhicule est comparable à l'accès root à un serveur, donc les deux menaces physique et cybernétique doivent être prises en compte.

EXEMPLE | Mystification par message

Les messages non chiffrés et falsifiés sont légion :

- Peuvent faire l'objet d'attaques répétées
- Peuvent faire l'objet de mystification ou de modification
- Les données de détection critiques telles que la détection d'objet peuvent être manipulées



Principaux cas pratiques : Nouvelles initiatives relatives à la cybersécurité dans l'écosystème des VCA

Les jeunes entreprises priorisent généralement un vecteur de menace clé aux VCA et développent une ou plusieurs technologies à fort impact. Elles peuvent commercialiser des produits de manière indépendante ou en collaboration avec une autre entité (par exemple, le gouvernement, les fabricants et les opérateurs de télécommunications).

Collaboration avec le gouvernement

LORCA

ÉTUDE DE CAS 1
Plaque tournante de l'innovation [Royaume-Uni]

Programme d'innovation sur 12 mois du London Office For Rapid Cybersecurity Advancement (LORCA) :
LORCA est un centre d'innovation financé par le gouvernement qui accompagne les jeunes entreprises œuvrant à l'innovation. Ces jeunes pousses participent à un programme qui met à leur disposition du soutien pour leur permettre de développer des solutions aux défis liés à la cybersécurité dans l'industrie automobile et d'autres secteurs. Angoka participe au programme d'innovation de LORCA.[40]

Société de technologies de VCA axée sur la cybersécurité

ANGOKA

ÉTUDE DE CAS 2
ANGOKA [Royaume-Uni]

Technologie de cybersécurité conçue pour le VCA :
Angoka développe S-CAN, une solution matérielle pérenne destinée à la protection des communications réseau. Initialement dédiée au réseau de communication CAN, qui est couramment utilisé dans le secteur automobile dans les communications embarquées à bord du véhicule entre les modules MCE, la technologie peut également être intégrée à d'autres types de réseau tels que les systèmes de contrôle industriel et les différentes formes de communications entre machines (M2M).[41]

Collaboration avec une société de fabrication

ARGUS CYBER SECURITY

ÉTUDE DE CAS 3
Argus cyber security [Israël]

Approche « marché » avec un fabricant :
Le fabricant allemand Continental AG a fait l'acquisition d'Argus. Argus collabore avec Continental - l'entreprise a conjointement lancé une technologie de transmission des mises à jour logicielles de véhicule en direct avec Elektrobit, une filiale de Continental. Argus fera désormais partie d'Elektrobit et continuera de nouer des relations commerciales avec l'ensemble des fournisseurs automobiles du monde.[42]

Collaboration avec une société de télécommunications

dellfer

ÉTUDE DE CAS 4
Dellfer [États-Unis]

Approche « marché » avec un opérateur de télécommunications :
Partenariat avec DENSO (le deuxième prestataire de mobilité au monde) dans le cadre d'un accord de développement conjoint (ADC) visant à commercialiser la solution ZeroDayGuard 1.0. ZeroDayGuard est une solution de cybersécurité basée sur l'IdO de Dellfer qui défend les appareils connectés à IdO contre les attaques cybernétiques du jour zéro au moyen d'un mécanisme de protection intégré à code d'exécution. Cette solution est activée via une instruction prévue dans le développement du code du dispositif connecté à IdO, et peut par la suite instantanément détecter les actes de piraterie et les cyberattaques sous-jacents à distance dans le nuage. [43]

Principaux cas pratiques : Nouvelles initiatives relatives à la cybersécurité dans l'écosystème des VCA [Canada]

Les jeunes entreprises ontariennes mènent des activités de recherche et de développement des technologies. Certaines jeunes entreprises et des centres d'innovation développent des technologies dans l'écosystème des VCA.

Société de technologies de VCA axée sur la cybersécurité

ÉTUDE DE CAS 5
ISARA
[Kitchener Waterloo, Canada]

Technologie de cybersécurité conçue pour le VCA :
ISARA, forte de l'expertise de cryptographes, de chercheurs, de développeurs et de professionnels expérimentés de l'industrie de la sécurité, œuvre à la création de solutions de cybersécurité prêtes en vue de la production, qui sont dotées d'un chiffrement optimisé susceptible d'être intégré de façon homogène dans une infrastructure existante, afin de garantir la sécurité des données à l'ère post-quantique.

ISARA offre deux solutions
ISARA Radiate™ Quantum-safe Toolkit est la première solution intégrale de sécurité qui offre une mise en œuvre prête en vue de la production et conviviale des algorithmes à résistance quantique et des outils d'intégration conçus pour les développeurs.

Les technologies souples *ISARA Catalyst™ vous permettent d'introduire une fonction d'agilité cryptographique dans vos systèmes d'origine sous la forme d'un mécanisme sans risques et fiable pour garantir une sécurité à résistance quantique.*[44]

Sites régionaux de développement de technologies

ÉTUDE DE CAS 6
SRDT DU RIVA
[Ontario, Canada]

Sites d'innovation et de développement :

Le Réseau d'innovation pour les véhicules autonomes (AVIN) regroupe les acteurs de l'industrie, du monde universitaire et des gouvernements en vue d'exploiter les opportunités économiques qu'offrent les véhicules connectés et autonomes tout en soutenant les systèmes de transport de la province et les infrastructures par l'adaptation de ces nouvelles technologies.

Les Sites régionaux de développement de technologies favorisent la création de centres sites qui permettent aux petites et moyennes entreprises de l'Ontario de développer des prototypes, de valider les nouvelles technologies, d'avoir accès aux équipements spécialisés (matériels et logiciels) et de bénéficier des conseils commerciaux et techniques.

Chaque SRDT n'a qu'une seule spécialité; toutefois, tous les six SRDT considèrent la cybersécurité des VCA comme une partie intégrante de leur propre spécialité en raison de l'impact considérable et significatif de la cybersécurité dans l'ensemble du système des VCA et des technologies sous-jacentes.[45]

Élaboration des solutions de cybersécurité des VCA à l'échelle mondiale

Tribunaux compétents	Entité :	Description de l'innovation en matière de cybersécurité des VCA Phase de l'innovation en cybersécurité : Conception [C], Développement [D], et sur le marché [M]*	*Phase
Canada	**ISARA**	ISARA mise sur l'expertise de cryptographes, chercheurs, développeurs et de professionnels expérimentés de l'industrie de la sécurité qui œuvrent à la création de solutions de cybersécurité prêtes pour la production qui sont dotées d'un cryptage optimisé qui peut être parfaitement intégré aux infrastructures existantes afin de garantir la sécurité des données en cas d'attaque d'un ordinateur quantique.[44]	D
	Rogers Cybersecure Catalyst (Université Ryerson)	L'organisme Rogers Cybersecure Catalyst de l'Université Ryerson est un nouveau centre dédié à la collaboration et à l'innovation en cybersécurité. Cet organisme à pour but de renforcer la cybersécurité dans les organismes canadiens grâce à la formation, au renforcement des capacités, à la sensibilisation des petites entreprises aux menaces cybernétiques et aux solutions préconisées pour les contrer, aux programmes de certification, à la mise en place d'un accélérateur commercial et d'un centre de simulation des opérations de sécurité situé dans le centre-ville de Brampton.[46]	C, D
	Blackberry	Le Centre d'innovation pour les véhicules autonomes de Blackberry a été créé pour promouvoir les innovations technologiques dédiées aux VCA, de manière indépendante en collaboration avec les organismes du secteur privé et public et les instituts de recherche.[47] BlackBerry propose actuellement un certain nombre de solutions et services de sécurité pour véhicules connectés sur le marché, notamment : BlackBerry Certicom et les solutions logicielles BlackBerry QNX qui prennent en charge les VCA.[48]	C, D, M
	CloudGRC	CloudGRC Inc. est un leader en cybersécurité automobile qui fournit l'expertise et l'expérience nécessaires à la construction d'un programme efficace de cybersécurité axé sur les risques pour les entreprises impliquées dans la production et le fonctionnement des VCA. Cela suppose l'élaboration d'un programme de cybersécurité d'entreprise, d'une stratégie de cybersécurité, la préparation d'une évaluation des risques et menaces, des tests d'intrusion et d'une évaluation des vulnérabilités, d'un processus d'assurance continu de l'identité et de surveillance des véhicules. CloudGRC offre également des formations et des ateliers dans le domaine de la cybersécurité automobile.[49]	C, D, M
	ESCRYPT Canada	Transports Canada a récemment octroyé un contrat à hauteur de 1,3 million de dollars à ESCRYPT visant à promouvoir l'élaboration d'un système de gestion des certificats de sécurité canadien (SGCS) pour les véhicules connectés. Le SGCS permettra de garantir la sécurité et la fiabilité des communications des véhicules connectés. Le SCMS intègre les principes de respect de la vie privée dès la conception et permet de communiquer sans divulguer de renseignements personnels sur le véhicule ou son conducteur. Dans le cadre du contrat, ESCRYPT élaborera les exigences canadiennes pour le système et recommandera un modèle opérationnel sur la manière dont la technologie pourrait être déployée au Canada.[50]	C, D, M
Allemagne	**ESCRYPT**	Le logiciel CycurHSM est un microprogramme de sécurité dédié au module de sécurité matériel novateur et flexible qui garantit le démarrage sécurisé du module de contrôle électronique (MCE), une communication sécurisée dans le véhicule, une protection des composants du MCE et un clignotement sécuritaire.[50]	C, D, M
	EasyMile	Les véhicules sont équipés d'un module de type « boîte noire ». Ce module enregistre les données brutes provenant de divers capteurs échangées entre les composants matériels et logiciels du véhicule. En cas d'incident critique, toutes les données sont enregistrées avant et après l'incident afin de faciliter la compréhension et le diagnostic de l'accident. Les paramètres pris en compte comprennent : Les indicateurs de qualité (capteurs, emplacement, surveillance de l'itinéraire), la position, les tâches envoyées au véhicule par le système de supervision, les statistiques d'utilisation. Services EZFleet adaptés aux véhicules de transport : EZFleet est le cerveau électronique derrière une flotte de véhicules sans conducteur. Flexible et modulable, il permet aux organismes d'adapter leur flotte en fonction des différents besoins et scénarios de fonctionnement.[51]	D
	Bigchain DB	Permet aux développeurs et aux entreprises de déployer les validations de principe des chaînes de blocs, les plateformes et les applications grâce à une base de données de chaîne de blocs modulable. Plutôt que d'essayer de développer la technologie des chaînes de blocs, Bigchain DB commence par une base de données distribuée et ajoute ensuite les caractéristiques de chaînes de blocs - commande décentralisée, immutabilité et la capacité de créer et de transférer les actifs.[52]	C

Élaboration des solutions de cybersécurité des VCA à l'échelle mondiale

Tribunaux compétents	Entité :	Description de l'innovation en matière de cybersécurité des VCA Phase de l'innovation en cybersécurité : Conception [C], Développement [D], et sur le marché [M]*	*Phase
Israël, Tel-Aviv et Ramla	**SafeRide Technologies**	SafeRide Technologies a récemment élargi sa gamme de solutions de sécurité dotées de la technologie avancée d'intelligence artificielle, aux solutions de détection d'anomalies déterministes et heuristiques multicouches et à la prévention des menaces pour les véhicules connectés. vXRay, est l'une des solutions de profilage comportemental et de détection d'anomalies pour les centres d'opération de sécurité (COS) dans les véhicules connectés. Sans dépendances ou connaissances antérieures des protocoles comportementaux des véhicules, vXRay utilise l'apprentissage machine pour créer un profil de comportement individuel que le système utilise pour identifier des comportements anormaux et alerter le COS du véhicule.[53]	C, D, M
États-Unis	**Centri**	Installe des puces et applications mobiles pour protéger les capteurs automobiles et les données. Ne nécessite pas de connexion Internet, relie les dispositifs de confiance à la technologie de gestion de l'identité.[54]	D, M
	Arxan technologies	Brouillage au niveau binaire, chiffrement des données et alertes relatives aux menaces cybernétiques en temps réel.[55]	D, M
	NVIDIA	Les processeurs de données et puces alimentés par l'intelligence artificielle; les technologies logicielles basées sur le cloud permettent aux véhicules autonomes d'apprendre et de transmettre les données de conduite en toute sécurité. Les systèmes d'apprentissage en profondeur ont été utilisés par Tesla, Mercedes-Benz, Audi, Toyota et Volkswagen pour alimenter et protéger les véhicules autonomes.[56]	C, D
Japon	**Mitsubishi**	Technologies de détection des menaces. Chiffrement dans les environnements infonuagiques : Le « chiffrement à base d'attributs » restreint les droits d'accès aux cryptogrammes.[57]	D
	Trillium Inc.	Sécurise tous les trois principaux « domaines en proie à des menaces cybernétiques » dans le véhicule grâce à une approche basée sur le logiciel compatible avec tous les systèmes d'architecture ou d'exploitation. Concept d'externalisation de la sécurité informatique (SaaS) via des plateformes de mise à jour en temps réel que les constructeurs automobiles ou compagnies d'assurance vendront aux propriétaires de véhicule. Expertise en matière de réalisation d'essais, « SecureCAR »' et « SecureIoT »' et d'expansion de l'intégration à bord de véhicules et de la mise à l'essai des mises à niveau relatives à la cybersécurité sur des modèles actuels de véhicules connectés.[58]	D
Mexique	**Partenariat entre AT&T et KIA**	MyKIA + est une application mobile développée par KIA. À travers son service de localisation, Find My Kia, les conducteurs disposent d'un dispositif en option qui leur permet non seulement de tracer et de localiser le véhicule à tout moment, mais également de déterminer avec précision, de manière virtuelle, l'itinéraire parcouru. Les services seront offerts via la plateforme centrale de contrôle d'AT&T où les solutions connectées à l'IdO sont gérées. RESSER, la société de surveillance par satellite qui fournit le service de localisation de véhicules travaillera en collaboration avec le centre de contrôle afin de suivre de près l'emplacement des véhicules à tout moment, ce qui accélèrera le processus de recherche.[59]	D
	Jooycar	Obtenir des données sur les véhicules et les conducteurs en temps réel tout en utilisant les techniques d'intelligence artificielle afin d'offrir une assurance connectée et des services intelligents à valeurs ajoutées.[60]	D
Corée du Sud	**SOS LAB**	Société de technologie qui fabrique des capteurs LiDAR, solutions de télédétection pour véhicules autonomes.[61]	D
	Cube Intelligence IO [CUBE.IO]	L'utilisation de l'IA protège contre les attaques malveillantes en cas de piratage des véhicules autonomes et connectés à l'aide des codes de hachage qui forment le cœur de la technologie de chaîne de blocs et des chaînes de blocs. Cube bloque ces attaques à l'aide de ses propres synapses développées. Afin de promouvoir l'innovation au niveau local, Cube AI à participé au programme « Open Innovation » (innovation accessible) destiné aux jeunes entreprises de technologie/produits novateurs parrainé par Volkswagen Corée.[62]	C, D
Pays-Bas	**Quantoz**	Incubateur spécialisé dans les applications liées à la technologie novatrice des chaînes de blocs. Quasar, la solution de paiement numérique de Quantoz fournit les infrastructures de paiement instantané et de règlement de transaction entre les entreprises, les consommateurs et l'Internet des objets, conformément aux règlements, tout en respectant la confidentialité de l'utilisateur.[63]	C, M

À propos du Réseau d'innovation pour les véhicules autonomes

Le Réseau d'innovation pour les véhicules autonomes (RIVA) est une initiative du gouvernement de l'Ontario qui est administrée par les Centres d'excellence de l'Ontario. Le RIVA s'assure que l'Ontario demeure un leader dans le secteur de l'automobile et des transports en exploitant les opportunités économiques offertes par les véhicules connectés et autonomes et les solutions de mobilité, tout en aidant l'Ontario à occuper le premier rang dans la préparation, l'adoption et le déploiement de ces technologies.

À propos des Centres d'excellence de l'Ontario

Les Centres d'excellence de l'Ontario (CEO) Inc. stimulent la commercialisation des recherches de pointe dans les secteurs clés du marché en vue de bâtir l'économie de demain et de garantir la compétitivité mondiale de l'Ontario. À cet effet, les CEO encouragent la formation et le perfectionnement de la prochaine génération d'innovateurs et d'entrepreneurs et établissent des partenariats clés avec l'industrie, les universités, les collèges, les hôpitaux de recherche, les investisseurs et les gouvernements de l'Ontario.

À propos d'APMA

L'Association des fabricants de pièces d'automobile (APMA) du Canada est une association nationale représentant les fabricants de pièces, d'équipements, d'outils, de fournitures, de technologies de pointe et de services pour l'industrie automobile dans le monde entier. Créée en 1952, ses membres représentent 90 % de la production indépendante de pièces d'automobile au Canada. L'objectif principal de l'association est de promouvoir l'industrie de fabrication des équipements d'origine pour le secteur automobile, tant au niveau national qu'international. En plus de ses services de plaidoyer, l'APMA propose également à ses membres des solutions de développement commercial ainsi que des conseils et de l'assistance relativement à la modernisation de leurs activités afin de répondre aux besoins de l'industrie 4.0. et une intégration CAPE (Connecté, Automatisé, Partagé et Électrique)

À propos de Deloitte

Deloitte, l'un des cabinets de services professionnels les plus importants au Canada, offre des services dans les domaines de l'audit, de la fiscalité, du consulting et de la consultation financière. Deloitte LLP, une société à responsabilité limitée de l'Ontario, est le cabinet membre canadien de Deloitte Touche Tohmatsu Limited.

Deloitte fait référence à un ou plusieurs cabinets membres de Deloitte Touche Tohmatsu Limited, une société privée de droit anglais à responsabilité limitée par garantie, et à son réseau de cabinets membres constitués en entités indépendantes et juridiquement distinctes. Veuillez consulter le site www.deloitte.com/about pour une description détaillée de la structure juridique de Deloitte Touche Tohmatsu Limited et de ses cabinets membres.

À propos de cette publication