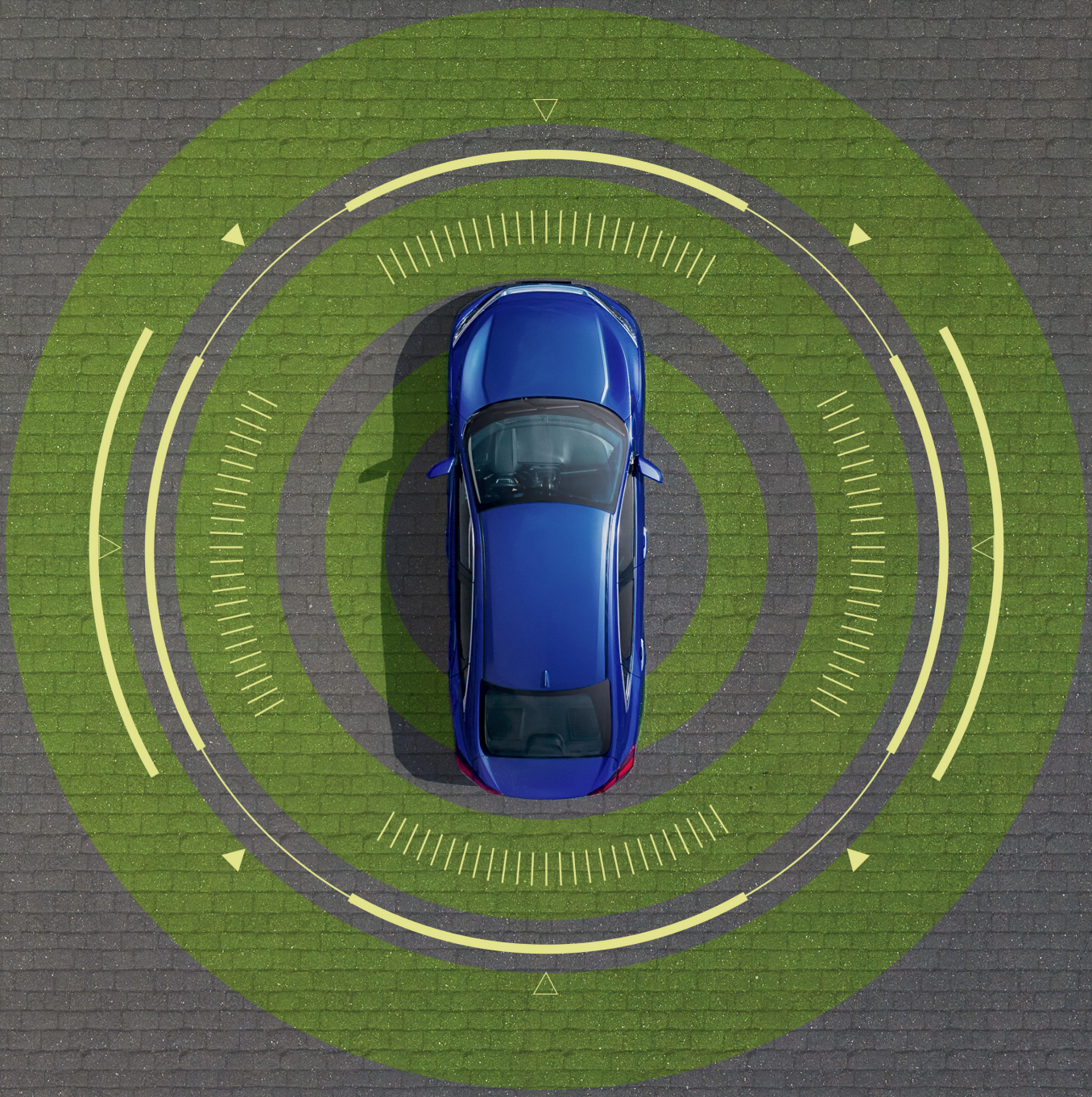
Deloitte.



Relier le Canada

Favoriser les véhicules de l’avenir

Table des matières

Introduction

Le transport terrestre connaît une révolution. Les véhicules hyperconnectés, l'électrification et des technologies de plus en plus autonomes mènent le pas.

Les véhicules connectés, autonomes, partagés et électriques (CAPE) ont déjà fait leur entrée sur le marché. On les retrouve partout dans le monde sous forme de taxis, de navettes et de parcs de véhicules de livraison sur de courtes et de longues distances dans une variété de secteurs, allant du commerce de détail au transport collectif[1]. En ce qui concerne l'intégration rapide des véhicules hyperconnectés et des mesures de sécurité stratégiques que les entreprises devront adopter, la question suivante se pose : que signifie cette nouvelle occasion qui s'offre aux entreprises?

Dans ce nouveau contexte des véhicules CAPE, la confiance est un nouvel obstacle pour les constructeurs, les fournisseurs, les organismes de réglementation, les propriétaires de parcs de véhicules et les gouvernements qui cherchent à assurer la sécurité et l'efficacité du transport terrestre connecté. Compte tenu des niveaux de complexité inédits, de l'intégration à l'architecture d'affaires actuelle, de la multiplication des surfaces d'attaque ainsi que du volume et de la valeur des données, les véhicules et l'infrastructure CAPE seront plus vulnérables aux cyberattaques. Et en raison des attentes élevées et du potentiel d'exploitation, toutes les entreprises au sein de la chaîne d'approvisionnement devront impérativement s'assurer que les technologies de cybersécurité automobile ont une grande longueur d'avance sur les auteurs de menaces. Sans prendre ces défis à la légère, il ne faut pas pour autant les laisser freiner l'accès à ce marché. Le désir de rivaliser, d'accroître l'efficacité opérationnelle et énergétique et de créer une nouvelle valeur pour les clients devrait offrir une motivation suffisante les défis. Aussi, les entreprises qui vont de l'avant avec les véhicules CAPE ont tout intérêt à adopter un point de vue stratégique et intégré, à comprendre les risques et à anticiper les difficultés à venir. En adoptant une vision stratégique et intégrée, et en comprenant les risques et les défis, les entreprises ne peuvent que bénéficier d'un engagement dans les véhicules CAPE.

Dans ce rapport, nous explorerons les caractéristiques de la technologie CAPE, en portant une attention particulière à la connectivité des données et à l'avenir des véhicules autonomes. Nous mettrons aussi en lumière les occasions qui s'offrent actuellement aux entreprises, et la façon dont ces dernières peuvent gérer la cybersécurité de façon globale pour maximiser l'engagement envers la technologie. Notre but est d'aider les entreprises à :

- comprendre les éléments moteurs de l'approche stratégique de cybersécurité et de gestion des risques au sein de l'écosystème des véhicules CAPE;
- déterminer comment la réglementation et les cadres de cybersécurité propres aux véhicules CAPE sont définis de manière à soutenir la croissance;
- examiner la façon dont l'élaboration et la mise en œuvre de la cybersécurité et de la gestion des risques liés aux véhicules CAPE constituent une responsabilité commune à toutes les parties au sein de l'écosystème;
- saisir l'importance d'une cyberstratégie inclusive pour l'ensemble du cycle de vie des parcs de véhicules CAPE.

Propulser l'avenir de la mobilité

Les dispositifs interconnectés, l'intelligence artificielle (IA), l'informatique de périphérie et l'analytique de données transforment la chaîne de valeur automobile d'un bout à l'autre (Figure 1)[2]. Il ne fait aucun doute que les entreprises qui ont investi dans ces technologies ont profité de nombreuses retombées positives. Cela dit, pour accéder à ces avantages accrus, les entreprises doivent relever les défis qui les attendent sur le plan de la cybersécurité et de la gestion des risques. Au fil de son parcours vers la connectivité et l'automatisation totales, le secteur des transports doit prendre en compte ces nouveaux défis. Les principes de cybersécurité doivent faire partie des fondements de l'intégration, de l'exploitation et de la gestion du cycle de vie des véhicules CAPE afin de prévenir les perturbations dans les activités d'affaires, le rendement et les processus, tout en assurant la cybersécurité et la sécurité physique des gens et des produits.

Figure 1. Éléments clés et avantages de l'intégration de la mobilité axée sur la cybersécurité

Vie et sécurité

Selon les estimations de l'Organisation mondiale de la santé, les accidents de la route entraînent **1,3 million de décès chaque année, une baisse de 3 % du PIB des pays et de 20 à 50 millions de blessés**[3], ce qui place la sécurité et l'expérience des utilisateurs au cœur des objectifs des leaders sectoriels. Les solutions logicielles, telles que l'aide au changement de voie, la correction de l'angle du volant et la vérification d'angles morts **confient la prise de décisions au véhicule, qui réagit plus rapidement et avec plus de précision qu'un être humain**.

Efficacité du transport

Alors que 68 % de la population mondiale devrait vivre en région urbaine d'ici 2050[4], l'analytique pour la planification efficace des trajets et la réduction de la congestion routière assurera une efficacité incontestée des déplacements **au premier kilomètre, au kilomètre intermédiaire et au dernier kilomètre**. La circulation en peloton se traduira par **le partage d'information, une meilleure connaissance de l'état des routes, une réduction de la consommation de carburant et des stratégies de coopération.**

Pénurie de main-d'œuvre

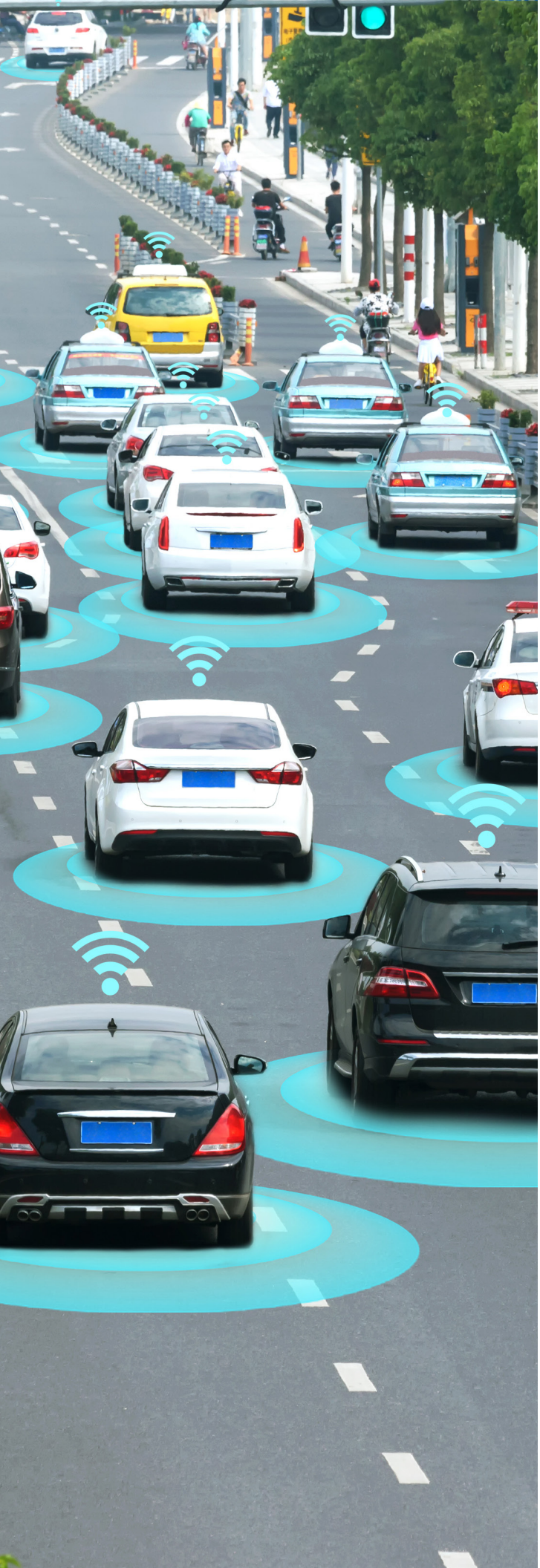
La pénurie de 20 000 travailleurs enregistrée en **février 2020** dans l'industrie canadienne du camionnage, qui **devrait atteindre 50 000 travailleurs d'ici 2024**, pourrait être réglée grâce à des camions **VCA** (véhicules connectés et autonomes) qui, en théorie, peuvent **fonctionner 24 heures sur 24, 7 jours sur 7**[5], Les entreprises de camionnage, d'entreposage ferroviaire et de logistique peuvent **gérer la demande en période de pointe avec plus de souplesse, prendre en charge des cargaisons plus lourdes et emballer des produits individuellement** en déployant des VCA (comme des parcs de véhicules automatisés, entre autres technologies CAPE) pour tirer parti de bassins de profits élargis.

Durabilité environnementale

Les solutions de transport plus vertes connaissent un essor, alors que le **gouvernement canadien exige que tous les véhicules vendus soient des véhicules zéro émission d'ici 2035**[6]. Cette tendance favorise **d'autres formes de mobilité qui réduisent les émissions de carbone et les embouteillages en rendant le transport collectif plus accessible, pratique et abordable**. Grâce à l'adoption croissante de la mobilité partagée, des milieux urbains **(par exemple, des stationnements) pourront être réutilisés sous forme d'espaces verts et de parcs**.

Perspectives fondées sur les données

Avec les niveaux record de ventes en ligne, la demande des consommateurs a amené les entreprises à trouver des solutions novatrices pour répondre **aux exigences croissantes des clients et à la panoplie de besoins**. L'utilisation des **grandes quantités de données générées par les VCA permet une meilleure visibilité de la chaîne d'approvisionnement, le recours à l'analytique prédictive et la personnalisation des services en fonction de chaque consommateur**. Grâce aux perspectives fondées sur les données, les organisations sont en mesure d'acheminer des biens plus rapidement aux clients.



Comprendre les cyberrisques liés au nouvel écosystème

L'intégration de l'Internet des objets (IdO) complexe, de la connectivité et de composantes logicielles (5G, Wi-Fi, caméras, capteurs LIDAR, etc.) aux véhicules CAPE modifie leurs surfaces d'attaque, ce qui crée l'un des risques les plus importants : ces composantes n'ont pas besoin d'être à proximité physique, comme les véhicules autres que CAPE, pour être la cible d'une attaque. L'exploitation de ces surfaces d'attaque élargies s'intensifie d'année en année – notamment une hausse de la mystification, l'écoute électronique et les cyberattaques – sont de plus en plus fréquentes (figures 2 and 3).

Hausse exponentielle des cyberrisques

La tendance à la hausse du nombre de cyberincidents au cours de la dernière décennie devrait se poursuivre[7]. L'an dernier, un leader sectoriel du marché des véhicules CAPE a pris conscience de la criticité et du danger associés à ces attaques lorsque 25 de ses véhicules ont été visés par un accès à distance[8]. Le pirate, un adolescent, a pu déterminer l'emplacement exact de chacun des véhicules, savoir si un chauffeur y prenait place et, surtout, exécuter des commandes à distance. Dans un autre incident qui s'est produit en 2021, les renseignements de cartes de crédit, les cotes de crédit autodéclarées et les numéros de permis de conduire des clients de la division nord-américaine d'un fabricant européen d'équipements d'origine (FEO) de luxe ont été exposés lors d'une fuite de données[9]. Puisque l'atteinte était attribuable au stockage d'un tiers qui avait été configuré incorrectement, la responsabilité réglementaire incombait au fournisseur, mais les coûts liés à la réputation ont été assumés par le fabricant.

Le regroupement de composantes matérielles et logicielles dans un véhicule CAPE mène à une répartition complexe des responsabilités advenant ce genre d'attaque ou d'atteinte. Dans bien des cas, la responsabilité peut incomber à une ou plusieurs des parties prenantes de la chaîne d'approvisionnement automobile.

Chaque partie prenante peut contribuer à la fortification contre l'évolution rapide de la tolérance aux risques, qu'il s'agisse d'organismes de réglementation ou de fournisseurs de premier, deuxième et troisième niveau (y compris les entreprises de fourniture de logiciels), de constructeurs automobiles, de fournisseurs de services de communication (FSC), d'entreprises d'infonuagique ou d'entreprises consommatrices de services de transport intelligent (figure 2). Les partenariats, la délégation de responsabilités et la détermination des occasions d'atténuer les cyberrisques seront des éléments clés pour que l'ensemble de l'écosystème puisse être utilisé de façon sécuritaire et en toute confiance.

Figure 2. Niveau de risques et attaques pour les véhicules connectés et automatisés

Niveau de risque	Menaces et attaques
Faible	• Manipulation des données de diagnostic des véhicules • Mise au point illégale des véhicules • Accès non autorisé aux systèmes administratifs (usines de fabrication, systèmes infonuagiques, etc.)
Moyen	• Logiciels malveillants ciblés • Exploitation des comptes d'utilisateurs • Mystification de touches
Élevé	• Surveillance et localisation par GPS • Manipulation des comportements des chauffeurs au moyen de tactiques trompeuses • Contrôle à distance de véhicules ou exécution à distance de codes dans le véhicule • Contrôle de l'accélération et du freinage

Source : Upstream Security Limited

« Le secteur de l'automobile et de la mobilité se transforme rapidement en raison de la technologie des véhicules électriques, connectés et autonomes. Par conséquent, la cybersécurité est devenue un élément fondamental des déplacements des gens et des biens dans le futur. »

—Raed Kadri, chef du Réseau Ontarien d'innovation pour les véhicules (ROIV)

Figure 3. Parties prenantes de la chaîne d'approvisionnement automobile et leurs responsabilités à l'égard de la protection des VCA

ORGANISMES DE RÉGLEMENTATION	FOURNISSEURS DE 1ER, 2E ET 3E NIVEAUX ET FEO	ENTREPRISES D'INFRASTRUCTURE INFONUAGIQUE	FOURNISSEURS DE SERVICES DE COMMUNICATION	ENTREPRISES CONSOMMATRICES VCA
Gouvernements fédéral, provinciaux et municipaux	Fournisseurs d'applications logicielles de VCA, de systèmes d'aide à la conduite, de systèmes d'exploitation et de modules électroniques; les usines d'assemblage, etc.	Fournisseurs d'infrastructure de données GPS, aspect administratif des applications de VCA et catalyseurs de communications	Entreprises de télécommunications, fourniture de services 5G, 4G, LTE, etc.	Exploitants de parcs de véhicules, fournisseurs de solutions au premier kilomètre, au kilomètre intermédiaire et au dernier kilomètre, logistique, etc.
• Habilitation sécurisée des technologies de transport • Respecter le modèle de responsabilité partagée (normes de publication, pratiques exemplaires et prévision des difficultés) • Assurer l'attestation de conformité • Favoriser la relation entre les gouvernements et l'industrie en peaufinant la législation, et en soutenant le développement économique et l'innovation grâce aux VCA tout en encourageant la sécurité globale	• Intégrer des normes internationales en matière de cybersécurité au matériel et au logiciel • Assurer la sécurité intégrale de tous les éléments automobiles regroupés • Respecter les lois transfrontalières (protection et confidentialité des données) • Chiffrement des dispositifs connectés (clés télécommandées, applications mobiles, etc.) • Sécuriser les codes des unités embarquées	• Responsabilité du renforcement du nuage, de la gestion des vulnérabilités et du contrôle de l'accès aux données stockées • Chiffrement des données en mouvement et des données au repos • Responsabilité à l'égard de la mauvaise utilisation, les vulnérabilités découlant de la manipulation de données ou de divulgation de codes, et accès illicite par des voies détournées • Souveraineté des données automobiles en stockage transfrontalier	• Disponibilité de réseaux de communication • Canaux de communication sécurisés pour différents services (par exemple, les communications urgentes ou non urgentes, etc.) • Connectivité dans les régions non urbaines, comme les autoroutes et la fourniture de services à l'échelle de la province ou du pays • Canaux de communication fiables	• Menaces internes • Sécuriser les intégrations entre les infrastructures sur place et en nuage • Surveiller les véhicules en tant qu'actifs (au moyen d'opérations de sécurité et de la gestion d'événements et d'incidents de sécurité) • Protéger les données et les actifs exclusifs au moyen d'ententes de niveau de service appropriées • Assurance et évaluation des risques des logiciels de tiers

Établir la protection dès la conception

En intégrant la sécurité à la conception des systèmes et des processus, les organisations peuvent augmenter la cyberrésilience à mesure qu'elles s'adaptent aux nouvelles façons d'exercer leurs activités. Cela nécessitera l'adoption de principes de développement d'actifs axés sur la sécurité – et la protection des données – dès la conception, ainsi que des solutions telles qu'une approche confiance zéro multicouches à l'égard des cyberdéfenses. Le modèle confiance zéro constituera une importante mesure de protection dans ce secteur, comme en témoigne le sondage de Deloitte sur l'avenir de la cybersécurité 2021[10].

Sécuriser l'écosystème des véhicules CAPE : une feuille de route vers la réglementation

La transition vers la mobilité entièrement intégrée sera complexe et ardue. La sécurité des véhicules CAPE repose d'abord et avant tout sur le véhicule en soi et les composantes matérielles et logicielles connexes. Les FEO et les fournisseurs de premier, deuxième et troisième niveau du secteur de l'automobile peuvent suivre les meilleures pratiques pour assurer la conformité à la réglementation, comme les normes de chiffrement matériel et les protocoles de communication pour les modules de commande électronique, auxquels s'ajoutent des évaluations des risques récurrents et des contrôles. En Europe, le Forum mondial de l'harmonisation des Règlements concernant les véhicules (WP.29) a commencé à élaborer un cadre pour harmoniser la réglementation à l'échelle mondiale[11]. Transports Canada a emboîté le pas en créant ses propres lignes directrices de cybersécurité et d'initiatives de conformité, qui auront une incidence sur les processus opérationnels[1]. L'un des principaux problèmes est que les cadres réglementaires élaborés dans chaque juridiction peuvent ne pas s'aligner les uns sur les autres, laissant les FEO courir après la conformité face à une complexité croissante. Par ailleurs, la norme R155 des Nations Unies deviendra bientôt obligatoire dans plusieurs pays, nécessitant que les constructeurs automobiles intègrent des systèmes de gestion de la cybersécurité des véhicules pour assurer une protection contre une liste précise de cybermenaces[12]. Pour une couverture complète, les FEO devront obtenir une attestation de conformité à la réglementation de la part des fournisseurs de premier et deuxième niveau, ainsi que des fournisseurs de logiciels.

Les sociétés de logiciels et les fournisseurs de premier niveau qui accompagnent leurs logiciels de matériel devraient intégrer des pratiques exemplaires et des méthodologies de tests de sécurité à leurs processus de développement. Les composantes matérielles comme les puces, les modules de commande électronique et les unités embarquées doivent être protégées dès la conception contre les modifications illicites après leur entrée sur le marché; il sera possible d'utiliser une validation à l'aide d'un microprogramme pour repérer les signes d'altération ou les modifications après l'entrée sur le marché. Étant donné l'étalement du produit final, les entreprises devraient aussi envisager de sécuriser les activités infonuagiques afin de déployer en toute confiance les mises à jour logicielles pour des composantes telles que les systèmes d'aide à la conduite. Les correctifs et les mises à jour des logiciels de véhicule seront installés à distance par l'intermédiaire d'Internet ou par la voie des ondes, de sorte que le chiffrement sera nécessaire pour assurer la confidentialité, l'intégrité et la disponibilité du logiciel fourni.

Outre la conformité des éléments individuels, la mise en place de contrôles adéquats pour l'ensemble du cycle de vie de production du véhicule permettra d'assurer la conformité intégrale aux normes de cybersécurité pour la totalité du véhicule CAPE. Cela est rendu possible grâce à des normes telles qu'ISO/SAE 21 434 (Véhicules routiers — Ingénierie de la cybersécurité) et ISO/DIS 24 089 (Véhicules routiers – Ingénierie de mise à jour du logiciel)[13,14]. La norme ISO/SAE 21 434, qui s'ajoute à la norme ISO/SAE 26262 (Véhicules routiers – Sécurité fonctionnelle), porte sur des aspects tels que la gestion de la sécurité, l'intégration des activités de cybersécurité en continu, les méthodes d'évaluation des risques et les facteurs liés à la cybersécurité dans le développement de produits.

La SAE fournit également des guides, des pratiques exemplaires et des leçons en matière de cybersécurité provenant des milieux sectoriels, gouvernementaux et universitaires concernant la sécurité des véhicules[15]. C'est là que les organismes de réglementation devraient se tourner pour prescrire la conformité et l'attestation réglementaires. Lorsque des exigences et des obligations régionales fondées sur des pratiques exemplaires et des politiques sont définies, la division des responsabilités entre les parties prenantes de l'ensemble de la chaîne d'approvisionnement automobile peut être clairement établie, tout comme le devoir de respecter de saines pratiques de cyberhygiène dans les procédés de fabrication d'automobiles.

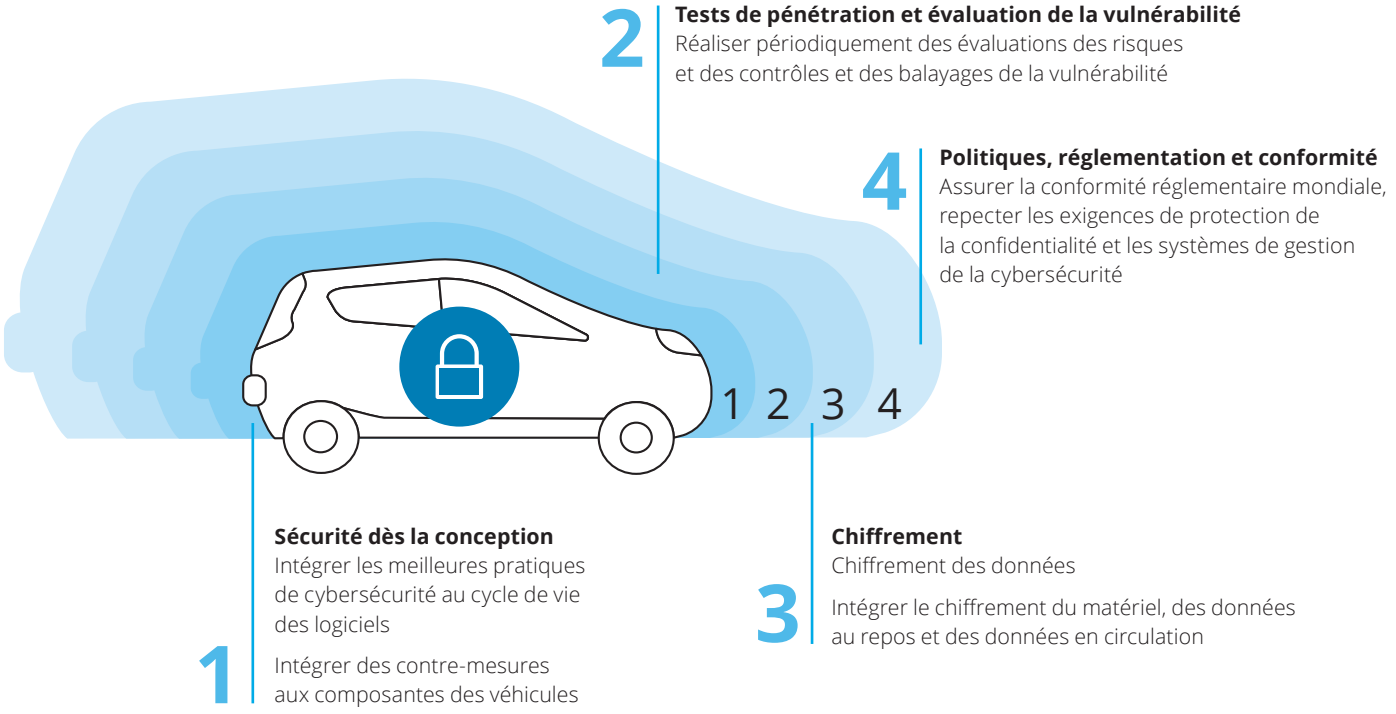
Chaque partie prenante a un rôle essentiel à jouer pour sécuriser la chaîne de valeur automobile; aussi, la collaboration entre les parties prenantes donnera lieu au renforcement des capacités de cybersécurité. Un modèle de responsabilité partagée permettra d'établir une véritable sécurité dès la conception aux fins de l'adoption des véhicules CAPE.

Figure 4. Grille de responsabilité partagée et responsabilité de chaque partie prenante dans le cycle de vie de production automobile.

	Fournisseurs de 1er, 2e et 3e niveaux et FEO	Gouvernement et organismes de réglementation	Infrastructure infonuagique	Fournisseurs de services de communication (4G/5G)	Exploitants de parcs automobiles VCA d'entreprise
Gestion de microprogrammes par la voie des ondes de façon sécurisée					
Centres des opérations de cybersécurité					
Confidentialité des données					
Sécurité des infrastructures de communication					
Sécurité des communications V2X (de véhicule à X)					
Sécurité des applications mobiles					
Sécurité des interfaces (Wi-Fi, Bluetooth, 5G)					
Sécurité des systèmes d'aide à la conduite					
Sécurité des systèmes embarqués					

Moins de responsabilité — **Plus de responsabilité**

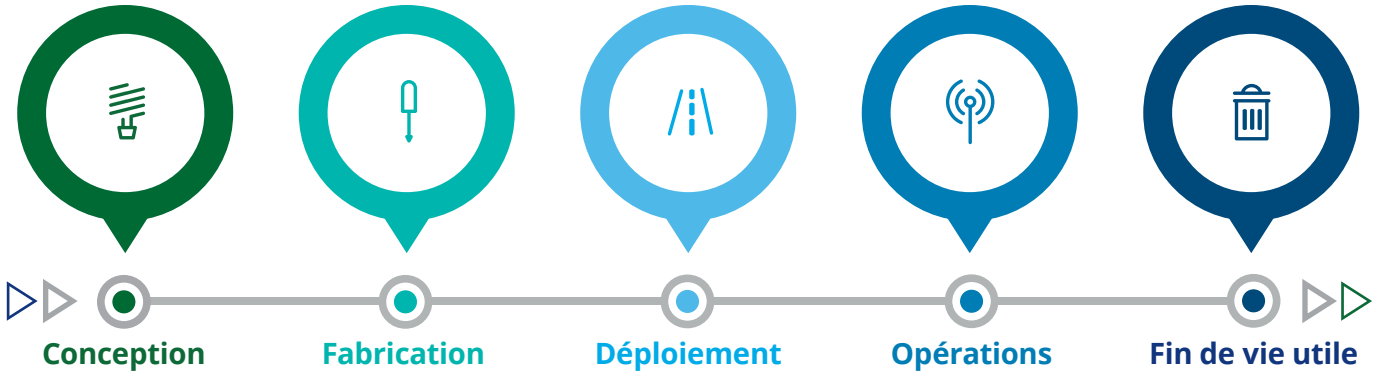
Figure 5. La défense en profondeur nécessite l'intégration de la cybersécurité à chaque niveau des opérations pour assurer la protection et la cybersécurité des VCA et des utilisateurs à l'intérieur comme à l'extérieur.



Passer à la vitesse supérieure

Les parties prenantes peuvent participer efficacement à un modèle de responsabilité partagée en intégrant à leurs activités différentes capacités de cybersécurité. De la protection des infrastructures aux évaluations de la vulnérabilité, en passant par les considérations relatives à la protection des renseignements personnels et la surveillance continue de la sécurité, ces capacités permettront aux organisations de transport d'entreprendre en toute confiance la transformation numérique qui s'impose. Pour celles qui adoptent les technologies CAPE, nous avons réparti les considérations relatives au cycle de vie des véhicules CAPE en cinq étapes : conception, fabrication, déploiement, opérations et fin de vie utile (Figure 6).

Figure 6. Considérations relatives à la cybersécurité pour le cycle de vie des VCA



	Conception	Fabrication	Déploiement	Opérations	Fin de vie utile
Parties prenantes	• FEO • Fournisseurs de 1er, 2e et 3e niveaux • Organismes de réglementation et législatifs	• FEO, fournisseurs de 1er, 2e et 3e niveaux • Fabrication de drones • Modernisation de VCA et installateurs • Entreprises de développement de logiciels pour VCA	• Entreprises consommatrices de VCA, logistique et solutions au premier kilomètre, au kilomètre intermédiaire et au dernier kilomètre • Tests de sécurité des applications; entreprises de télécommunications	• Entreprises consommatrices de VCA, logistique et solutions au premier kilomètre, au kilomètre intermédiaire et au dernier kilomètre • Entreprises de solutions logicielles après l'entrée sur le marché	• Entreprises consommatrices de VCA • Logistique • Solutions au premier kilomètre, au kilomètre intermédiaire et au dernier kilomètre
Capacités de cybersécurité	• Politiques de protection des données et des renseignements personnels • Certification de la conformité pour les données, les tests et l'intégration des VCA • Évaluations de la maturité et de l'état de préparation à l'intégration des VCA • Structures de gouvernance, rôles et responsabilités liés à la gestion des cyberrisques • Formation et sensibilisation en cybersécurité des VCA	• Évaluation des risques et des contrôles liés aux tiers • Présentation et suivi des vulnérabilités • Intégration sécurisée au cycle de vie des logiciels • Gestion des identités et de l'accès • Protection des terminaux des VCA • Considérations relatives à la sécurité des infrastructures sur place et en nuage	• Configuration du système de détection et de prévention des intrusions a bord des véhicules • Application des correctifs et mises à jour par la voie des ondes de façon sécuritaire • Examen des contrats de cybersécurité et des ententes de niveau de service • Renseignements sur les cybermenaces et analyse des cybermenaces • Tests d'applications (tests statiques et dynamiques de sécurité des applications)	• Production de de tableaux de bord et de rapports sur les cyberrisques • Intervention en cas d'incidents et gestion des incidents • Exercices sur table et simulations • Développement, sécurité et opérations (DevSecOps) • Analyse et rapport criminalistique après un incident impliquant un VCA • Croissance stratégique pour l'adoption de technologies émergentes (5G, informatique de périphérie, chaîne de blocs, etc.)	• Mise hors service sécurisée du logiciel et du matériel • Conservation des données (à l'interne et par des tiers) • Conformité à la réglementation et aux politiques liées à la fin du cycle de vie • Cyberrisques associés à la revente des VCA • Considérations relatives à l'infrastructure et à l'infonuagique pour la fin de vie utile • Profilage des dispositif et fin de contrats

Conception

Tout au long de ces étapes, les différents acteurs peuvent favoriser la réussite des activités en intégrant des pratiques de cybersécurité qui assurent la sécurité, la fiabilité et la confidentialité pour l'ensemble des gens, des processus et des technologies.

Les organismes de réglementation devraient donner l'exemple en élaborant des cadres et des règlements visant à orienter les parties prenantes tout au long du cycle de production. Il pourrait s'agir notamment de meilleures pratiques pour l'évaluation de la maturité et des risques, et de normes pour la mise à l'essai des véhicules CAPE sécuritaires et leur déploiement sur les routes publiques. Il importe qu'ils définissent les responsabilités à l'échelle de la chaîne de production automobile, appuyée par des méthodes d'attestation. Il convient aussi de mettre en place des intégrations aux infrastructures publiques et des lignes directrices sur la confidentialité des données ainsi que des exigences relatives aux essais des véhicules CAPE pour veiller à ce que la cybersécurité au sein du secteur des transports stimule la croissance économique tout en protégeant les citoyens.

Les fournisseurs de premier, deuxième et troisième niveaux et les FEO peuvent ensuite utiliser ces normes pour guider la conception des véhicules CAPE à cybersécurité intégrée. La gestion des cyberrisques doit être calibrée en fonction des structures de gouvernance existantes, et les rôles et responsabilités doivent être clairement énoncés. À partir de là, les lignes directrices prédéfinies et les exigences réglementaires peuvent tracer la voie vers l'assurance de la conformité. Cela peut comprendre des facteurs liés à la sécurité pour la numérisation et l'acquisition de processus de base, des évaluations de la maturité pour la production de véhicules CAPE, l'établissement d'une stratégie pour la mise à l'essai des véhicules CAPE après la production, et le stockage et l'utilisation des données sur les véhicules CAPE. À cette étape, les parties prenantes peuvent bénéficier de l'harmonisation entre leur stratégie de cybersécurité et les objectifs organisationnels. Par exemple, un fournisseur de solutions au dernier kilomètre peut déterminer ses objectifs de développement durable et d'amélioration de la satisfaction de la clientèle au cours des dix prochaines années, puis tirer parti des technologies CAPE pour les atteindre en mettant en œuvre des camions qui optimisent les trajets et qui acheminent plus rapidement les produits à destination en générant moins d'émissions.

Fabrication

Lorsque le véhicule CAPE passe de la phase de conception à celle de la fabrication, des capacités de cybersécurité qui tiennent compte du regroupement des composantes des divers systèmes intégrés (systèmes d'aide à la conduite, infodivertissement, systèmes d'exploitation en temps réel, etc.) seront cruciales. Pour les FEO, cela signifie qu'il faudra réaliser des évaluations des menaces et des risques et cerner les risques associés aux partenariats avec des entreprises de fourniture de logiciels et des fournisseurs de premier, deuxième et troisième niveaux.

Premièrement, les principaux contrôles de sécurité devraient être intégrés aux activités de chaque partie prenante, de la fabrication aux processus de la chaîne d'approvisionnement, et tout ce qui se trouve entre les deux. Si la sécurité des véhicules CAPE est mal configurée, cela peut facilement créer des points d'entrée tout au long du processus.

À toutes les étapes, les fournisseurs de logiciels, les fabricants de composantes, les fournisseurs de services infonuagiques et les fournisseurs de services de communication devraient effectuer simultanément leurs propres évaluations des menaces et des risques. Les fabricants doivent établir clairement les normes qui s'appliquent à la chaîne d'approvisionnement et déterminer les exigences de sécurité dès la conception. De cette manière leurs produits peuvent obtenir l'attestation de conformité avant d'être intégrés au véhicule. Le renforcement du logiciel, du matériel et des composantes, et le chiffrement, le stockage et la gestion des données sont tous des éléments clés à considérer pour chacun des systèmes intégrés.

Le fait de tenir compte de ces éléments à l'étape du cycle de fabrication du véhicule CAPE peut protéger les parties prenantes contre de nombreuses vulnérabilités, alors qu'elles créent des produits auxquels les consommateurs peuvent faire confiance.

Déploiement

Une fois fabriqués, les véhicules CAPE devront être mis à l'essai avant d'être déployés à grande échelle. Compte tenu des diverses exigences imposées par les organismes de réglementation concernant l'essai des véhicules CAPE, assurer la conformité devrait être une priorité absolue. Parmi les considérations importantes, citons le renforcement de la sécurité au moyen de tests de pénétration des véhicules CAPE, la délimitation de l'étendue fondée sur les risques au moyen de vecteurs de menaces, et la mise à l'essai des fonctions et des composantes de la plateforme globale. Les FEO devraient aussi collaborer étroitement avec les FSC pour définir les plages de connectivité et les exigences de communication, et de protéger la visibilité des véhicules CAPE sur le terrain.

Pour les entreprises consommatrices de véhicules CAPE, ces technologies devraient faire l'objet d'un projet pilote à des fins d'évaluation des vulnérabilités et des risques imprévus, le cas échéant, avant leur intégration complète à l'écosystème. Un lancement réussi exige aussi une approche fondée sur la sécurité dès la conception, y compris la protection de la sécurité et des opérations de l'infrastructure de base, notamment la microsegmentation des réseaux pour restreindre les mouvements latéraux. Les organisations doivent assurer la visibilité sur l'ensemble de l'infrastructure, à laquelle s'ajoutent des contrôles de sécurité afin de gérer les zones de menace actuelles. Cela comprend l'intégration de capacités d'identification selon le principe du moindre privilège et confiance zéro pour déléguer l'accès associé aux véhicules CAPE (à des fins de protection des terminaux). Grâce à l'analyse des identités, les organisations peuvent favoriser une gestion rapide des changements et assurer aisément un accès sécurisé.

Les entreprises consommatrices et les propriétaires de parcs de véhicules devraient collaborer avec les tiers fournisseurs de services d'infonuagique et de communication appropriés afin de comprendre où et comment les véhicules CAPE seront utilisés et définir les risques qui peuvent en découler. Ces considérations favoriseront l'intégration sécuritaire à plus petite échelle de même qu'à grande échelle, selon les exigences, de manière à soutenir les capacités de l'organisation.

Opérations

L'une des principales considérations à l'étape opérationnelle est de favoriser la confiance dans les véhicules CAPE grâce à la visibilité et à la supervision. À mesure que les technologies évoluent vers la communication V2V (véhicule à véhicule), la sécurité dès la conception doit être renforcée par la sécurité dès l'intégration. Les organisations doivent explorer les exigences uniques liées à l'application des correctifs et des mises à jour sur les véhicules CAPE, et rester à l'affût des risques critiques pour la sécurité, comme les vulnérabilités du jour zéro. Cela comprend la remise en état rapide à l'aide des correctifs disponibles et la mise en œuvre de processus de confiance pour vérifier et installer les mises à jour logicielles par la voie des ondes. Dans le cas des mises à jour de la technologie des véhicules CAPE, les organisations devront établir des partenariats avec des tiers fournisseurs. Ici, l'infrastructure infonuagique et les FSC jouent un rôle de premier plan dans la prestation de services sécurisés.

Ce n'est pas une question de « si », mais plutôt de « quand » un incident de sécurité frappera; aussi, il convient de prendre des mesures pour planifier en prévision de l'inévitable. Il sera essentiel d'élaborer des plans d'intervention en cas d'incident, qui peuvent être renforcés par des exercices sur table et des simulations pour assurer la préparation et mettre les canaux de communication à l'essai. Les plans de continuité des activités doivent être mis à jour pour assurer la réactivité des véhicules CAPE et un retour à la normale le plus rapidement possible.

Au fil des nouveaux développements en technologie 5G, IA, informatique quantique, réseaux définis par les logiciels et chaîne de blocs, ceux-ci auront des conséquences sur la cybersécurité et les véhicules CAPE. Les fabricants, consommateurs et organismes de réglementation devraient effectuer des évaluations des risques pour déterminer les nouvelles possibilités d'exécuter les activités en toute sécurité. Les acteurs qui constituent les piliers des communications (comme les FSC et les fournisseurs d'infrastructure infonuagique) devraient constamment peaufiner et intégrer les meilleures pratiques et une stratégie bien expliquée. Les organisations qui font preuve de souplesse et mettent leurs capacités à jour multiplieront les avantages tirés des véhicules CAPE et gagneront la confiance du public envers leurs services.

Fin de vie utile

Dans le cas des technologies CAPE en fin de vie utile, certaines des considérations liées à la cybersécurité sont uniques. Lorsqu'un véhicule CAPE a atteint la fin de sa durée de vie opérationnelle, on ne peut pas tout simplement s'en départir ou le vendre. Ses composantes de connexion (matérielles et logicielles) devront être mises hors service pour assurer la protection des données et des actifs organisationnels.

Une mise hors service fructueuse nécessite aussi la prise en compte de l'infrastructure et des environnements infonuagiques. L'accès du véhicule aux emplacements physiques et numériques de l'organisation doit être révoqué. Il faut évaluer les données recueillies par le véhicule CAPE de manière à répondre aux exigences de conservation. Les données stockées, le cas échéant, doivent être traitées conformément aux lois et règlements en protection des renseignements personnels de la région où le véhicule CAPE a été utilisé, et les organisations doivent assurer le respect de leurs échéanciers. Ces mesures visent également la conservation des données de tiers.

Enfin, les organisations qui souhaitent revendre un véhicule CAPE doivent effectuer le profilage des dispositifs qui présentent un risque de surface d'attaque. De cette façon, il n'y a aucune possibilité d'accès accidentel aux données ou aux actifs organisationnels. La fin de vie utile d'un véhicule CAPE doit être prise en compte par tous les membres du cycle de vie de production, y compris les concessionnaires, les propriétaires temporaires et les fabricants. À cette étape-ci, une bonne hygiène numérique aura une valeur inestimable pour l'utilisation sécuritaire des véhicules CAPE.

Dernières réflexions

Partout dans le monde, les entreprises seront touchées par l'arrivée de la technologie CAPE au cours des cinq prochaines années. La connectivité à des fins de télématique, de diagnostic et de divertissement ainsi que divers niveaux d'autonomie sont devenus des enjeux cruciaux pour les fabricants. Même si un propriétaire de parc de véhicules ou un consommateur individuel ne souhaite pas adopter ces nouvelles caractéristiques de façon proactive, le véhicule connecté est là pour de bon et, par conséquent, devrait être pris en compte par toute entreprise qui revoit sa stratégie de cybersécurité.

Il s'agit d'une responsabilité partagée. Les gouvernements, les organismes de réglementation, les propriétaires de parcs de véhicules, les FEO et les autres organisations qui font partie de la chaîne d'approvisionnement ont tous un rôle à jouer dans le cadre des occasions et des menaces qui se présentent dans les véhicules CAPE et l'infrastructure connexe. À défaut de quoi, les risques concernant la confidentialité, les risques pour la confidentialité, les données et la sécurité deviendront un défi de taille pour l'adoption et l'utilisation de cette nouvelle technologie, et la concrétisation des excellentes occasions qu'elle présente.

Quelques considérations finales :

1. Pour gérer la multitude de risques émergents, la sécurité dès la conception devrait être la nouvelle devise dans l'ensemble de la chaîne d'approvisionnement automobile. Ce n'est qu'à ce moment-là que la cybersécurité pourra devenir un catalyseur plutôt qu'un obstacle à l'adoption rapide et généralisée des véhicules CAPE.

2. Le gouvernement et les organismes de réglementation joueront un rôle essentiel pour l'avenir de la sécurité des services et des infrastructures de transport. Le besoin de mettre en place les normes de cybersécurité et de les faire respecter doit être abordé par les organismes de réglementation; le marché n'attendra pas que la réglementation rattrape la technologie.

3. Les leaders d'affaires et technologiques doivent prendre totalement en compte tous les risques associés à un parc de véhicules hyperconnectés. La stratégie de cybersécurité doit s'étendre à tous les actifs, à tous les niveaux, pour faire en sorte que l'ensemble des risques et des menaces soient contrôlés.

4. La responsabilité de la sécurité à l'échelle de la chaîne de valeur CAPE est partagée. La chaîne d'approvisionnement, les FSC, les FEO et les propriétaires de parcs de véhicules assument différentes parts de la responsabilité à l'égard de la sécurité, de la protection des renseignements personnels et des risques pour leur entreprise et la sécurité des utilisateurs.

Les nouvelles possibilités qu'engendrent les véhicules et l'infrastructure CAPE continueront de changer la donne. Des modèles de produit et de service novateurs donneront lieu à une augmentation de l'efficacité, à un avantage concurrentiel, à une conformité environnementale et à des économies de coûts. La promesse de nouveaux clients et de l'augmentation de la part de marché pour les organisations qui prennent ce virage signifie que peu d'organisations ignorent fi de l'incidence de la connectivité et de l'autonomie sur leurs activités. Même si elles gagnent en importance, les préoccupations à propos de la sécurité peuvent, et doivent, être gérées au moyen d'une stratégie claire et inclusive tout au long du cycle de vie des véhicules CAPE, de l'approvisionnement à la fin de vie utile. Si l'on comprend bien les responsabilités partagées de sécurité des véhicules CAPE et que l'on exerce un contrôle rigoureux, axé sur la gestion des risques, la voie vers la création d'une valeur ajoutée se révélera un parcours fructueux vers un avenir nouveau.

Notes de fin

1. Transports Canada, « Véhicules connectés et automatisés », 7 mai 2021. [En ligne].
2. B. De Muynck, « *The 2020 Top Strategic Transportation Technology Trends* », 9 juin 2020. [En ligne].
3. OMS, « Accidents de la route », 21 juin 2021. [En ligne].
4. Nations Unies, « *68% of the world population projected to live in urban areas by 2050, says UN* », 16 mai 2018. [En ligne].
5. M. Sconci et D. Buksner, « LABOUR SHORTAGE IN THE TRUCKING INDUSTRY: FURTHER IMPACTS OF COVID-19 », 2 juillet 2020. [En ligne].
6. Gouvernement du Canada, « Programme d'infrastructure pour les véhicules à émission zéro », 21 décembre 2021. [En ligne].
7. Upstream Security Limited, *2022 Global Automotive Cybersecurity Report*, Upstream Security Limited, 2022.
8. M. DeGeurin, *Teen Security Researcher Claims He Can Remotely Access 25 Teslas Around the Globe*, Gizmodo, 2022.
9. Upstream, *Luxury OEM experiences data leak*, Upstream, 2021.
10. Deloitte, « Sondage sur l'avenir de la cybersécurité 2021 », 2021. [En ligne]. Accessible : https://www2.deloitte.com/ca/fr/pages/risk/articles/avenir-de-la-cybersecurite.html.
11. UNECE, « Forum mondial de l'harmonisation des Règlements concernant les véhicules (WP.29) », 2021. [En ligne].
12. Gartner, « *How Automotive CIOs Can Lead a Successful Cybersecurity Implementation and Comply With WP.29 UN R155* », 18 juin 2021. [En ligne].
13. ISO, « ISO/DIS 24 089 Véhicules routiers — Ingénierie de mise à jour du logiciel », 2021. [En ligne].
14. ISO, « ISO/SAE 21434:2021 Véhicules routiers — Ingénierie de la cybersécurité », août 2021. [En ligne].
15. SAE International, « Cybersecurity Guidebook for Cyber-Physical Vehicle Systems », 14 janvier 2016. [En ligne].

Personne-ressource

Stephen Meagher
Directeur de service,
Conseils en gestion des risques
416-202-2319
smeagher@deloitte.ca

Collaborateurs

Damu Prabhu
Associé,
Conseils en gestion des risques

Vaibhav Jani
Directeur principal,
Conseils en gestion des risques

Noorullah Nouri
Conseiller principal,
Conseils en gestion des risques

Aawista Chaudhry
Conseillère,
Conseils en gestion des risques

William Chinnery
Analyste,
Conseils en gestion des risques

Leon Nash
Associé,
Conseils en gestion des risques et leader,
Véhicules CAPE

Darren Plested
Associé,
Secteur national de l'automobile et leader,
Innovation en transports

Yvonne Rene de Cotret
Associée,
Secteur national du transport et leader,
Avenir de la mobilité

Andrew Pau
Associé, Secteur national du transport,
Services gouvernementaux et publics
et leader du groupe de comptes
de la Colombie-Britannique

Remerciements

Les auteurs tiennent à remercier les leaders suivants de Deloitte,
qui ont contribué aux recherches et à la révision du présent rapport :

Amir Belkhelladi, Ashok Divakaran, Noemi Chanda, Don MacPherson, Marc MacKinnon, D'Arcy Moynaugh, Justin Fong, Kevvie Fowler, Ryan Robinson, Dejan Markovic, Ryan Ernst, Sima Gupta, Ian Davidson et **Bear Zak.** Les points de vue des personnes suivantes nous ont également aidés à façonner ce rapport : **Ian Todd, Bob Oates, Rita Barrios** et **Aditya Deshpande** de **BlackBerry Limited**, ainsi que **Raed Kadri, chef du Réseau Ontarien d'innovation pour les véhicules (ROIV).**

À propos de Deloitte
Deloitte offre des services dans les domaines de l'audit et de la certification, de la consultation, des conseils financiers, des conseils en gestion des risques, de la fiscalité et d'autres services connexes à de nombreuses sociétés ouvertes et fermées dans différents secteurs. Deloitte sert quatre entreprises sur cinq du palmarès Fortune Global 500[MD] par l'intermédiaire de son réseau mondial de cabinets membres dans plus de 150 pays et territoires, qui offre les compétences de renommée mondiale, le savoir et les services dont les clients ont besoin pour surmonter les défis d'entreprise les plus complexes. Deloitte S.E.N.C.R.L./s.r.l., société à responsabilité limitée constituée en vertu des lois de l'Ontario, est le cabinet membre canadien de Deloitte Touche Tohmatsu Limited. Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société fermée à responsabilité limitée par garanties du Royaume-Uni, ainsi que son réseau de cabinets membres dont chacun constitue une entité juridique distincte et indépendante. Pour une description détaillée de la structure juridique de Deloitte Touche Tohmatsu Limited et de ses sociétés membres, voir www.deloitte.com/ca/apropos.

Notre raison d'être mondiale est d'avoir une influence marquante. Chez Deloitte Canada, cela se traduit par la création d'un avenir meilleur en accélérant et en élargissant l'accès au savoir. Nous croyons que nous pouvons concrétiser cette raison d'être en incarnant nos valeurs communes qui sont d'ouvrir la voie, de servir avec intégrité, de prendre soin les uns des autres, de favoriser l'inclusion et de collaborer pour avoir une influence mesurable.

Pour en apprendre davantage sur les quelque 330 000 professionnels de Deloitte, dont plus de 11 000 font partie du cabinet canadien, veuillez nous suivre sur LinkedIn, Twitter, Instagram ou Facebook.

Conçu et produit par l'Agence | Deloitte Canada. 22-5608617