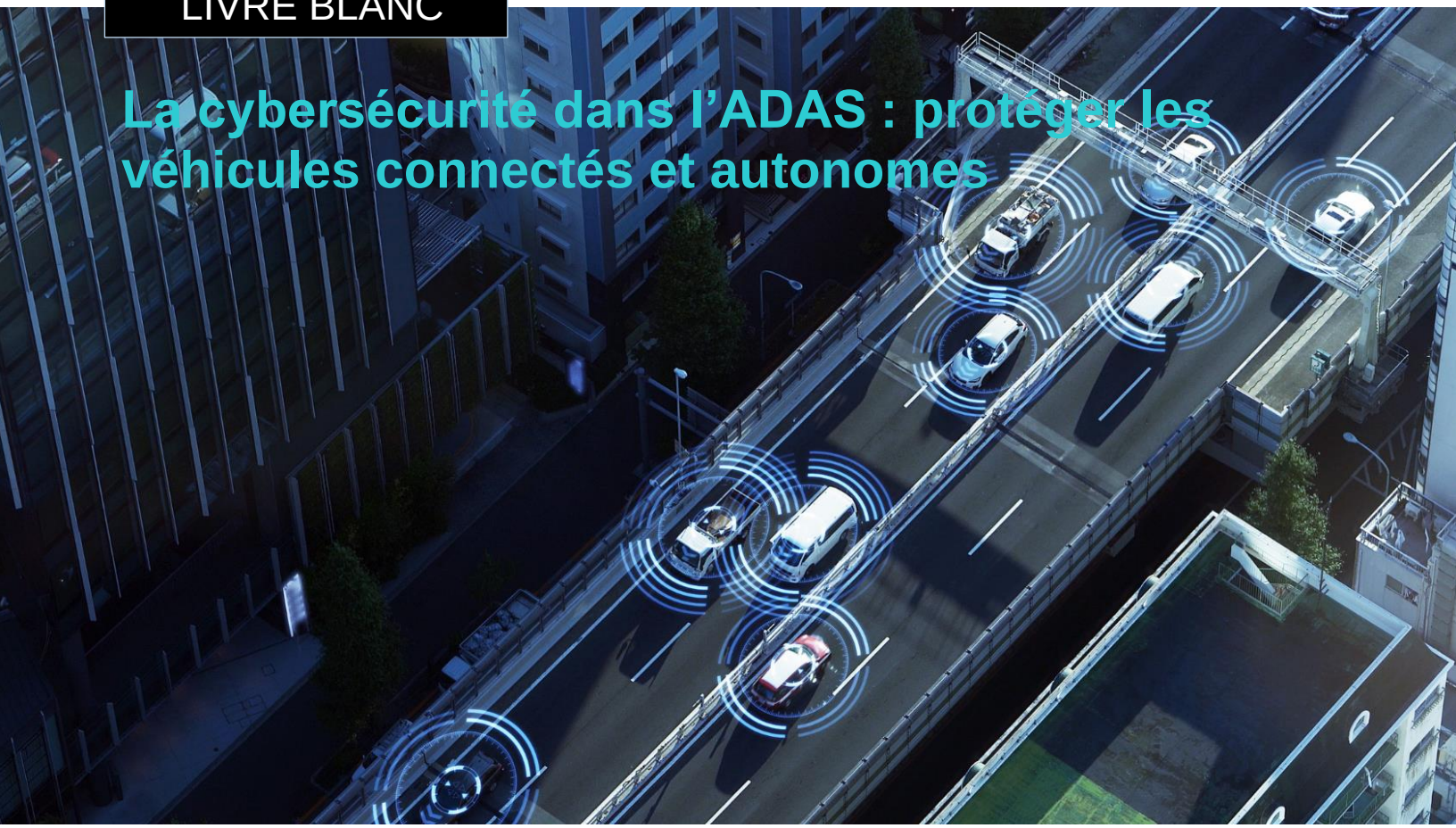
LivreBlanc

La cybersécurité dans l’ADAS : protéger les véhicules connectés et autonomes



Date de publication : 12 septembre 2024

Résumé analytique

Juillet 2024[1] : une cyberattaque frappe l’aéroport de la ville côtière de Split, en Croatie, entraînant l’annulation et le retard de plusieurs vols et obligeant les passagers à passer la nuit à l’aéroport.

Juin 2024 : le fournisseur de logiciels automobiles CDK Global subit plusieurs cyberattaques, entraînant la mise hors ligne de plus de 15 000 concessionnaires à travers l’Amérique du Nord.

Juin 2024 : le gouvernement japonais annonce que son agence spatiale est la cible d’une série de cyberattaques depuis 2023. Heureusement, le réseau compromis ne contient pas d’informations sensibles sur les fusées ou les satellites.

Avril 2024 : des pirates informatiques attaquent le portefeuille national de cryptomonnaie du Salvador, Chivo, exposant les informations personnelles sensibles de millions de Salvadoriens. Ils divulguent également le code source de Chivo.

1 Les liens externes peuvent renvoyer à du contenu en anglais.

© 2024 LeddarTech Holdings Inc. Tous droits réservés. Le présent document ne peut être reproduit, distribué ou communiqué, en totalité ou en partie, sans l’accord écrit explicite de LeddarTech.
LeddarTech Holdings Inc. est une société publique cotée au NASDAQ sous le symbole « LDTC ».

Les cyberattaques touchent de plus en plus d'industries[2]. Qu'elle soit privée ou publique, grande ou petite, aucune entreprise n'est à l'abri de ce type de menace. Les motivations des hackers varient, allant de la demande de rançon à la divulgation publique de renseignements privés. À mesure que l'industrie automobile évolue vers un avenir défini par logiciel, il est essentiel de donner la priorité à la cybersécurité dans la conception et le déploiement des véhicules.

Le présent livre blanc explore l'impact de la cybersécurité sur l'industrie automobile, en mettant l'accent sur les véhicules définis par logiciel, les véhicules connectés, les systèmes avancés d'aide à la conduite (ADAS[3]) et les véhicules automatisés (AV[4]), ainsi que sur les pratiques de conception qui peuvent être mises en œuvre pour renforcer la cybersécurité.

Comprendre les véhicules définis par logiciel

Les véhicules définis par logiciel (SDV[5]) représentent l'avenir de la technologie automobile, où les fonctionnalités, les performances, les caractéristiques et la valeur découlent des capacités logicielles du véhicule plutôt que du matériel comme le châssis, la boîte de vitesses ou le moteur. Aujourd'hui, les fabricants d'équipements d'origine (OEM[6]) ou équipementiers, tant traditionnels que nouveaux, s'engagent dans la voie des SDV, offrant aux utilisateurs la possibilité d'acheter des fonctionnalités telles que la régulation de vitesse adaptative (ACC[7]), la conduite pilotée et les phares adaptatifs par le biais d'un service d'abonnement. Les SDV sont équipés du matériel nécessaire à la prise en charge de ces fonctionnalités dès leur sortie d'usine. Lorsque les clients s'abonnent à ces fonctionnalités supplémentaires, le véhicule est mis à jour en temps réel par voie hertzienne[8], ce qui leur permet de profiter des nouvelles options disponibles sans la nécessité d'une visite chez un concessionnaire.

Les SDV sont construits sur des plateformes logicielles avancées qui peuvent être mises à jour, personnalisées et optimisées au fil du temps. Cette approche permet d'améliorer en continu les fonctionnalités du véhicule, comme l'ADAS, l'infodivertissement et même les performances du groupe motopropulseur, sans qu'il soit nécessaire d'apporter des modifications physiques au véhicule. Les mises à jour logicielles, souvent fournies en temps réel, permettent aux fabricants d'introduire de nouvelles fonctionnalités, de corriger des bogues et d'améliorer la sécurité après l'achat initial, transformant ainsi le véhicule en un produit dynamique qui évolue tout au long de son cycle de vie.

Une voiture moderne fonctionne avec plus de 100 millions de lignes de code et 250 Go de données qui circulent dans son système. Elle contient plus de 1 500 fils qui s'étendent sur des kilomètres. Comparativement, les véhicules produits au début des années 2000 comportaient beaucoup moins de composants logiciels et de câblage, et ceux des années 1970 encore moins. Compte tenu de l'importance qu'ont prise les logiciels dans la vie quotidienne, il n'est guère étonnant qu'ils aient eu un impact sur l'industrie automobile. Ce qui est surprenant, en revanche, c'est qu'il ait fallu autant de temps pour que les logiciels deviennent la pierre angulaire de cette évolution.

2 Comme mentionné dans un article de Forbes mis à jour le 28 août 2024 : Cybersecurity Statistics.
3 Advanced driver assistance systems.
4 Automated vehicles.
5 Software-defined vehicles.
6 Original equipment manufacturers.
7 Adaptive cruise control.
8 Technologie "over-the-air" (OTA).

© 2024 LeddarTech Holdings Inc. Tous droits réservés. Le présent document ne peut être reproduit, distribué ou communiqué, en totalité ou en partie, sans l'accord écrit explicite de LeddarTech.
LeddarTech Holdings Inc. est une société publique cotée au NASDAQ sous le symbole « LDTC ».

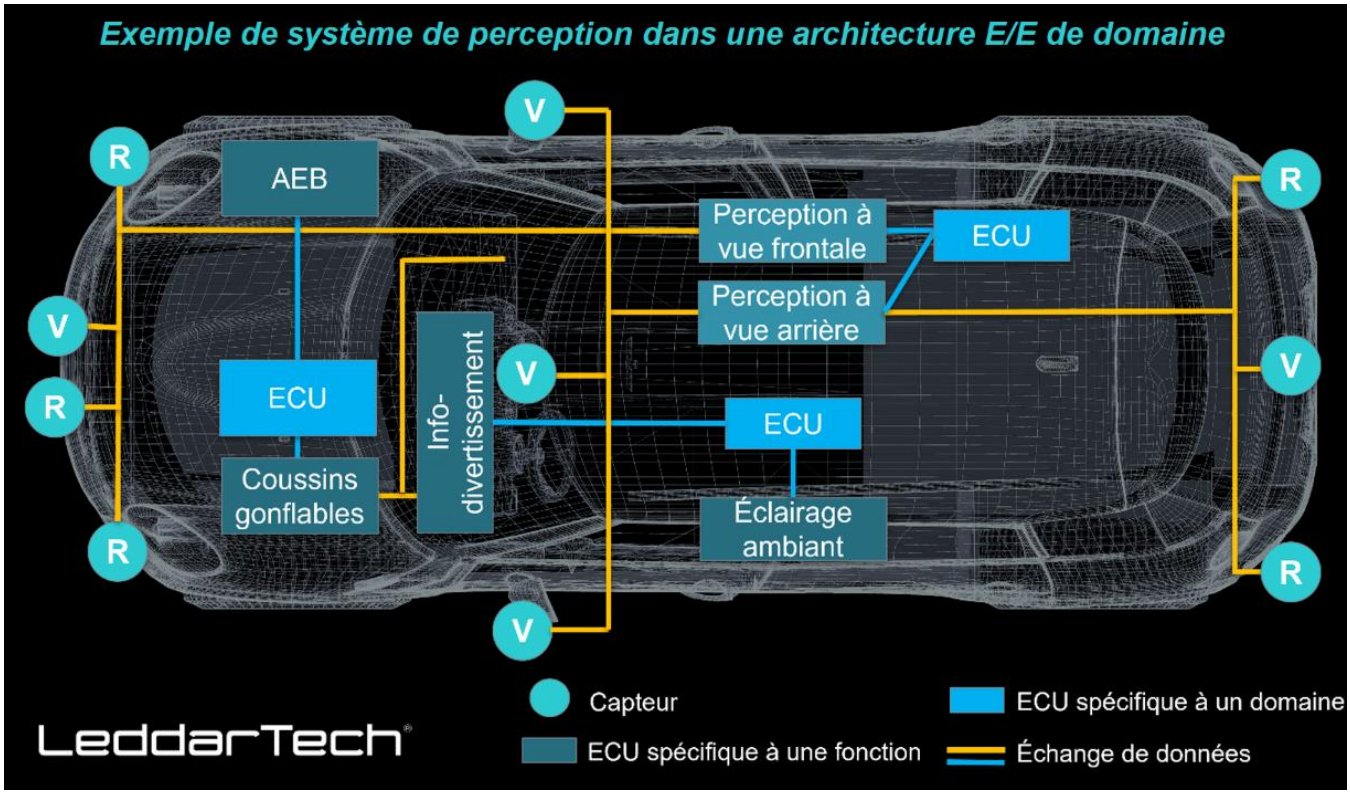


Figure 1 – Exemple d'échange de données dans un véhicule moderne. Les SDV du futur transformeront la conception électrique/électronique en adoptant une architecture zonale.

Les défis de la cybersécurité dans l'industrie automobile

L'industrie automobile fait face à des défis uniques, rarement rencontrés par de nombreux produits reposant sur des logiciels. Les constructeurs automobiles doivent se conformer à des exigences de sécurité strictes, intégrer de multiples systèmes provenant de fournisseurs tiers et sur lesquels ils n'ont souvent qu'un contrôle limité, respecter les normes réglementaires nationales et internationales, et coordonner leurs efforts avec les concessionnaires pour livrer le produit aux clients. Les constructeurs automobiles traditionnels sont confrontés à des défis supplémentaires dans la transition vers un avenir défini par logiciel en raison de l'important bagage technique qu'ils détiennent. Après avoir fabriqué des véhicules pendant des décennies, acquis des entreprises et adopté diverses suites technologiques, ces constructeurs doivent désormais trouver un moyen de concevoir des véhicules de manière cohérente et d'intégrer plusieurs infrastructures technologiques en douceur. Traditionnellement, la conception des véhicules était modulaire, avec des domaines distincts tels que le châssis, l'infodivertissement, la régulation de température et la motorisation. Cependant, le virage vers un avenir piloté par logiciel exige une approche de conception holistique. Les nouveaux constructeurs, dépourvus de contraintes héritées, peuvent développer leurs SDV sur un nombre réduit de plateformes technologiques, ce qui favorise une approche plus intégrée dans la conception des véhicules ainsi qu'une gestion client optimisée.

Une cybersécurité exceptionnelle est indispensable pour que les constructeurs automobiles puissent déployer avec succès leurs véhicules définis par logiciel. Les vols de voitures sont en augmentation dans de nombreuses régions d'Amérique du Nord et d'Europe, l'une des méthodes les plus répandues étant l'attaque par relais[9]. Lors d'une attaque par relais, les voleurs utilisent des relais radio portatifs pour étendre la portée de communication entre la voiture et sa clé. Ils utilisent d'abord un relais pour

[9] Ken Tindell, "Can Injection," Canis Automotive Labs, CTO Blog.

© 2024 LeddarTech Holdings Inc. Tous droits réservés. Le présent document ne peut être reproduit, distribué ou communiqué, en totalité ou en partie, sans l'accord écrit explicite de LeddarTech.
LeddarTech Holdings Inc. est une société publique cotée au NASDAQ sous le symbole « LDTC ».

capter le signal de la voiture et le transmettre à un deuxième relais placé près de la clé. Ce deuxième relais renvoie ensuite le signal à la voiture, ce qui provoque son déverrouillage. Les voleurs peuvent alors s'emparer du véhicule. Lorsque cette méthode a été connue, les propriétaires d'autos ont commencé à ranger leurs clés dans des boîtes métalliques pour bloquer le signal. En réponse, les voleurs ont mis au point de nouvelles techniques.

Dans les véhicules plus modernes, le risque de vol est atténué grâce au couplage d'une clé intelligente avec le véhicule. Cette clé intelligente échange des messages cryptographiques avec le véhicule. Lorsque celui-ci demande l'authentification de la clé, il exige une réponse cryptographique valide pour déverrouiller la voiture et désactiver le dispositif d'antidémarrage. Cette mesure de sécurité avancée aide à prévenir l'accès non autorisé et le vol.

Figure 2 – Illustration d'un vol de voiture résultant de mesures de cybersécurité inadéquates

En réponse aux fonctionnalités de sécurité renforcées des véhicules modernes, les voleurs ont commencé à utiliser l'injection CAN[10]. Le CAN, ou Controller Area Network, est un protocole de communication qui permet aux différentes unités de commande électroniques (ECU[11]) d'un véhicule de communiquer entre elles par l'intermédiaire d'un câble de communication. L'injection CAN fonctionne comme suit : les voleurs accèdent au système de communication interne de la voiture, le bus CAN, et transmettent de faux messages qui imitent ceux envoyés par la clé intelligente. Ces messages frauduleux déverrouillent le véhicule et neutralisent l'antidémarreur. La plupart des voitures actuelles ne vérifient pas l'authenticité des messages internes du bus CAN, ce qui les rend vulnérables au vol.

La cybersécurité des véhicules est primordiale, car les voitures d'aujourd'hui sont de plus en plus connectées et dépendantes des logiciels pour contrôler des systèmes critiques tels que le freinage, la direction et l'ADAS. Une faille dans la cybersécurité pourrait permettre à des pirates de prendre le contrôle de ces systèmes, ce qui pourrait entraîner des accidents, des vols de voiture ou même de la surveillance illicite. De plus, les véhicules collectent et transmettent des données personnelles sensibles, ce qui en fait des cibles attrayantes pour les violations de sécurité. Des mesures de cybersécurité robustes sont donc indispensables non seulement pour protéger la sécurité physique des conducteurs et des passagers, mais aussi pour préserver leur vie privée et maintenir la confiance des consommateurs dans une industrie automobile en rapide évolution.

10 Zac Palmer, "Thieves are now stealing cars via a headlight CAN injection," Autoblog.

11 Electronic control units.

© 2024 LeddarTech Holdings Inc. Tous droits réservés. Le présent document ne peut être reproduit, distribué ou communiqué, en totalité ou en partie, sans l'accord écrit explicite de LeddarTech.
LeddarTech Holdings Inc. est une société publique cotée au NASDAQ sous le symbole « LDTC ».

La plupart des véhicules aujourd'hui sont équipés de caméras, souvent multiples. Lorsque ces véhicules circulent sur les routes et se déplacent d'un point A à un point B, ils capturent des images des visages de personnes. Veiller à ce que les voitures ne soient pas utilisées à des fins d'espionnage et protéger la vie privée et les données des individus sont également des préoccupations majeures pour tous les acteurs concernés.

Les implications de la cybersécurité pour les véhicules autonomes et les systèmes ADAS sont considérables. Une cybersécurité défaillante dans les systèmes ADAS et les systèmes de conduite autonome peut avoir des conséquences dévastatrices, telles que la perte de contrôle du véhicule, des problèmes de navigation, la possibilité de se retrouver piégé à l'intérieur du véhicule ou des accidents. Pour garantir la sécurité des véhicules présents et futurs, l'industrie automobile a adopté des normes et des processus visant à fabriquer des produits sûrs, sécurisés et fiables.

Normes applicables à l'ADAS et à la conduite autonome

Bien qu'il existe de nombreuses normes applicables aux différents aspects de la conduite autonome, ce document met l'accent sur les principales d'entre elles :

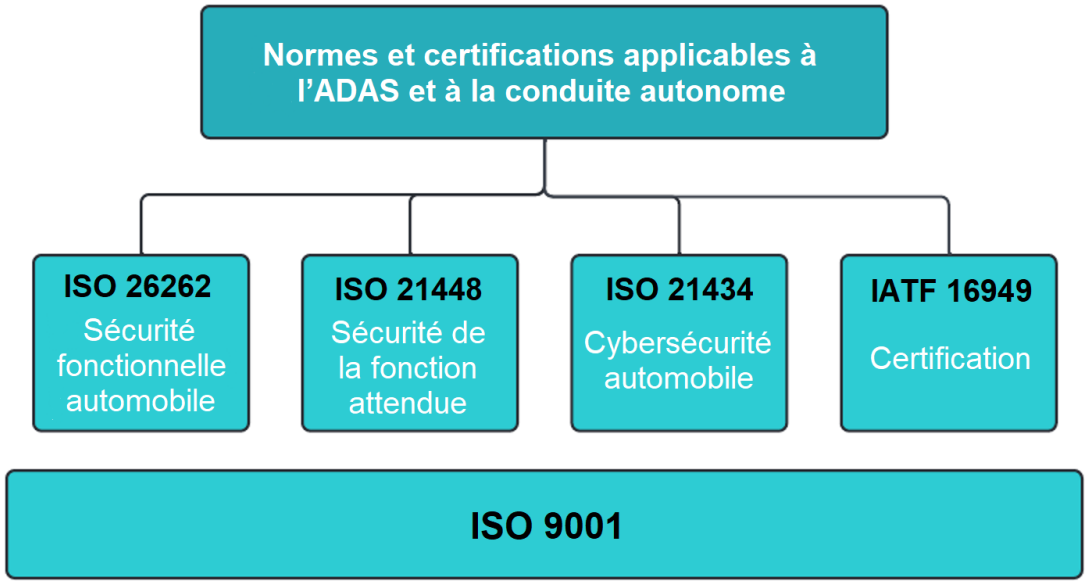


Figure 3 – Normes et certifications applicables à l'ADAS et à la conduite autonome (schéma fonctionnel)

- **ISO 26262 – Sécurité fonctionnelle automobile (FuSA)** : FuSA[12] est une approche complète qui vise à garantir la sécurité électronique des véhicules. Elle a pour objectif de protéger les conducteurs, les passagers et les usagers vulnérables de la route (VRU[13]), notamment les piétons, les cyclistes, les motocyclistes et autres, contre les blessures causées par des défaillances dans l'électronique et les logiciels embarqués dans les véhicules.
- **ISO 21448 – Sécurité de la fonction attendue (SOTIF)** : SOTIF[14] se concentre sur l'élimination des risques déraisonnables causés par des dangers résultant d'inadéquations fonctionnelles de la fonctionnalité prévue ou d'une mauvaise utilisation prévisible par des individus. La norme ISO 21448 fournit des lignes directrices pour atteindre ce niveau de sécurité.

12 Functional Safety.
13 Vulnerable road users.
14 Safety of the Intended Functionality.

© 2024 LeddarTech Holdings Inc. Tous droits réservés. Le présent document ne peut être reproduit, distribué ou communiqué, en totalité ou en partie, sans l'accord écrit explicite de LeddarTech.
LeddarTech Holdings Inc. est une société publique cotée au NASDAQ sous le symbole « LDTC ».

- **ISO 21434 – Cybersécurité automobile** : cette norme fournit des lignes directrices pour améliorer la cybersécurité dans l'industrie automobile et aborde des questions telles que :
  - Gestion de la cybersécurité organisationnelle et au niveau des projets
  - Gestion de la cybersécurité avec les fournisseurs
  - Cybersécurité durant les phases de conception, de développement et de production du produit
  - Réponse aux incidents, analyse des menaces et évaluation des risques
- **IATF 16949 – International Automotive Task Force** : IATF 16949 est une norme de système de gestion de la qualité automobile axée sur l'amélioration continue. Elle met l'accent sur la prévention des défauts et la réduction des variations dans la chaîne d'approvisionnement et les processus d'assemblage du secteur automobile.

Ces normes sont indispensables dans l'industrie automobile, car elles fournissent un cadre pour garantir la sûreté et la sécurité de véhicules de plus en plus complexes. Dans le contexte de ce livre blanc, la norme ISO 21434 propose l'ensemble de lignes directrices le plus complet pour consolider la cybersécurité des véhicules, couvrant tous les volets, de la conception et du développement à la production en passant par la maintenance.

L'ISO 21434 garantit que les constructeurs mettent en œuvre des pratiques de cybersécurité rigoureuses pour se protéger contre des menaces comme le piratage, les violations de données et les accès non autorisés, susceptibles de compromettre la sécurité des véhicules et la vie privée des utilisateurs. Cette norme s'applique à divers sous-systèmes du véhicule, y compris les véhicules connectés, les systèmes électroniques, les logiciels, l'ADAS et la conduite autonome, entre autres. Elle fournit aux développeurs les connaissances nécessaires pour intégrer des mesures de cybersécurité durant tout le cycle de développement et la chaîne d'approvisionnement.

Cette norme repose sur une approche fondée sur le risque, exigeant des constructeurs qu'ils identifient de façon systématique les menaces potentielles entourant la cybersécurité, évaluent leur impact et mettent en place les mesures d'atténuation appropriées. Elle englobe, entre autres aspects, l'intégration de la cybersécurité dans la conception et le développement afin de s'assurer que les véhicules sont conçus *dans une optique de sécurité*. L'ISO 21434 met fortement l'accent sur la surveillance continue et la capacité de réponse aux incidents, permettant ainsi de détecter et de réagir rapidement aux menaces tout au long du cycle de vie du véhicule.

De plus, l'ISO 21434 établit une base de coopération entre toutes les parties prenantes de la chaîne d'approvisionnement automobile, en insistant sur le fait que la cybersécurité est affaire de responsabilité collective.

La cybersécurité jouera un rôle de plus en plus important à mesure que l'industrie automobile évoluera vers un avenir dominé par les véhicules définis par logiciel. Ces véhicules, qui offriront des mises à jour de performance et des corrections de bogues et permettront de débrider des fonctionnalités avancées d'aide à la conduite, le tout à distance et en direct, nécessiteront des fournisseurs fiables qui comprennent l'importance de développer des solutions logicielles conformes aux normes mentionnées plus haut, tout en conciliant les défis en termes de performance et de coût.

© 2024 LeddarTech Holdings Inc. Tous droits réservés. Le présent document ne peut être reproduit, distribué ou communiqué, en totalité ou en partie, sans l'accord écrit explicite de LeddarTech.
LeddarTech Holdings Inc. est une société publique cotée au NASDAQ sous le symbole « LDTC ».

Cybersécurité pour les véhicules équipés de systèmes ADAS

La cybersécurité pour les véhicules dotés de systèmes avancés d'aide à la conduite implique la protection des systèmes électroniques, des réseaux de communication, des logiciels et des données contre les cybermenaces et les intrusions. Les fonctionnalités ADAS, comme la régulation de vitesse adaptative (ACC[15]), l'aide au suivi de voie (LKA[16]) et le freinage automatique d'urgence (AEB[17]), s'appuient sur des capteurs, des caméras, des radars et des logiciels complexes. L'intégration croissante de ces technologies introduit de nouveaux défis en matière de cybersécurité et des vulnérabilités potentielles. Voici un aperçu des éléments clés de la cybersécurité pour les véhicules équipés de systèmes ADAS :

1. **Protection des réseaux de communication** : l'ADAS repose sur divers protocoles de communication internes, tels que CAN (Controller Area Network), LIN (Local Interconnect Network) et Ethernet, ainsi que sur des communications externes comme V2X[18] (« véhicule-à-tout »). Protéger ces canaux de communication contre les cybermenaces –y compris les attaques dites « par interception », « par mystification » ou par usurpation d'identité et par brouillage– est essentiel pour garantir la sécurité et la fonctionnalité du système.
2. **Sécurité des capteurs** : les systèmes ADAS reposent sur des capteurs tels que des caméras, des radars, des LiDARs et des capteurs à ultrasons pour interpréter l'environnement du véhicule. Les cybercriminels peuvent cibler ces capteurs pour leur fournir de fausses données, ce qui peut entraîner des prises de décision erronées. Assurer l'intégrité des données de capteurs par le biais de techniques de validation et de protocoles de communication sécurisés est primordial.
3. **Sécurité logicielle et pratiques de codage sécurisées** : les fonctionnalités ADAS sont régies par des algorithmes logiciels complexes. Il est essentiel de garantir l'utilisation de pratiques de codage sécurisées, ainsi que des tests rigoureux et des évaluations de vulnérabilité, afin de minimiser le risque d'attaques logicielles. Des mises à jour régulières et une gestion efficace des correctifs sont également capitales pour traiter les vulnérabilités nouvellement constatées et maintenir la sécurité du système.
4. **Mises à jour logicielles sécurisées (OTA)** : les véhicules équipés de systèmes ADAS peuvent recevoir des mises à jour logicielles en direct et à distance grâce à la technologie OTA (par voie hertzienne). Il est indispensable de garantir que ces mises à jour sont livrées en toute sécurité sans être interceptées, modifiées ni corrompues. Les mécanismes OTA sécurisés reposent généralement sur le cryptage, les signatures numériques et l'authentification pour protéger le processus de mise à jour.
5. **Contrôle d'accès et authentification** : des mesures de contrôle d'accès strictes sont impératives pour garantir que seuls les utilisateurs et les dispositifs autorisés peuvent interagir avec les fonctionnalités ADAS du véhicule. Cela implique la mise en œuvre d'une authentification multifactorielle, de clés cryptographiques et de certificats sécurisés pour les systèmes interagissant avec l'ADAS, afin de prévenir tout accès ou manipulation illicite.
6. **Systèmes de détection et de prévention des intrusions (IDPS)** : il est indispensable de surveiller le réseau et les systèmes du véhicule pour détecter tout signe d'accès non autorisé ou d'activité malveillante. Les IDPS peuvent détecter des anomalies ou des cyberattaques potentielles en temps réel, ce qui permet au système de déclencher des contre-mesures pour prévenir ou minimiser les dommages.

15 Adaptive cruise control.
16 Lane keep assist.
17 Automatic emergency braking.
18 Vehicle-to-everything.

© 2024 LeddarTech Holdings Inc. Tous droits réservés. Le présent document ne peut être reproduit, distribué ou communiqué, en totalité ou en partie, sans l'accord écrit explicite de LeddarTech.
LeddarTech Holdings Inc. est une société publique cotée au NASDAQ sous le symbole « LDTC ».

7. **Confidentialité et protection des données** : les systèmes ADAS génèrent et traitent un volume important de données, notamment la vitesse du véhicule, sa localisation et d'autres informations spécifiques au conducteur. Sécuriser le stockage, la transmission et le traitement de ces données est vital pour protéger la confidentialité des utilisateurs et prévenir les violations de données.
8. **Intégrité du micrologiciel et démarrage sécurisé** : les mécanismes de démarrage sécurisé sont indispensables pour empêcher l'exécution de code malveillant dans les systèmes du véhicule. Ces mécanismes vérifient l'intégrité du micrologiciel lors du démarrage, garantissant que seul un micrologiciel autorisé et non modifié est utilisé.

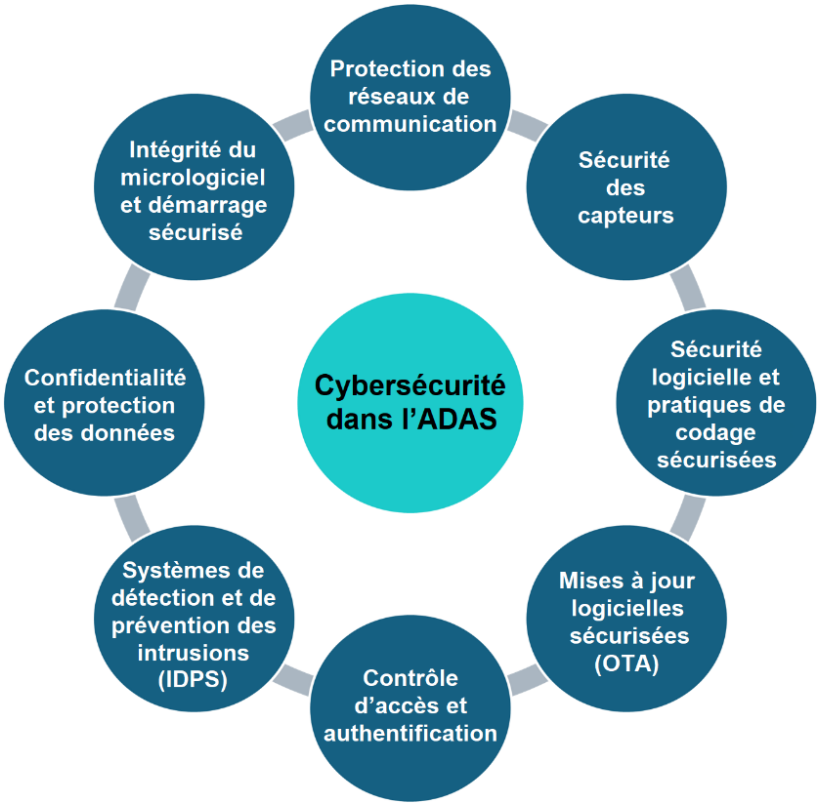


Figure 4 – Divers aspects de la cybersécurité dans l'ADAS

La cybersécurité est fondamentale pour les véhicules équipés de systèmes ADAS, car elle affecte directement la sécurité, la fiabilité et la conformité réglementaire. Les cyberattaques visant ces systèmes pourraient entraîner la prise de contrôle non autorisée de fonctions cruciales telles que la direction, le freinage ou l'accélération, posant ainsi des risques significatifs pour le conducteur, les passagers et les autres usagers de la route. La mise en œuvre de mesures de cybersécurité robustes contribue à maintenir la fiabilité des fonctionnalités ADAS, ce qui est essentiel pour renforcer la confiance du public et encourager l'acceptation par les utilisateurs. L'adoption croissante de ces technologies va de pair avec la nécessité de se conformer aux réglementations et aux normes de cybersécurité, ces dernières devenant obligatoires à mesure que les gouvernements et les organismes industriels reconnaissent l'importance de sécuriser les systèmes embarqués dans les véhicules contre les menaces potentielles. Le défaut de protéger les véhicules équipés de systèmes ADAS peut avoir de grâces conséquences, notamment des accidents, des pertes financières et des responsabilités juridiques, ce qui fait de la cybersécurité une priorité absolue pour les constructeurs automobiles et les fournisseurs de technologies.

© 2024 LeddarTech Holdings Inc. Tous droits réservés. Le présent document ne peut être reproduit, distribué ou communiqué, en totalité ou en partie, sans l'accord écrit explicite de LeddarTech.
LeddarTech Holdings Inc. est une société publique cotée au NASDAQ sous le symbole « LDTC ».

Optimiser performances et coûts avec LeddarTech

LeddarTech est une entreprise mondiale de logiciels fondée en 2007, dont le siège est situé à Québec, au Canada, et qui dispose de centres de R&D supplémentaires à Montréal et à Tel Aviv (Israël). L'entreprise propose une technologie de fusion bas niveau de capteurs et de perception innovatrice basée sur l'IA pour systèmes ADAS et AD. La technologie de LeddarTech génère un modèle environnemental 3D détaillé à partir de différents types (caméra, radar, LiDAR…) et configurations de capteurs. La solution phare de LeddarTech, LeddarVision™, répond à de nombreuses exigences de performance, telles que :

- Portée accrue
- Précision supérieure
- Réduction des fausses alertes
- Détection supérieure des objets, y compris les VRU et les objets occultés
- Détection des objets de petites dimensions

Trois avenues principales permettent aux fournisseurs de rang 1 et aux constructeurs automobiles de bénéficier de l'efficacité économique des solutions LeddarTech :

1. **Coût système inférieur** : LeddarTech réduit le coût global du système de perception en nécessitant moins de capteurs par rapport aux solutions de fusion de niveau objet. Par exemple, alors que la plupart des solutions à vue périphérique s'appuient aujourd'hui sur une configuration à 11 caméras et 5 radars, le LeddarVision « Surround » (LVS-2⁺) utilise une configuration à 5 caméras et 5 radars. Comme de nombreux capteurs sont nécessaires pour la perception à vue frontale ou périphérique dans chaque véhicule, les économies par véhicule peuvent augmenter rapidement sur les millions de véhicules produits par les équipementiers automobiles. Selon une étude interne de LeddarTech et des estimations basées sur l'information disponible sur le marché, les solutions de perception à vue frontale (LVF-E) et à vue périphérique (LVS-2⁺) de LeddarTech sont respectivement 44 % et 48 % plus économiques que leurs homologues centrées sur la caméra.
2. **Compression des coûts à long terme** : les solutions LeddarTech sont évolutives, ce qui permet à la même plateforme de prendre en charge l'ADAS de niveau 2 et d'être adaptée à des niveaux de conduite automatisée supérieurs. Cette approche architecturale unifiée réduit les efforts de réingénierie requis par les changements de capteurs et permet d'accroître efficacement la puissance de calcul suivant l'ajout des capteurs nécessaires pour appuyer des niveaux d'aide à la conduite et de conduite autonome plus élevés. Par conséquent, cette évolutivité peut réduire considérablement le temps, les efforts et les dépenses de R&D pour les fournisseurs de rang 1 et les équipementiers automobiles.
3. **Économies de coûts indirectes** : la réduction des exigences en matière de capteurs offre non seulement des avantages directs en termes de coûts, mais affecte aussi indirectement d'autres coûts système. Une réduction du nombre de capteurs permet une diminution des coûts de traitement, une meilleure gestion thermique et davantage d'économies d'énergie. De plus, la réduction du nombre de capteurs entraîne une diminution des exigences de câblage et du poids du véhicule, ce qui génère à son tour une baisse des coûts en termes d'électricité et d'électronique (E/E).

© 2024 LeddarTech Holdings Inc. Tous droits réservés. Le présent document ne peut être reproduit, distribué ou communiqué, en totalité ou en partie, sans l'accord écrit explicite de LeddarTech.
LeddarTech Holdings Inc. est une société publique cotée au NASDAQ sous le symbole « LDTC ».

Le présent livre blanc ne constitue pas un modèle de référence. Les recommandations contenues aux présentes sont fournies « en l'état » et sans garantie quant à leur exhaustivité ou leur exactitude.

LeddarTech® a tout mis en œuvre pour s'assurer que les renseignements contenus dans le présent document sont exacts. La totalité des renseignements contenus aux présentes sont fournis « en l'état ». LeddarTech ne pourra être tenue pour responsable d'aucune erreur ou omission dans le présent document ni d'aucun préjudice découlant de l'information contenue aux présentes ou y afférent. LeddarTech se réserve le droit de modifier la conception ou les caractéristiques de ses produits à tout moment, sans préavis et à sa seule discrétion.

LeddarTech ne répond pas de l'installation de ses produits ni de l'usage qui en est fait, et décline toute responsabilité si un produit est utilisé pour une application pour laquelle il ne convient pas. Il vous incombe entièrement (1) de sélectionner les produits appropriés pour votre application, (2) de valider, concevoir et tester votre application, et (3) de vous assurer que votre application répond aux normes de sûreté et de sécurité en vigueur.

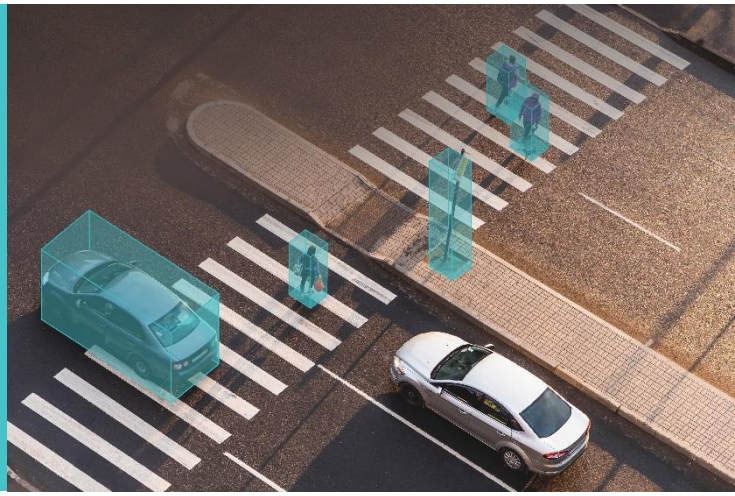
De plus, les produits LeddarTech sont assujettis aux conditions générales de vente de LeddarTech ou autres conditions applicables convenues par écrit. En achetant un produit LeddarTech, vous vous engagez également à lire attentivement l'information contenue dans le guide d'utilisation qui accompagne le produit acheté et à y être lié.

Leddar, LeddarTech, LeddarVision, LeddarSP, VAYADrive, VayaVision et les logos associés sont des marques de commerce ou des marques déposées de LeddarTech Holdings Inc. et de ses filiales. Tous les autres noms de marques, noms de produits et marques sont ou peuvent être des marques de commerce ou des marques déposées utilisées pour désigner les produits ou les services de leurs propriétaires respectifs.

À propos de LeddarTech

Entreprise mondiale de logiciels fondée en 2007, basée à Québec et disposant de centres de R&D supplémentaires à Montréal et Tel Aviv (Israël), LeddarTech développe et propose des solutions logicielles complètes de fusion bas niveau de capteurs et de perception reposant sur l'intelligence artificielle qui permettent le déploiement d'applications ADAS, de conduite autonome (AD) et de stationnement. Les logiciels de classe automobile de LeddarTech appliquent des algorithmes d'intelligence artificielle et de vision numérique avancés afin de générer des modèles 3D précis de l'environnement, pour une meilleure prise de décision et une navigation plus sûre. Cette technologie performante, évolutive et économique permet la mise en œuvre efficace de solutions ADAS pour véhicules automobiles et hors route par les équipementiers et les fournisseurs de rang 1 et 2. Ayant déposé plus de 160 demandes de brevets (dont 87 accordées) qui améliorent les capacités des systèmes d'aide à la conduite, de conduite autonome et de stationnement, l'entreprise a contribué à plusieurs innovations liées à des applications de télédétection. Une plus grande conscience situationnelle est essentielle pour rendre la mobilité plus sûre, plus efficace, plus durable et plus abordable : c'est ce qui motive LeddarTech à vouloir devenir la solution logicielle de fusion de capteurs et de perception la plus largement adoptée.

Renseignements complémentaires : sales@leddartech.com



LeddarTech®

CANADA – ÉTATS-UNIS – AUTRICHE – FRANCE – ALLEMAGNE – ITALIE – ISRAËL – HONG KONG – CHINE

Siège social
4535, boulevard Wilfrid-Hamel, bureau 240
Québec (Québec) G1P 2J7, Canada
leddartech.com

Tél. : + 1-418-653-9000
Sans frais : 1-855-865-9900

© 2024 LeddarTech Holdings Inc. Tous droits réservés. Le présent document ne peut être reproduit, distribué ou communiqué, en totalité ou en partie, sans l'accord écrit explicite de LeddarTech.
LeddarTech Holdings Inc. est une société publique cotée au NASDAQ sous le symbole « LDTC ».