Nations Unies ECE/TRANS/WP.29/GRVA/2019/2

Conseil économique et social

Distr. générale
19 novembre 2018
Français
Original : anglais

Commission économique pour l'Europe

Comité des transports intérieurs

Forum mondial de l'harmonisation des Règlements concernant les véhicules

Groupe de travail des véhicules automatisés/autonomes et connectés*

Deuxième session
Genève, 28 janvier-1er février 2019
Point 5 b) de l'ordre du jour provisoire
Véhicules automatisés/autonomes et connectés : Cybersécurité et protection des données

Proposition de recommandation sur la cybersécurité

Communication du groupe spécial de la cybersécurité et des questions de sûreté des transmissions sans fil**

La présente proposition a été élaborée par les experts du groupe spécial de la cybersécurité et des questions de sûreté des transmissions sans fil conformément au mandat approuvé par le Forum mondial de l'harmonisation des Règlements concernant les véhicules (WP.29), comme indiqué au paragraphe 28 du document ECE/TRANS/WP29/1126 et au paragraphe 27 du document ECE/TRANS/WP29/1131. Elle est fondée sur le document informel GRVA-01-17, qui a été présenté à la première session du Groupe de travail des véhicules automatisés/autonomes et connectés (GRVA), en septembre 2018. L'annexe A du présent document contient un projet de Règlement ONU sur la cybersécurité. Ledit projet comporte quatre annexes numérotées de 1 à 4.

* Ancien **Groupe de travail en matière de roulement et de freinage (GRRF)**.

** Conformément au programme de travail du Comité des transports intérieurs pour la période 2018-2019 (ECE/TRANS/274, par. 123, et ECE/TRANS/2018/21/Add.1, module 3), le Forum mondial a pour mission d'élaborer, d'harmoniser et de mettre à jour les Règlements ONU en vue d'améliorer les caractéristiques fonctionnelles des véhicules. Le présent document est soumis dans le cadre de ce mandat.

GE.18-19708 (F) 070119 090119
1819708

Table des matières

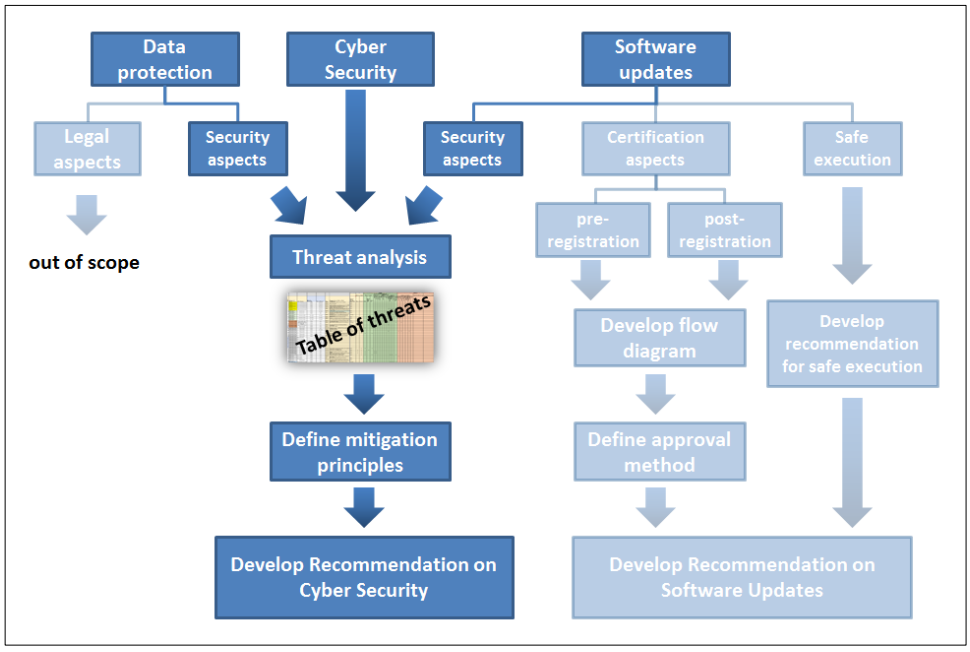
I. Introduction

A. Préambule

1.1 Un groupe spécial a été créé en tant que sous-groupe du groupe de travail informel des systèmes de transport intelligents et de la conduite automatisée (ITS/AD) du WP.29 pour examiner les questions relatives à la cybersécurité et à la sûreté des transmissions sans fil. Ce groupe est composé de représentants des Parties contractantes et d'organisations non gouvernementales telles que l'Association européenne des fournisseurs de l'automobile (CLEPA), le Comité international de l'inspection technique automobile (CITA), la Fédération internationale de l'automobile (FIA), l'Union internationale des télécommunications (UIT) et l'Organisation internationale des constructeurs automobiles (OICA).

1.2 La figure 1 illustre le champ d'application du projet de recommandation. Il est à noter qu'il existe des points communs entre la protection des données, la cybersécurité et les mises à jour de logiciels. Ces dernières comportent des aspects liés à la sécurité, à l'homologation et à l'exécution en toute sécurité qui doivent être pris en compte. Le groupe spécial a déterminé que les questions relatives à la cybersécurité et à la sûreté des transmissions sans fil étaient différentes et devaient être évaluées séparément. Le présent document examine les questions de cybersécurité, y compris la sûreté des mises à jour des logiciels. Un document distinct, intitulé « Recommandation sur les questions de sûreté des transmissions sans fil du groupe spécial de la cybersécurité et des questions de sûreté des transmissions sans fil du groupe de travail informel des systèmes de transport intelligents et de la conduite automatisée du WP.29 », examine la gestion des mises à jour de logiciels ainsi que les processus d'homologation de type.

Figure 1
Activités et produits du groupe spécial



1.3 Pour ses travaux, le groupe spécial a tenu compte du document ECE/TRANS/WP.29/2017/46 intitulé « Directive sur la cybersécurité et la protection des données », élaboré par le groupe de travail informel des systèmes de transport intelligents et de la conduite automatisée, ainsi que d'autres normes, pratiques, directives et règlements pertinents concernant la cybersécurité. Il s'agit de documents en cours d'élaboration, ainsi que de normes existantes applicables à l'industrie automobile. Ces documents sont énumérés dans l'annexe D.

1.4 Le présent document tient compte de l'état des connaissances au moment de son élaboration. Les présentes recommandations devront donc faire l'objet d'examens périodiques visant à vérifier qu'elles tiennent compte des menaces et des mesures d'atténuation nouvelles et naissantes et à les actualiser le cas échéant. Ces examens devront être effectués à l'initiative du GRVA et sous sa supervision.

B. Champ d'application

1.5 Le présent document définit les principes qui doivent être appliqués pour gérer les principales cybermenaces et vulnérabilités repérées afin d'assurer la sécurité des véhicules en cas de cyberattaques. Il définit en outre de façon détaillée des orientations ou des mesures en vue du respect de ces principes et donne notamment des exemples de procédures et d'approches techniques. Il examine enfin les évaluations ou les indicateurs qui peuvent être nécessaires pour vérifier le respect des prescriptions définies ou en vue de certifications.

1.6 Les véhicules traitent divers types de données. Le présent document définit les principes à respecter pour protéger ces données contre les accès, les modifications ou les suppressions non autorisés, tant au moment de leur stockage que de leur transmission.

C. Approche

1.7 Une évaluation a été réalisée pour inventorier les principales menaces pesant sur les véhicules et leurs principales vulnérabilités, ainsi que les principales mesures d'atténuation nécessaires pour les réduire ou les minimiser. Dans les conclusions de cette évaluation, il a délibérément été évité de prescrire des solutions techniques spécifiques (certaines sont toutefois proposées à titre d'exemples). Les principales mesures d'atténuation ont ensuite été présentées sous forme de principes.

1.8 Une analyse des menaces a été effectuée en tenant compte de l'état de la technique. Une liste des menaces a été dressée à partir de sources multiples (voir l'annexe B). Elle ne doit pas être considérée comme exhaustive, mais illustre très bien les cybermenaces pouvant peser sur les véhicules. Elle examine les différentes formes qu'elles peuvent prendre et donne des exemples précis de la façon dont elles peuvent affecter un véhicule.

1.9 Les menaces ont été regroupées selon leur similarité, et une liste de mesures d'atténuation a été dressée pour chacun de ces groupes. Une ou plusieurs façons d'atténuer les exemples de menaces relevés sont proposées. Plusieurs documents de référence ont été consultés pour recenser ces mesures d'atténuation (voir l'annexe C). Celles-ci se présentent sous forme de principes à mettre en œuvre ; si, dans certains cas, des exemples d'application de ces principes sont fournis, il n'est pas prévu de les intégrer à un règlement.

II. Définitions

2. Aux fins de la présente recommandation, on entend par :

2.1 « *Marché secondaire* », le marché du secteur automobile relatif à la fabrication, à la remise à neuf, à la distribution, à la vente au détail et à l'installation de pièces de véhicules, ainsi qu'aux logiciels, services, produits chimiques, équipements et accessoires les concernant, postérieur à la vente du véhicule au client par le constructeur automobile.

2.2 « *Authentification* », le fait de garantir qu'une caractéristique revendiquée pour une entité est correcte.

2.3 « *Accès* », le fait de pouvoir utiliser une ressource.

2.4 « *Secteur automobile* », l'ensemble des constructeurs, fournisseurs et prestataires de services d'entretien de véhicules et des fournisseurs de systèmes et de services qui interagissent avec les véhicules.

2.5 « *Cybersécurité* », la protection des véhicules routiers et de leurs fonctions contre les menaces planant sur les composants électriques ou électroniques.

2.6 « *Système de gestion de la cybersécurité (CSMS)* », une approche systématique fondée sur les risques définissant les processus, les responsabilités et les mesures de gouvernance de l'organisation ayant pour objet d'atténuer les cybermenaces et de protéger les véhicules des cyberattaques.

2.7 « *Protection des données* », la mise en œuvre de moyens administratifs, techniques ou physiques appropriés pour parer à toute divulgation, modification ou destruction non autorisée, intentionnelle ou accidentelle, des données.

2.8 « *Défense en profondeur* », un système à plusieurs niveaux de protection qui garantit un niveau de protection absolu même en cas de défaillance ou de pénétration d'un seul niveau de protection.

2.9 « *Cycle de vie* », l'ensemble des phases que traverse un véhicule, depuis sa mise au point jusqu'à son obsolescence, en passant par sa commercialisation et son utilisation active.

2.10 « *Durée de vie* », la durée de vie d'un véhicule en ce qui concerne la cybersécurité, c'est-à-dire la période comprise entre sa première immatriculation et sa mise au rebut.

2.11 « *Mesure d'atténuation* », une mesure qui modifie le risque.

2.12 « *Organisation* », une personne ou un groupe de personnes ayant des fonctions propres et disposant des responsabilités, des prérogatives et des relations nécessaires à l'atteinte de ses objectifs.

2.13 « *Mise à jour à distance* », toute méthode permettant d'effectuer des transferts de données sans fil au lieu d'utiliser un câble ou une autre connexion locale.

2.14 « *Risque* », l'effet de l'incertitude sur l'atteinte des objectifs de sécurité.

2.15 « *Appréciation du risque* », le processus englobant la recherche, la reconnaissance et la description des risques (définition des risques), en vue de comprendre la nature du risque et de déterminer son niveau (analyse du risque), et la comparaison des résultats de l'analyse du risque aux critères de risque afin de déterminer si le risque et/ou son importance sont acceptables ou tolérables (évaluation du risque).

2.16 « *Gestion du risque* », les activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque.

2.17 « *Système* », un ensemble de composants ou de sous-systèmes qui assurent une fonction.

2.18 « *Menace* », la source potentielle d'événements indésirables susceptibles de nuire à un système ou à une organisation.

2.19 « *Vulnérabilité* », un point faible d'un élément ou d'une commande, qui l'expose à une ou plusieurs menaces.

III. Principes de cybersécurité

3.1 Les principes de cybersécurité peuvent être utilisés pour illustrer comment les organisations doivent mettre en œuvre la cybersécurité tout au long du cycle de vie du véhicule. Ils peuvent être utilisés par les constructeurs automobiles, les sous-traitants, les fournisseurs et les prestataires de services.

3.2 La manière dont ces principes peuvent être respectés n'est pas explicitement définie dans le présent document. Il est plutôt recommandé que les organisations utilisent les normes (telles que la norme ISO/SAE 21434) et les processus pertinents et prennent des mesures d'atténuation appropriées pour démontrer leur respect des principes correspondant aux exigences des autorités.

3.3 Les principes de cybersécurité sont les suivants :

3.3.1 La sécurité de l'organisation doit être prise en charge, gérée et promue au plus haut niveau de l'organisation ;

3.3.2 Les risques de sécurité sont évalués et gérés de manière appropriée et proportionnée, y compris ceux propres à la chaîne d'approvisionnement ;

3.3.3 Les organisations doivent mettre en œuvre des mesures de contrôle de la cybersécurité et d'intervention en cas d'incident pour s'assurer que les systèmes sont sécurisés pendant toute leur durée de vie ;

3.3.4 Toutes les organisations, y compris les sous-traitants, les fournisseurs et les éventuels tiers, doivent conjuguer leurs efforts pour renforcer la sécurité du système ;

3.3.5 Le véhicule doit être conçu selon une approche de défense en profondeur. Le constructeur du véhicule doit concevoir son architecture de manière à réduire la probabilité que la compromission des actifs d'un élément architectural entraîne la propagation de l'attaque à d'autres éléments architecturaux ;

3.3.6 La sécurité des logiciels doit être gérée tout au long de leur durée de vie ;

3.3.7 Le stockage et la transmission des données doivent être sécurisés et contrôlés ;

3.3.8 Le constructeur du véhicule doit évaluer les fonctions de sécurité au moyen de procédures de test ;

3.3.9 Le véhicule doit être conçu pour résister aux cyberattaques ;

3.3.10 Le véhicule doit être conçu de manière à pouvoir détecter les cyberattaques et à y réagir de manière appropriée.

IV. Menaces pour les véhicules

4.1 La liste des menaces dont il est question dans le présent document est à la disposition des parties intervenant dans le lancement, la conception ou la modification de produits ou de services intégrés aux véhicules ou interagissant avec ceux-ci. Cette liste, qui correspond à l'état des connaissances au moment de la rédaction du présent document, devra être réexaminer pour s'assurer de son exhaustivité lorsqu'elle sera utilisée.

Elle devrait servir de point de départ pour s'assurer que les risques sont suffisamment atténués. Elle peut être utilisée pour faciliter l'inventaire des vulnérabilités aux cybermenaces potentielles et veiller à ce que des mesures appropriées soient en place pour atténuer ces risques.

4.2 La présente section fournit des détails sur les menaces et les vulnérabilités potentielles. Une liste plus détaillée d'exemples de menaces potentielles pouvant être utilisés est reproduite à l'annexe B.

4.3 On trouvera ci-après une description détaillée des menaces et des vulnérabilités potentielles devant être prises en compte lors de la conception d'un produit ou service nouveau ou modifié. Les références numériques correspondent à celles utilisées à l'annexe B :

4.3.1 Menaces concernant les serveurs dorsaux :

a) Serveurs dorsaux utilisés pour attaquer un véhicule ou extraire des données (1.) ;

b) Services d'un serveur dorsal perturbé, affectant le fonctionnement d'un véhicule (2.) ;

c) Données stockées sur des serveurs dorsaux perdues ou compromises (« atteinte à la sécurité des données ») (3.).

4.3.2 Menaces pour les véhicules liées à leurs voies de communication :

a) Simulation de messages ou de données reçus par le véhicule (4.) ;

b) Voies de communication utilisées pour effectuer des manipulations, suppressions ou autres modifications non autorisées du code ou des données du véhicule (5.) ;

c) Voies de communication permettant l'acceptation de messages non fiables, ou vulnérables au piratage ou aux attaques par rejeu (6.) ;

d) Les informations peuvent être facilement divulguées. Par exemple, en interceptant les communications ou en permettant l'accès non autorisé à des fichiers ou dossiers sensibles (7.) ;

e) Attaques par déni de service sur les voies de communication pour perturber les fonctions du véhicule (8.) ;

f) Un utilisateur sans privilèges peut obtenir un accès privilégié aux systèmes du véhicule (9.) ;

g) Des virus introduits dans les moyens de communication peuvent infecter les systèmes du véhicule (10.) ;

h) Des messages reçus par le véhicule (par exemple messages X2V ou de diagnostic.), ou transmis à l'intérieur de celui-ci, contiennent des contenus malveillants (11).

4.3.3 Menaces pour les véhicules liées à leurs procédures de mise à jour :

a) Utilisation abusive ou compromission des procédures de mise à jour (12.) ;

b) Possibilité d'empêcher des mises à jour légitimes (13.).

4.3.4 Menaces pour les véhicules liées à des actions humaines non intentionnelles :

a) Mauvaise configuration de l'équipement ou des systèmes par un acteur légitime, par exemple le propriétaire ou la communauté de maintenance (14.) ;

b) Des acteurs légitimes peuvent prendre des mesures susceptibles de faciliter involontairement une cyberattaque (15.).

4.3.5 Menaces pour les véhicules liées à leur connectivité et leurs connexions externes :

a) La manipulation de la connectivité des fonctions du véhicule permet une cyberattaque, les moyens utilisés comprenant : la télématique, les systèmes permettant des opérations à distance et les systèmes utilisant des communications sans fil à courte portée (16.) ;

b) Utilisation de logiciels tiers embarqués, comme les applications de divertissement, pour attaquer les systèmes du véhicule (17.) ;

c) Utilisation de dispositifs connectés à des interfaces externes, par exemple des ports USB ou le port OBD, pour attaquer les systèmes du véhicule (18.).

4.3.6 Cibles ou motivations potentielles d'une attaque :

a) Extraction des données ou du code du véhicule (19.) ;

b) Manipulation des données ou du code du véhicule (20.) ;

c) Effacement des données ou du code (21.) ;

d) Introduction de logiciels malveillants (22.) ;

e) Introduction de nouveaux logiciels ou écrasement de logiciels existants (23.) ;

f) Perturbation des systèmes ou des opérations (24.) ;

g) Manipulation des paramètres du véhicule (25.).

4.3.7 Vulnérabilités potentielles susceptibles d'être exploitées si elles ne sont pas suffisamment protégées ou réduites :

a) Les technologies cryptographiques peuvent être compromises ou ne sont pas suffisamment appliquées (26.) ;

b) Des pièces ou des fournitures pourraient être compromises pour permettre l'attaque des véhicules (27.) ;

c) La conception des logiciels ou du matériel est source de vulnérabilités (28.) ;

d) La conception des réseaux est source de vulnérabilités (29.) ;

e) La perte physique de données est possible (30.) ;

f) Le transfert involontaire de données est possible (31.) ;

g) La manipulation physique des systèmes peut permettre une attaque (32.).

4.3.8 L'analyse des menaces doit également inclure un examen des éventuelles conséquences d'une attaque. Cet examen peut permettre de déterminer le niveau de risque et de déceler d'autres risques. Une attaque peut :

a) Compromettre la sécurité d'utilisation du véhicule ;

b) Interrompre certaines fonctions du véhicule ;

c) Modifier des logiciels avec altération des performances ;

d) Modifier des logiciels sans effet sur le fonctionnement ;

e) Compromettre l'intégrité des données ;

f) Compromettre la confidentialité des données ;

g) Interdire l'accès aux données ;

h) Avoir d'autres conséquences, par exemple d'ordre criminel.

4.4 Des exemples plus détaillés de vulnérabilités ou de méthodes d'attaque sont donnés pour chaque élément du tableau 1 de l'annexe B. Ils peuvent être utilisés pour mieux comprendre les informations ci-dessus. Il est probable que des exemples nouveaux et imprévus de vulnérabilités et de méthodes d'attaque apparaissent avec le temps. Il s'ensuit que ni la liste ci-dessus ni les exemples cités ne doivent être considérés comme exhaustifs.

V. Mesures d'atténuation

5.1 La présente section dresse une liste des mesures devant être prises en compte lors de la conception d'un produit ou d'un service nouveau ou modifié afin d'atténuer les menaces et les risques recensés. Les éléments de cette liste utilisant le mode indicatif (« doit/doivent ») sont obligatoires tandis que ceux utilisant le mode conditionnel (« devrait/devraient ») doivent être pris en compte s'il y a lieu.

5.1.1 Des contrôles de sécurité doivent être réalisés sur les systèmes dorsaux afin de réduire au minimum le risque d'attaques d'initié.

5.1.2 Des contrôles de sécurité doivent être réalisés sur les systèmes dorsaux afin de réduire au minimum les accès non autorisés.

5.1.3 Lorsque les serveurs dorsaux sont essentiels à la prestation des services, des mesures de rétablissement doivent être disponibles en cas de panne du système.

5.1.4 Des contrôles de sécurité doivent être réalisés pour réduire au minimum les risques associés à l'informatique en nuage.

5.1.5 Des contrôles de sécurité doivent être réalisés sur les systèmes dorsaux pour éviter les atteintes à la sécurité des données.

5.1.6 Le principe d'intégration de la sécurité dès la conception doit être adopté pour réduire au minimum l'impact d'une attaque sur le véhicule .

5.1.7 Des techniques et des conceptions de contrôle de l'accès doivent être utilisées pour protéger les données ou le code du système.

5.1.8 La conception du système et le contrôle de l'accès devraient empêcher que des personnes non autorisées puissent accéder à des données personnelles ou des données critiques du système.

5.1.9 Des mesures doivent être prises pour empêcher et détecter les accès non autorisés.

5.1.10 Le véhicule doit vérifier l'authenticité et l'intégrité des messages qu'il reçoit.

5.1.11 Des contrôles de sécurité doivent être mis en œuvre pour le stockage des clefs cryptographiques.

5.1.12 Les données confidentielles reçues et transmises par le véhicule doivent être protégées.

5.1.13 Des mesures visant à détecter une attaque par déni de service et à s'en remettre devraient être envisagées.

5.1.14 Des mesures de protection des systèmes contre les virus/logiciels malveillants intégrés devraient être envisagées.

5.1.15 Des mesures de détection des messages ou activités internes malveillant(e)s devraient être envisagées.

5.1.16 Des procédures sécurisées de mise à jour logicielle doivent être utilisées.

5.1.17 Des mesures doivent être mises en œuvre pour définir et contrôler les procédures de maintenance.

5.1.18 Des mesures doivent être mises en œuvre pour définir et contrôler les rôles des utilisateurs et les privilèges d'accès, en se fondant sur le principe du moindre privilège.

5.1.19 Les organisations doivent s'assurer que les procédures de sécurité sont définies et suivies.

5.1.20 Des contrôles de sécurité doivent être réalisés sur les systèmes qui ont un accès à distance.

5.1.21 Les logiciels doivent faire l'objet d'une évaluation de sécurité, être authentifiés et leur intégrité doit être protégée.

5.1.22 Des contrôles de sécurité doivent être réalisés sur les interfaces externes.

5.1.23 Les meilleures pratiques de cybersécurité doivent être suivies lors du développement des logiciels et du matériel.

5.1.24 Les meilleures pratiques de protection des données doivent être suivies pour le stockage des données privées et sensibles.

5.1.25 Les systèmes devraient être conçus de manière à réagir de façon appropriée en cas de détection d'une attaque contre un véhicule.

5.2 Les annexes B et C donnent des exemples de mesures d'atténuation susceptibles d'être utilisées. Elles ne sont pas exhaustives et ne sont pas nécessairement applicables à la mise en œuvre spécifique d'un produit ou d'un service donné.

5.3 Pour faciliter la détermination de mesures d'atténuation spécifiques, chaque exemple de menace peut être évalué en appliquant l'« approche CIA étendue ». Cette évaluation devrait examiner comment une attaque liée à une menace ou à une vulnérabilité pourrait être déclenchée et propagée sur les réseaux d'un véhicule. L'approche CIA étendue définit sept objectifs :

a) Confidentialité ;

b) Intégrité ;

c) Disponibilité ;

d) Non-répudiation ;

e) Authenticité ;

f) Responsabilité ;

g) Autorisation.

VI. Prescriptions relatives aux processus de cybersécurité et comment démontrer leur application

6.1 La présente section décrit les moyens devant être mis en œuvre par un constructeur de véhicules pour prouver à une autorité qu'il a tenu compte des menaces, des mesures d'atténuation et des principes applicables à ses produits pour que cette autorité puisse certifier leur conformité.

6.2 Cette section ne précise pas les moyens mis en œuvre par le constructeur du véhicule pour recueillir les informations nécessaires. Ces moyens peuvent être internes à l'organisation ou nécessiter des échanges entre les différents maillons d'une chaîne d'approvisionnement (par exemple le constructeur et le fournisseur).

6.3 Certification du système de gestion de la cybersécurité

6.3.1 Un système de gestion de la cybersécurité doit être mis en œuvre par le constructeur du véhicule.

6.3.2 Les fournisseurs et les prestataires de services doivent mettre en œuvre un système de gestion de la cybersécurité.

6.3.3 Les fournisseurs et les prestataires de services doivent être en mesure de fournir au constructeur du véhicule des preuves de la mise en œuvre de leur système de gestion de la cybersécurité.

6.3.4 Le constructeur du véhicule doit démontrer à une autorité que son système de gestion de la cybersécurité couvre les phases suivantes :

6.3.4.1 Phase de mise au point ;

6.3.4.2 Phase de production ;

6.3.4.3 Phase de postproduction.

6.3.5 Le constructeur du véhicule doit démontrer à une autorité comment son système de gestion de la cybersécurité gérera les dépendances pouvant exister avec ses fournisseurs et prestataires de services.

6.3.6 Le constructeur du véhicule doit définir, dans son système de gestion de la cybersécurité, des processus de surveillance des risques et des menaces pesant sur le véhicule ainsi que des processus d'intervention en cas d'incident.

6.4 Prescriptions relatives au véhicule après sa production :

6.4.1 La cybersécurité doit être intégrée dans le cycle de vie d'un véhicule ;

6.4.2 Le constructeur du véhicule doit démontrer comment il prévoit de maintenir une protection adéquate et le respect des principes de cybersécurité décrits dans le présent document tout au long du cycle de vie du véhicule. Cette capacité est nécessaire pour qu'il puisse démontrer que la sécurité et la disponibilité de son véhicule et des fonctions de son système seront assurées malgré l'évolution des cybermenaces. Cette question est particulièrement importante pour les systèmes critiques pour la sécurité, y compris les systèmes homologués ;

6.4.3 Les organisations du secteur automobile doivent être en mesure de déterminer comment les menaces pesant sur les véhicules ou les systèmes et leurs vulnérabilités évoluent au fil du temps et de déceler des menaces qui n'auraient pas été décelées ou prises en compte pendant la phase de mise au point ;

6.4.4 Les organisations du secteur automobile doivent être en mesure d'évaluer si les mesures de sécurité mises en œuvre sont toujours efficaces à la lumière des nouvelles cybermenaces ou vulnérabilités qu'elles ont repérées. Cette évaluation devrait déterminer si la sécurité ou la disponibilité du véhicule, ou de ses fonctions, sont affectées ;

6.4.5 Les organisations du secteur automobile doivent disposer de processus d'intervention en cas d'incident.

6.5 Homologation du type de véhicule :

6.5.1 L'homologation du type de véhicule ne doit avoir lieu que si le système de gestion de la cybersécurité du constructeur du véhicule est accompagné d'un certificat de conformité CSMS valide ;

6.5.2 Le constructeur du véhicule doit démontrer qu'une appréciation du risque a été effectuée pour le type de véhicule en ce qui concerne les systèmes du véhicule et leurs interactions et l'ensemble du véhicule ;

6.5.3 Le constructeur du véhicule doit s'assurer que les éléments critiques du véhicule sont conçus de sorte à offrir une protection contre les risques identifiés dans son appréciation du risque. Des mesures d'atténuation proportionnées doivent être mises en œuvre pour protéger ces éléments.

6.5.4 Le constructeur du véhicule doit prendre des mesures appropriées et proportionnées pour protéger les environnements prévus (le cas échéant) pour le stockage et l'exécution des logiciels, services, applications ou données du marché de l'après-vente ;

6.5.5 Les preuves requises pour l'homologation du véhicule doivent comprendre :

6.5.5.1 La manière dont le constructeur du véhicule a tenu compte des menaces et des vulnérabilités, y compris celles décrites à l'annexe A, dans son appréciation du risque ;

6.5.5.1 Les mesures d'atténuation mises en œuvre par le constructeur du véhicule pour minimiser les risques à un niveau acceptable, en décrivant :

a) L'architecture et les systèmes du véhicule ;

b) Les éléments importants de l'architecture et de ses (sous-)systèmes qui sont pertinents pour la cybersécurité ;

c) Les interactions de ces architectures et systèmes avec d'autres architectures, systèmes et interfaces externes du véhicule ;

d) Les risques posés aux architectures et systèmes qui ont été identifiés dans l'appréciation du risque ;

e) Les mesures d'atténuation qui ont été mises en œuvre sur les systèmes recensés et la façon dont elles gèrent les risques définis.

6.5.6 La manière dont le constructeur du véhicule a mis en œuvre les principes de cybersécurité définis dans le présent document peut également servir de preuve pour l'homologation de type.

VII. Conclusion et recommandation pour la suite de la procédure

7.1 La conclusion de cette recommandation est la suivante :

7.1.1 L'évaluation s'est appuyée sur les travaux, les connaissances et l'expérience des parties prenantes (voir annexe D) pour formuler une recommandation sur la cybersécurité. Le groupe spécial considère qu'il s'est acquitté de son mandat ;

7.1.2 La spécification de solutions techniques serait inappropriée, car elles ne résisteraient pas à l'épreuve du temps et décourageraient l'innovation et la concurrence. Aussi, la présente recommandation contient plutôt des exemples de processus, de procédures et de technologies qui pourraient être envisagés en matière de cybersécurité ;

7.1.3 La démonstration de la manière dont les prescriptions énoncées dans la présente recommandation peuvent être satisfaites ne devrait pas être explicitement définie. Il est plutôt recommandé que les constructeurs de véhicules utilisent les normes et processus pertinents et prennent des mesures d'atténuation appropriées pour démontrer à l'autorité compétente qu'ils respectent les prescriptions ;

7.1.4 Le champ d'application de la présente recommandation couvre le cycle de vie du véhicule, mais pas son retrait de la circulation ni son devenir ultérieur.

7.2 Les mesures suivantes sont nécessaires pour réglementer la cybersécurité :

7.2.1 La vérification par une autorité d'homologation que les processus et procédures d'un constructeur de véhicules (tels qu'ils sont décrits dans son système de gestion de la cybersécurité) appuient la mise en œuvre des recommandations du présent document ;

7.2.2 L'approbation, par une autorité d'homologation, que les risques identifiés pour un type de véhicule donné ont été correctement évalués et que les mesures d'atténuation prises pour faire face à ces risques sont appropriées.

7.3 Pour faciliter l'évaluation du système de gestion de la cybersécurité, de l'analyse du risque entreprise et des mesures d'atténuation mises en œuvre, la recommandation comprend :

7.3.1 Des principes de cybersécurité qui peuvent être utilisés pour illustrer comment les organisations doivent mettre en œuvre la cybersécurité pendant la durée de vie du véhicule ;

7.3.2 Des exemples de menaces, de risques, de vulnérabilités et de conséquences d'attaques qui devraient être pris en compte ;

7.3.3 Des exemples de mesures d'atténuation qui devraient être pris en compte.

7.4 Il est probable que des exemples nouveaux et imprévus de vulnérabilités et de méthodes d'attaque apparaissent avec le temps. Par conséquent, les exemples fournis ne doivent pas être considérés comme une liste exhaustive ou une liste applicable à chaque conception de véhicule, et devront plutôt être utilisés après avoir évalué leur exhaustivité et leur applicabilité.

7.5 Le groupe spécial recommande que le présent document soit divisé en deux parties :

7.5.1 Le corps du texte (sect. 1 à 6) et les annexes B et C feraient l'objet d'un document de travail officiel du WP.29. Il pourrait également servir de base à une résolution sur la cybersécurité, mais d'autres révisions pourraient être nécessaires pour le rendre conforme au format requis ;

7.5.2 L'annexe A deviendrait un Règlement ONU, conformément à l'Accord de 1958, pour donner suite aux recommandations formulées au paragraphe 7.2 ci-dessus. Elle contient des prescriptions qui portent sur :

7.5.2.1 Un certificat CSMS de conformité du système de gestion de la cybersécurité du constructeur du véhicule ;

7.5.2.2 L'homologation de type des véhicules en ce qui concerne la cybersécurité.

7.5.3 L'annexe C pourra être utile aux parties prenantes en tant que document de référence. Elle ne peut être incluse dans le Règlement ONU du fait de son caractère informatif.

7.5.4 L'annexe D ne peut être incluse dans un Règlement ou une Résolution et est uniquement fournie pour compléter le présent document.

7.5.5 Le groupe de tutelle devrait décider des étapes suivantes, par exemple l'élaboration d'un Règlement technique mondial (RTM) sur la cybersécurité. Le groupe spécial souligne que l'élaboration d'un RTM nécessitera des travaux supplémentaires.

7.5.6 Pour l'annexe au Règlement, les catégories L, O, R, S et T pourraient être incluses, mais elles ne sont que peu (dans le cas de la catégorie L) ou pas (dans les autres cas) représentées au sein du groupe spécial. Il convient donc de se demander si le Règlement devrait s'appliquer à ces catégories de véhicules.

7.5.7 Il est proposé dans l'annexe au Règlement que la durée de validité du certificat de conformité CSMS soit de trois ans et que les contrôles de conformité de la production soient également effectués tous les trois ans.

7.5.8 Le groupe spécial recommande que les dispositions du projet de Règlement (annexe A) soient vérifiées pour s'assurer qu'elles sont légalement autorisées par l'Accord de 1958. Il est notamment recommandé de vérifier si, contrairement à l'avis du groupe spécial, les paragraphes 7.2.2.1 et 7.2.2.2 de l'annexe A dépassent les limites de ce qui peut être autorisé par la législation sur l'homologation de type.

7.6 Les évolutions suivantes pourraient être examinées à l'avenir :

7.6.1 Les menaces pour la cybersécurité peuvent apparaître à tout moment de la vie d'un véhicule. Le groupe spécial définit les prescriptions au paragraphe 7, « Spécifications » de l'annexe A (et plus précisément au paragraphe 7.2, « Prescriptions relatives à l'organisation du constructeur du véhicule »). Ces prescriptions en matière de cybersécurité peuvent s'appliquer pendant toute la durée de vie d'un véhicule (conception, production et postproduction). Le groupe spécial reconnaît toutefois que l'homologation de type n'a pas besoin d'être valable une fois que la production a été définitivement arrêtée (conformément à l'Accord de 1958). Un cadre juridique visant à améliorer l'intégration des prescriptions dans la phase de postproduction, autre que celui déjà prévu par les exigences d'homologation de type, par exemple, devrait être examiné plus avant ;

7.6.2 L'analyse des menaces a identifié des risques qui ont été jugés sortir du cadre du présent document. Ces risques ne doivent toutefois pas être ignorés et il est donc recommandé de les renvoyer à l'organe compétent de l'ONU pour examen ;

7.6.3 Il convient de noter que le domaine de la cybersécurité est en pleine évolution. Il est recommandé que le présent document fasse l'objet d'examens périodiques, pour s'assurer qu'il tient compte des menaces et des mesures d'atténuation nouvelles et émergentes, et qu'il est actualisé le cas échéant. Ces examens devront être supervisés et pourront nécessiter la reconstitution du groupe spécial ;

7.6.4 Au moment de la rédaction de la présente recommandation, l'ISO et la SAE élaboraient une nouvelle norme commune intitulée ISO/SAE 21434 Véhicules routiers − Ingénierie de la cybersécurité. Lorsque ces travaux auront suffisamment progressé, le présent document devra être revu et actualisé si nécessaire ;

7.6.5 Il a été noté qu'un dialogue entre les autorités sera nécessaire à l'avenir pour assurer une approche cohérente en matière d'homologation et que le WP.1 de la CEE pourrait faciliter ce processus.

7.7 Recommandations pour la mise en œuvre

7.7.1 Le groupe spécial recommande que le projet de Règlement prévoie une phase d'essai avant sa mise en œuvre complète. L'objectif de cette phase serait de valider les procédures prévues tant pour les constructeurs de véhicules que pour les autorités d'homologation et de vérifier qu'elles fonctionnent comme prévu et permettent une nouvelle révision du Règlement, si nécessaire. Le GRVA devrait réfléchir à ce qui pourrait être approprié pour une telle phase d'essai ;

7.7.2 Le groupe spécial recommande qu'un délai soit accordé avant l'entrée en vigueur du Règlement pour permettre aux constructeurs de véhicules et aux autorités d'homologation d'adapter leurs procédures afin de se conformer au présent Règlement. Le GRVA devrait réfléchir à la durée de ce délai et envisager un calendrier d'introduction par étapes, tout en tenant compte de la nécessité d'agir dans ce domaine.

Annexe A — Projet de proposition d'établissement d'un Règlement sur la cybersécurité

Projet de Règlement sur la cybersécurité

Nations Unies ECE/TRANS/WP.29/201x/xx

Conseil économique et social

Distr. générale
JJ MM AAAA
Français
Original : anglais

Commission économique pour l'Europe

Comité des transports intérieurs

Forum mondial de l'harmonisation des Règlements concernant les véhicules

xxx[e] session
Genève, JJ-JJ MM AAAA
Point XXX de l'ordre du jour provisoire
Projet de nouveau Règlement ONU sur les mises à jour des logiciels

Projet de nouveau Règlement ONU énonçant des prescriptions uniformes concernant l'homologation de la cybersécurité

Communication de l'expert de xxx

Le texte reproduit ci-après a été établi par les experts de xxx.

I. Proposition

Projet de nouveau Règlement ONU énonçant des prescriptions uniformes concernant l'homologation de la cybersécurité

Table des matières

1. Champ d'application

1.1 Le présent Règlement s'applique aux véhicules des catégories [L], M, N, [O, R, S et T].

2. Définitions

Aux fins du présent Règlement, on entend par :

2.1 « *Type de véhicule* », l'ensemble des véhicules d'une catégorie donnée qui ne présentent pas entre eux de différences, au moins au regard des critères de base suivants :

a) Le constructeur ;

b) La désignation de type attribuée par le constructeur ;

c) Les aspects essentiels de la conception des véhicules en ce qui concerne la cybersécurité.

2.2 « *Cybersécurité* », la protection des véhicules routiers et de leurs fonctions contre les menaces planant sur les composants électriques ou électroniques.

2.3 « *Système de gestion de la cybersécurité (CSMS)* », une approche systématique fondée sur les risques définissant les processus, les responsabilités et les mesures de gouvernance de l'organisation ayant pour objet d'atténuer les cybermenaces et de protéger les véhicules des cyberattaques.

3. Demande d'homologation

3.1 La demande d'homologation d'un type de véhicule en ce qui concerne la cybersécurité doit être présentée par le constructeur du véhicule ou par son représentant dûment accrédité.

3.2 Elle doit être accompagnée des pièces mentionnées ci-après, en triple exemplaire, et des informations suivantes :

3.2.1 Une description du type de véhicule en ce qui concerne les points mentionnés à l'annexe 1 du présent Règlement ;

3.2.2 Dans les cas où il est indiqué que les informations font l'objet de droits de propriété intellectuelle, ou qu'elles constituent un savoir-faire spécifique du constructeur ou de ses fournisseurs, le constructeur ou les fournisseurs doivent fournir des éléments d'information suffisants pour permettre d'effectuer convenablement les vérifications mentionnées dans le présent Règlement. Ces éléments d'information doivent être utilisés de façon confidentielle ;

3.2.3 Le certificat de conformité CSMS, conformément aux dispositions du paragraphe 6 du présent Règlement.

4. Marque d'homologation

4.1 Sur tout véhicule conforme à un type de véhicule homologué en application du présent Règlement doit être apposée de manière visible, en un endroit facilement accessible et indiqué sur la fiche d'homologation, une marque d'homologation internationale composée :

4.1.1 D'un cercle à l'intérieur duquel figure la lettre « E » suivie du numéro distinctif du pays ayant délivré l'homologation ;

4.1.2 Du numéro du présent Règlement, suivi de la lettre « R », d'un tiret et du numéro d'homologation, à la droite du cercle prévu au paragraphe 4.1.1 ci-dessus.

4.2 Si le véhicule est conforme à un type de véhicule homologué en application d'un ou de plusieurs autres Règlements joints en annexe à l'Accord dans le pays même qui a accordé l'homologation en application du présent Règlement, il n'est pas nécessaire de répéter le symbole prescrit au paragraphe 4.1.1 ci-dessus ; dans un tel cas, les numéros de Règlement et d'homologation et les symboles additionnels pour tous les Règlements en application desquels l'homologation a été accordée dans le pays qui l'a accordée en application du présent Règlement doivent être mentionnés l'un au-dessous de l'autre à droite du symbole prescrit au paragraphe 4.1.1.

4.3 La marque d'homologation doit être nettement lisible et indélébile.

4.4 Elle doit être placée sur la plaque signalétique apposée par le constructeur, ou à proximité de celle-ci.

4.5 On trouvera à l'annexe 3 du présent Règlement des exemples de marques d'homologation.

5. Homologation

5.1 Les autorités d'homologation accordent, selon qu'il convient, l'homologation de type en ce qui concerne la cybersécurité, uniquement aux types de véhicules qui satisfont aux prescriptions du présent Règlement.

5.2 L'homologation ou l'extension ou le refus d'homologation d'un type de véhicule en application du présent Règlement est notifié aux Parties à l'Accord de 1958 appliquant ledit Règlement au moyen d'une fiche conforme au modèle reproduit dans l'annexe 2 du présent Règlement.

5.3 Les autorités d'homologation ne délivrent pas d'homologation de type sans s'assurer que le constructeur a mis en place des dispositions et des procédures satisfaisantes pour mettre en œuvre convenablement les aspects de la cybersécurité dont il est question dans le présent Règlement.

5.4 Aux fins du paragraphe 7.2. du présent Règlement, le constructeur veille à ce que les aspects de cybersécurité couverts par le présent Règlement soient appliqués.

6. Certificat de conformité du système de gestion de la cybersécurité

6.1 Les Parties contractantes désignent une autorité d'homologation ou un service technique chargés de procéder à l'évaluation préliminaire du constructeur et de délivrer le certificat de conformité CSMS.

6.2 Dans le cadre de l'évaluation préliminaire, l'autorité d'homologation ou le service technique s'assure que le constructeur a mis en place les processus requis pour se conformer à toutes les dispositions légales pertinentes en ce qui concerne la cybersécurité conformément au présent Règlement.

6.3 À l'issue de l'évaluation préliminaire, un certificat de conformité au sens de l'annexe 4 du présent Règlement (ci-après le certificat de conformité CSMS) est délivré au constructeur.

6.4 L'autorité d'homologation ou le service technique utilise le modèle figurant à l'annexe 4 du présent Règlement pour le certificat de conformité CSMS.

6.5 Le certificat de conformité CSMS a une durée de validité de trois ans à compter de la date de sa délivrance.

6.6 L'autorité d'homologation qui a délivré le certificat de conformité CSMS peut à tout moment vérifier sa validité. Le certificat de conformité CSMS peut être retiré si les prescriptions énoncées dans le présent Règlement ne sont plus respectées.

6.7 Le constructeur informe l'autorité d'homologation ou le service technique de toute modification importante susceptible d'avoir une incidence sur la validité du certificat de conformité CSMS. Après avoir consulté le constructeur, l'autorité d'homologation ou le service technique détermine s'il convient de procéder à de nouvelles vérifications.

6.8 À la fin de la période de validité du certificat de conformité CSMS, l'autorité d'homologation délivre un nouveau certificat de conformité CSMS ou prolonge la validité du certificat périmé pour une nouvelle période de trois ans, selon le cas. L'autorité d'homologation délivre un nouveau certificat lorsque des modifications importantes ont été portées à son attention ou à celle du service technique.

6.9 Les homologations de type en vigueur pour les véhicules ne perdent pas leur validité du fait de l'expiration du certificat de conformité CSMS accordé au constructeur.

7. Spécifications

7.1 Spécifications générales

7.1.1 Les prescriptions du présent Règlement ne doivent pas limiter les dispositions ou prescriptions d'autres Règlements ONU.

7.1.2 Le constructeur du véhicule peut se référer à [la Recommandation/ Résolution sur la cybersécurité] dans son appréciation des risques de cybersécurité et des mesures d'atténuation, ainsi que dans sa description des processus employés.

7.2 Prescriptions relatives au système de gestion de la cybersécurité

7.2.1 Aux fins de l'évaluation préliminaire, l'autorité d'homologation ou le service technique doit vérifier que le constructeur du véhicule dispose d'un système de gestion de la cybersécurité et qu'il se conforme au présent Règlement.

7.2.2 Le système de gestion de la cybersécurité doit couvrir les aspects suivants :

7.2.2.1 Le constructeur du véhicule doit démontrer à une autorité d'homologation ou à un service technique que son système de gestion de la cybersécurité comporte les phases suivantes :

- Phase de développement ;
- Phase de production ;
- Phase de postproduction.

7.2.2.2 Le constructeur du véhicule doit démontrer que les procédures mises en œuvre dans le cadre de son système de gestion de la cybersécurité garantissent que la sécurité est dûment prise en compte. Celles-ci comprennent :

a) Les processus mis en œuvre en interne par le constructeur pour gérer la cybersécurité ;

b) Les processus mis en œuvre pour répertorier les risques auxquels chaque type de véhicules est exposé ;

c) Les processus utilisés pour l'appréciation, la catégorisation et la gestion des risques décelés ;

d) Les processus en place pour vérifier que les risques décelés sont correctement gérés ;

e) Les processus utilisés pour contrôler la sécurité du système tout au long de ses phases de développement et de production ;

f) Les processus mis en œuvre pour s'assurer que l'appréciation du risque est actualisée ;

g) Les processus utilisés pour surveiller et détecter les cyberattaques sur les types de véhicules et y répondre ;

h) Les processus utilisés pour déceler les cybermenaces et les vulnérabilités nouvelles et évolutives pour les types de véhicules ;

i) Les processus utilisés pour réagir de manière appropriée aux cybermenaces et aux vulnérabilités nouvelles et évolutives.

7.2.2.3 Le constructeur du véhicule peut se référer à [la Recommandation/ Résolution sur la cybersécurité] pour décrire les procédés qu'il a employés.

7.2.2.4 Le constructeur du véhicule est tenu de montrer comment son système de gestion de la cybersécurité gérera les dépendances pouvant exister avec ses fournisseurs et prestataires de services en ce qui concerne les prescriptions du paragraphe 7.2.2.2.

7.3 Prescriptions relatives aux types de véhicules

7.3.1 Avant de procéder à l'évaluation d'un type de véhicule aux fins de l'homologation de type, le constructeur du véhicule doit démontrer à l'autorité d'homologation ou au service technique que son système de gestion de la cybersécurité possède un certificat de conformité CSMS valide correspondant au type de véhicule à homologuer.

7.3.2 L'autorité d'homologation ou le service technique doit vérifier que le constructeur a pris les mesures nécessaires concernant le type de véhicule pour :

a) Recueillir et vérifier, le cas échéant, les informations requises en vertu du présent Règlement, tout au long de la chaîne d'approvisionnement ;

b) Tenir à jour des informations appropriées sur la conception et les essais ;

c) Mettre en œuvre des mesures de sécurité appropriées lors de la conception du véhicule et de ses systèmes.

7.3.3 Le constructeur du véhicule doit démontrer qu'une appréciation du risque a été effectuée pour le type de véhicule en ce qui concerne les systèmes du véhicule et leurs interactions et l'ensemble du véhicule.

7.3.4 Le constructeur du véhicule doit démontrer comment les éléments critiques du véhicule sont conçus de sorte à offrir une protection contre les risques signalés dans son appréciation du risque. Des mesures d'atténuation proportionnées doivent être mises en œuvre pour protéger ces éléments.

7.3.5 Le constructeur du véhicule doit démontrer qu'il a pris des mesures appropriées et proportionnées pour protéger les environnements du type du véhicule prévus (le cas échéant) pour le stockage et l'exécution des logiciels, services, applications ou données du marché de l'après-vente.

7.3.6 Le constructeur du véhicule doit décrire les essais qui ont été effectués pour vérifier l'efficacité des mesures de sécurité mises en œuvre et les résultats de ces essais.

8. Modification du type de véhicule et extension de l'homologation de type

8.1 Toute modification du type de véhicule doit être notifiée à l'autorité qui a accordé l'homologation de type. Cette dernière peut alors :

8.1.1 Soit considérer que les modifications apportées ne prêtent guère à conséquence et qu'en tout état de cause le véhicule demeure conforme aux prescriptions ;

8.1.2 Soit demander au service technique chargé des essais d'établir un nouveau procès-verbal d'essai.

8.1.3 La confirmation, l'extension ou le refus de l'homologation, faisant mention des modifications apportées, doit être notifié au moyen d'une fiche de communication conforme au modèle présenté dans l'annexe 2 du présent Règlement. L'autorité d'homologation qui délivre une extension d'homologation attribue un numéro de série à ladite extension et en informe les autres Parties à l'Accord de 1958 appliquant le présent Règlement au moyen d'une fiche de communication conforme au modèle de l'annexe 2 dudit Règlement.

9. Conformité de la production

9.1 Les procédures relatives à la conformité de la production doivent satisfaire aux prescriptions énoncées à l'annexe 1 de l'Accord de 1958 (E/ECE/TRANS/505/Rev.3), comme suit :

9.1.1 Le détenteur de l'homologation doit veiller à ce que les résultats des essais de contrôle de la conformité de la production soient enregistrés et que les documents annexés restent disponibles pour une période fixée en accord avec l'autorité d'homologation ou le service technique. Cette période ne doit pas excéder dix ans à partir de la date à laquelle il est définitivement mis fin à la production ;

9.1.2 L'autorité qui a accordé l'homologation de type peut à tout moment vérifier les méthodes de contrôle de conformité appliquées dans chaque unité de production. La fréquence normale de ces vérifications est d'une fois tous les trois ans.

10. Sanctions pour non-conformité de la production

10.1 L'homologation délivrée pour un type de véhicule en application du présent Règlement peut être retirée si les prescriptions énoncées dans ledit Règlement ne sont pas respectées ou si les véhicules prélevés ne satisfont pas auxdites prescriptions.

10.2 Dans le cas où une Partie contractante retire une homologation qu'elle avait accordée, elle en avise immédiatement les autres Parties contractantes appliquant le présent Règlement en envoyant une fiche de communication conforme au modèle de l'annexe 2 dudit Règlement.

11. Noms et adresses des services techniques chargés des essais d'homologation et des autorités d'homologation de type

11.1 Les Parties contractantes à l'Accord appliquant le présent Règlement doivent communiquer au Secrétariat de l'Organisation des Nations Unies les noms et adresses des services techniques chargés des essais d'homologation, ainsi que des autorités d'homologation de type qui délivrent des homologations et auxquelles doivent être envoyées les fiches d'homologation ou d'extension, de refus ou de retrait d'homologation émises dans les autres pays.

Annexe 1

Fiche de renseignements

Les renseignements ci-dessous doivent, s'il y a lieu, être fournis en triple exemplaire et être accompagnés d'une table des matières. Les schémas, s'il y en a, doivent être fournis à l'échelle appropriée, au format A4 ou pliés à ce format, et être suffisamment détaillés. Les photographies, s'il y en a, doivent être suffisamment détaillées.

0. Généralités

0.1 Marque (raison sociale du constructeur) :

0.2 Type :

0.2.0.1 Châssis :

0.2.1 Dénomination(s) commerciale(s) (le cas échéant) :

0.3 Moyen d'identification du type, s'il est marqué sur le véhicule (b) :

0.3.1 Emplacement de cette marque :

0.4 Catégorie du véhicule (c) :

0.8 Nom(s) et adresse(s) de l'usine ou des usines de montage :

0.9 Nom et adresse du représentant du constructeur (le cas échéant) :

12. DIVERS

12.8 Cybersécurité

12.8.1 Caractéristiques générales de conception du type de véhicule

12.8.1.1 Représentation schématique du type de véhicule :

12.8.1.2 Documents relatifs au type de véhicule à homologuer, décrivant :

a) Les résultats de l'appréciation du risque pour le type de véhicule ;

b) Les systèmes du véhicule (homologués ou non) qui sont pertinents pour la cybersécurité du type de véhicule ;

c) Les composants de ces systèmes qui sont pertinents pour la cybersécurité ;

d) Les interactions de ces systèmes avec d'autres systèmes du type de véhicule et les interfaces externes ;

e) Les risques auxquels sont exposés les systèmes qui ont été signalés lors de l'évaluation des risques pour ce type de véhicule ;

f) Les mesures d'atténuation qui ont été mises en œuvre sur les systèmes recensés ou sur le type de véhicule, et la façon dont elles gèrent les risques définis ;

g) Les essais qui ont été effectués pour vérifier la cybersécurité du type de véhicule et de ses systèmes et les résultats de ces essais.

12.8.2 Numéro du certificat de conformité CSMS

Annexe 2

Fiche de communication

Communication
(format maximal : A4 (210 x 297 mm))

Émanant de: Nom de l'administration:
.....
.....
.....

concernant[2]: Délivrance d'une homologation
Extension d'homologation
Refus d'homologation
Retrait d'homologation
Arrêt définitif de la production

d'un type de véhicule en ce qui concerne l'équipement xxx, en application du Règlement nº **X**.

Nº d'homologation .....

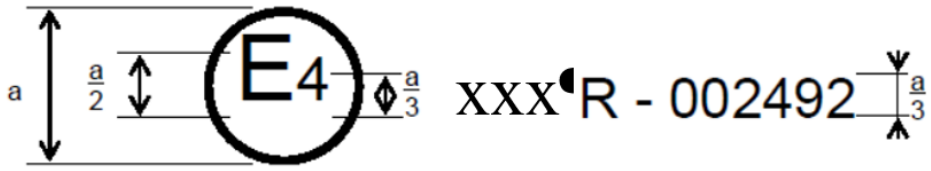
…

x.y .....

Annexe 3

Exemple de marque d'homologation

Modèle A
(voir le paragraphe 4.2 du présent Règlement)



a = 8 mm min.

La marque d'homologation ci-dessus, apposée sur un véhicule, indique que le type de véhicule routier visé a été homologué aux Pays-Bas (E 4), en application du Règlement n° xxx, sous le numéro d'homologation 002492. Les deux premiers chiffres du numéro d'homologation indiquent que l'homologation a été délivrée conformément aux dispositions du Règlement n° xx.

Annexe 4

Modèle de certificat de conformité du système de gestion de la cybersécurité (CSMS)

Certificat de conformité du système de gestion de la cybersécurité
avec le Règlement nº [Règlement sur la cybersécurité] xxx
Numéro [Numéro de référence]
[……. Autorité d'homologation]

Certifie que

Constructeur : .....

Adresse du constructeur : .....

Se conforme aux dispositions du paragraphe 7 du Règlement nº xxx

Des contrôles ont été effectués le :

par (nom et adresse de l'autorité d'homologation de type ou du service technique) :

Numéro du procès-verbal :

Le présent certificat est valable jusqu'au [… date]

Fait à [… lieu]

Le [… date]

[… Signature]

Annexe B

Liste des menaces et des mesures d'atténuation correspondantes

1. Les exemples donnés dans la présente annexe ne doivent pas être considérés comme obligatoires dans le cadre de l'évaluation d'un système. Cette annexe a un caractère informatif. Les exemples de menaces et de mesures d'atténuation possibles qu'elle contient ne doivent pas être considérés comme exhaustifs ou appropriés pour tous les systèmes ou conceptions du véhicule.

2. La présente annexe se divise en deux parties. La partie A décrit des exemples de vulnérabilités ou de méthodes d'attaque. La partie B décrit des exemples d'atténuation des menaces.

3. Ces exemples devraient être pris en considération par les constructeurs de véhicules et les fournisseurs lors de la conception, du développement, des essais et de la mise en œuvre des véhicules et de leurs systèmes, le cas échéant. Les exemples de vulnérabilités ou de méthodes d'attaque de la partie A visent à aider les constructeurs de véhicules, les fournisseurs et les autorités compétentes à comprendre les menaces, par exemple les points d'attaque ou les failles de sécurité. Les exemples de mesures d'atténuation présentés dans la partie B visent à aider les constructeurs de véhicules, les fournisseurs et les autorités compétentes à examiner les mesures d'atténuation disponibles pour réduire les risques liés aux menaces décelées, par exemple les normes industrielles applicables. Les contrôles de sécurité détaillés correspondant aux mesures d'atténuation sont décrits à l'annexe C de la présente recommandation.

4. La vulnérabilité de haut niveau et les exemples correspondants ont été indexés dans la partie A. La même indexation a été référencée dans les tableaux de la partie B pour établir un lien entre chaque attaque ou vulnérabilité et les mesures d'atténuation correspondantes.

5. L'analyse des menaces doit également inclure un examen des éventuelles conséquences d'une attaque. Cet examen peut permettre de déterminer le degré de risque et de déceler d'autres risques. Une attaque peut :

   - Compromettre la sécurité d'utilisation du véhicule ;
   - Interrompre certaines fonctions du véhicule ;
   - Modifier des logiciels avec altération des performances ;
   - Modifier des logiciels sans effet sur le fonctionnement ;
   - Compromettre l'intégrité des données ;
   - Compromettre la confidentialité des données ;
   - Interdire l'accès aux données ;
   - Avoir d'autres conséquences, par exemple d'ordre criminel.

6. De nouvelles menaces ou mesures d'atténuation devront être envisagées pour suivre les progrès de la technologie. La présente annexe pourrait également être actualisée à intervalles réguliers, pour s'assurer que son contenu reflète l'état de la technique.

Partie A
Exemples de vulnérabilités ou de méthodes d'attaque liées aux menaces

1. Des descriptions de haut niveau des menaces et des vulnérabilités ou des méthodes d'attaque correspondantes sont présentées dans le tableau 1.

Tableau 1
Liste d'exemples de vulnérabilités ou de méthodes d'attaque liées aux menaces

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			*Exemple de vulnérabilité ou de méthode d'attaque*	
4.3.1 Menaces concernant les serveurs dorsaux	1	Serveurs dorsaux utilisés pour attaquer un véhicule ou extraire des données	1.1	Abus de privilèges de la part du personnel (**attaque d'initié**)
			1.2	**Accès Internet non autorisé** au serveur (activé par exemple par des portes dérobées, des vulnérabilités logicielles système non corrigées, des attaques SQL ou d'autres moyens)
			1.3	**Accès physique non autorisé** au serveur (en utilisant, par exemple, des clefs USB ou d'autres supports connectés au serveur)
	2	Services d'un serveur dorsal perturbé, affectant le fonctionnement d'un véhicule	2.1	**Attaque d'un serveur dorsal bloquant son fonctionnement**, par exemple en l'empêchant d'interagir avec les véhicules et de fournir les services dont ils ont besoin
	3	Données stockées sur des serveurs dorsaux perdues ou compromises (« atteinte à la sécurité des données »)	3.1	Abus de privilèges de la part du personnel (**attaque d'initié**)
			3.2	**Perte d'informations dans le « nuage »**. Des données sensibles peuvent être perdues en raison d'attaques ou d'accidents lorsque les données sont stockées par des prestataires de services tiers de stockage dans le nuage
			3.3	**Accès Internet non autorisé** au serveur (activé par exemple par des portes dérobées, des vulnérabilités logicielles système non corrigées, des attaques SQL ou d'autres moyens)
			3.4	**Accès physique non autorisé** au serveur (en utilisant, par exemple, des clefs USB ou d'autres supports connectés au serveur)
			3.5	**Atteinte à la sécurité de l'information** due au partage involontaire de données (par exemple, erreurs administratives, stockage des données sur des serveurs situés dans des garages)
4.3.2 Menaces pour les véhicules liées à leurs voies de communication	4	Simulation de messages ou de données reçus par le véhicule	4.1	**Simulation de messages** par usurpation d'identité (802.11p V2X en cas de circulation en peloton, messages GNSS, etc)
			4.2	**Attaque Sybil** (visant à simuler d'autres véhicules pour faire croire qu'il y en a beaucoup sur la route)

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			*Exemple de vulnérabilité ou de méthode d'attaque*	
	5	Voies de communication utilisées pour effectuer des manipulations, suppressions ou autres modifications non autorisées du code ou des données du véhicule	5.1	Les voies de communication permettent l'**injection de code**, par exemple un code binaire altéré peut être injecté dans le flux de communication
			5.2	Les voies de communication permettent de **manipuler** les données ou le code du véhicule
			5.3	Les voies de communication permettent d'**écraser** les données ou le code du véhicule
			5.4	Les voies de communication permettent d'**effacer** les données ou le code du véhicule
			5.5	Les voies de communication permettent l'introduction de données ou de code dans le véhicule (écriture de données ou de code)
	6	Voies de communication permettant l'acceptation de messages non fiables, ou vulnérables au piratage ou aux attaques par rejeu	6.1	Acceptation d'informations provenant d'une **source non fiable**
			6.2	**Attaque de l'homme du milieu**/détournement de session
			6.3	**Attaque par rejeu**, par exemple une attaque contre une passerelle de communication permettant à l'attaquant d'installer une version antérieure du logiciel d'une unité de commande électronique (UCE) ou du microprogramme de la passerelle
	7	Les informations peuvent être facilement divulguées. Par exemple, en interceptant les communications ou en permettant l'accès non autorisé à des fichiers ou dossiers sensibles	7.1	**Interception de l'information**/rayonnements brouilleurs/surveillance des communications
			7.2	Obtention d'un **accès non autorisé** à des fichiers ou des données
	8	Attaques par déni de service sur les voies de communication pour perturber les fonctions du véhicule	8.1	**Envoi** d'un grand nombre de **données** parasites au système d'information du véhicule, **de sorte qu'il soit incapable de fournir des services** de manière normale
			8.2	**Attaque par trou noir**, visant à perturber la communication entre les véhicules en bloquant les messages entre ceux-ci
	9	Un utilisateur sans privilèges peut obtenir un accès privilégié aux systèmes du véhicule	9.1	Un utilisateur sans privilèges peut **obtenir un accès privilégié**, par exemple un accès racine
	10	Des virus introduits dans les moyens de communication peuvent infecter les systèmes du véhicule	10.1	Un **virus** introduit dans les moyens de communication infecte les systèmes du véhicule

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			*Exemple de vulnérabilité ou de méthode d'attaque*	
	11	Des messages reçus par le véhicule (par exemple, messages X2V ou de diagnostic), ou transmis à l'intérieur de celui-ci, contiennent des contenus malveillants	11.1	**Messages internes** malveillants (par exemple, bus CAN)
			11.2	**Messages V2X** malveillants, par exemple, messages d'infrastructure à véhicule ou de véhicule à véhicule (CAM, DENM, etc.)
			11.3	Messages de diagnostic malveillants
			11.4	**Messages propriétaires** malveillants (par exemple, ceux normalement envoyés par les fabricants d'équipement d'origine OEM ou les fournisseurs de composants/systèmes/fonctions)
4.3.3. Menaces pour les véhicules liées à leurs procédures de mise à jour	12	Utilisation abusive ou compromission des procédures de mise à jour	12.1	Compromission des **procédures de mise à jour logicielle sans fil**, y compris la fabrication du programme ou du microprogramme de mise à jour du système
			12.2	Compromission des **procédures de mise à jour logicielle locales/physiques**, y compris la fabrication du programme ou du microprogramme de mise à jour du système
			12.3	Le **logiciel** est **manipulé avant le processus de mise à jour** (et est donc corrompu), bien que le processus de mise à jour soit intact
			12.4	**Compromission** des clefs cryptographiques du fournisseur du logiciel **pour permettre une mise à jour non valide**
	13	Possibilité d'empêcher des mises à jour légitimes	13.1	Attaque par déni de service contre le serveur ou le réseau de mise à jour pour **empêcher le déploiement de mises à jour logicielles critiques** et/ou le déverrouillage de fonctionnalités spécifiques au client
4.3.4 Menaces pour les véhicules liées à des actions humaines non intentionnelles	14	Mauvaise configuration de l'équipement ou des systèmes par un acteur légitime, par exemple le propriétaire ou la communauté de maintenance	14.1	**Mauvaise configuration de l'équipement** par la communauté de maintenance ou le propriétaire lors de l'installation, la réparation ou l'utilisation, avec des conséquences imprévues
			14.2	**Utilisation** ou administration **erronée** de dispositifs et de systèmes (y compris les mises à jour sans fil)
	15	Des acteurs légitimes peuvent prendre des mesures susceptibles de faciliter involontairement une cyberattaque	15.1	Victime innocente (par exemple, propriétaire, opérateur ou ingénieur de maintenance) **amenée par la ruse** et à son insu à charger un logiciel malveillant ou à permettre une attaque
			15.2	Les **procédures de sécurité définies** ne sont pas suivies

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			*Exemple de vulnérabilité ou de méthode d'attaque*	
4.3.5 Menaces pour les véhicules liées à leur connectivité et leurs connexions externes	16	La manipulation de la connectivité des fonctions du véhicule permet une cyberattaque, les moyens utilisés comprenant : la télématique, les systèmes permettant des opérations à distance et les systèmes utilisant des communications sans fil à courte portée	16.1	Manipulation des **fonctions conçues pour commander à distance des systèmes**, tels qu'une clef à distance, un dispositif d'immobilisation et une pile de chargement
			16.2	**Manipulation de la télématique du véhicule** (par exemple, manipulation de la mesure de la température de biens sensibles, déverrouillage à distance des portes de chargement)
			16.3	Interférence avec des **systèmes** ou capteurs **sans fil à courte portée**
	17	Utilisation de logiciels tiers embarqués, comme les applications de divertissement, pour attaquer les systèmes du véhicule	17.1	Utilisation d'**applications corrompues**, ou dont la sécurité logicielle est déficiente, pour attaquer des systèmes du véhicule
	18	Utilisation de dispositifs connectés à des interfaces externes, par exemple des ports USB ou le port OBD, pour attaquer les systèmes du véhicule	18.1	**Interfaces externes** telles que les ports USB ou autres utilisées comme point d'attaque, par exemple par injection de code
			18.2	Support infecté par un **virus** connecté à un système du véhicule
			18.3	**Accès diagnostique (par exemple, dongles dans le port OBD)** utilisé pour faciliter une attaque, comme la manipulation (directe ou indirecte) des paramètres du véhicule
4.3.6 Cibles ou motivations potentielles d'une attaque	19	Extraction des données ou du code du véhicule	19.1	Extraction de logiciels soumis à des droits d'auteur ou exclusifs des systèmes du véhicule (**piratage** de produits)
			19.2	Accès non autorisé aux **données personnelles du propriétaire**, notamment concernant son identité, son compte de paiement, son carnet d'adresses, sa localisation, l'identifiant électronique du véhicule, etc.
			19.3	Extraction de clefs cryptographiques
	20	Manipulation des données ou du code du véhicule	20.1	Modifications illicites/non autorisées de l'**identifiant électronique du véhicule**
			20.2	**Usurpation d'identité**. Par exemple, si un utilisateur souhaite afficher une autre identité lorsqu'il communique avec les systèmes de péage, le système dorsal du constructeur
			20.3	Mesure visant à **contourner les systèmes de surveillance** (par exemple, piratage/altération/ blocage de messages tels que les données ODR Tracker ou le nombre de passages)
			20.4	Manipulation des données visant à **falsifier les données de conduite du véhicule** (kilométrage, vitesse de conduite, itinéraire, etc.)
			20.5	Modifications non autorisées des **données de diagnostic du système**

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			*Exemple de vulnérabilité ou de méthode d'attaque*	
	21	Effacement des données ou du code	21.1	Effacement/manipulation non autorisé(e) des **journaux d'événements du système**
	22	Introduction de logiciels malveillants	22.2	Introduire un **logiciel malveillant** ou une activité logicielle malveillante
	23	Introduction de nouveaux logiciels ou écrasement de logiciels existants	23.1	**Fabrication du logiciel** du système de commande ou d'information du véhicule
	24	Perturbation des systèmes ou des opérations	24.1	**Déni de service** pouvant, par exemple, être déclenché sur le réseau interne en inondant un bus CAN, ou en provoquant des pannes sur une UCE en envoyant un grand nombre de messages
	25	Manipulation des paramètres du véhicule	25.1	Accès non autorisé visant à **falsifier les paramètres de configuration** des fonctions critiques du véhicule, telles que les données de freinage, le seuil de déploiement de l'airbag, etc.
			25.2	Accès non autorisé visant à **falsifier les paramètres de charge**, tels que la tension de charge, la puissance de charge, la température de la batterie, etc.
4.3.7 Vulnérabilités potentielles susceptibles d'être exploitées si elles ne sont pas suffisamment protégées ou réduites	26	Les technologies cryptographiques peuvent être compromises ou ne sont pas suffisamment appliquées	26.1	L'utilisation de courtes **clefs cryptographiques** ayant une longue période de validité permet à l'attaquant de casser le cryptage
			26.2	Recours insuffisant aux algorithmes cryptographiques pour protéger les systèmes sensibles
			26.3	Utilisation d'**algorithmes cryptographiques** obsolètes ou sur le point de l'être
	27	Des pièces ou des fournitures pourraient être compromises pour permettre l'attaque des véhicules	27.1	**Matériel ou logiciel modifié pour permettre une attaque** ou ne répondant pas aux critères de conception permettant de bloquer une attaque
	28	La conception des logiciels ou du matériel est à l'origine de vulnérabilités	28.1	**Bogues logiciels**. La présence de bogues logiciels peut être la cause de vulnérabilités potentiellement exploitables. Ceci est particulièrement vrai si le logiciel n'a pas été testé pour vérifier l'absence de mauvais code ou de bogues connus et pour réduire le risque de leur présence.
			28.2	**L'utilisation des restes** de la phase de développement (ports de débogage, ports JTAG, microprocesseurs, certificats de développement, mots de passe des développeurs, etc) peut permettre l'accès aux UCE ou permettre à des attaquants d'obtenir des privilèges plus élevés
	29	La conception des réseaux introduit des vulnérabilités	29.1	**Ports Internet superflus laissés ouverts**, permettant l'accès aux systèmes réseau

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			*Exemple de vulnérabilité ou de méthode d'attaque*	
			29.2	Contourner la **séparation réseau** pour en prendre le contrôle. Par exemple, en utilisant des passerelles non protégées, ou des points d'accès (tels que les passerelles camion-remorque), pour contourner les protections et accéder à d'autres segments du réseau pour commettre des actes malveillants, comme l'envoi de messages arbitraires du bus CAN
	30	La perte physique de données est possible	30.1	**Dommages** causés par un tiers. Des données sensibles peuvent être perdues ou compromises en raison de dommages matériels subis en cas d'accident de la circulation ou de vol
			30.2	Perte due à des conflits de gestion des droits numériques (**DRM**). Les données de l'utilisateur peuvent être effacées en raison de problèmes de DRM
			30.3	Des données sensibles (ou leur intégrité) peuvent être perdues en raison de l'**usure des composants** informatiques, ce qui peut entraîner des problèmes en cascade (en cas de modification des clefs, par exemple)
	31	Le transfert involontaire de données est possible	31.1	Atteinte à la sécurité de l'information. Des données privées ou sensibles peuvent être divulguées lorsque la **voiture change de main** (par exemple, en cas de vente ou d'utilisation comme véhicule de location par de nouveaux clients)
	32	La manipulation physique des systèmes peut permettre une attaque	32.1	**Manipulation du matériel OEM**, par exemple ajout de matériel non autorisé à un véhicule pour permettre une attaque de « l'homme du milieu »

Partie B
Exemples de mesures d'atténuation des menaces

1. Exemples de mesures d'atténuation − « Serveurs dorsaux »

Des exemples de mesures d'atténuation des menaces liées aux « serveurs dorsaux » sont donnés dans le tableau B1.

Tableau B1
Exemples de mesures d'atténuation des menaces liées aux « serveurs dorsaux »

Référence du tableau 1	*Menaces liées aux « serveurs dorsaux »*	*Réf.*	*Mesure d'atténuation*
1.1 et 3.1	Abus de privilèges de la part du personnel (attaque d'initié)	M1	Des contrôles de sécurité doivent être réalisés sur les systèmes dorsaux afin de réduire au minimum le risque d'attaques d'initié. Pour des exemples de contrôles de sécurité, voir OWASP.
1.2 et 3.3	Accès Internet non autorisé au serveur (activé par exemple par des portes dérobées, des vulnérabilités logicielles système non corrigées, des attaques SQL ou d'autres moyens)	M2	Des contrôles de sécurité doivent être réalisés sur les systèmes dorsaux afin de réduire au minimum les accès non autorisés. Pour des exemples de contrôles de sécurité, voir OWASP.
1.3 et 3.4	Accès physique non autorisé au serveur (en utilisant, par exemple, des clefs USB ou d'autres supports connectés au serveur)	M8	La conception du système et le contrôle de l'accès devraient empêcher que des personnes non autorisées puissent accéder à des données personnelles ou des données critiques du système. Pour des exemples de contrôles de sécurité, voir OWASP.
2.1	Attaque d'un serveur dorsal bloquant son fonctionnement, par exemple en l'empêchant d'interagir avec les véhicules et de fournir les services dont ils ont besoin.	M3	Des contrôles de sécurité doivent être réalisés sur les systèmes dorsaux. Lorsque les serveurs dorsaux sont essentiels à la prestation des services, des mesures de rétablissement sont disponibles en cas de panne du système. Pour des exemples de contrôles de sécurité, voir OWASP.
3.2	Perte d'informations dans le « nuage ». Des données sensibles peuvent être perdues en raison d'attaques ou d'accidents lorsque les données sont stockées par des prestataires de services tiers de stockage dans le nuage	M4	Des contrôles de sécurité doivent être réalisés pour réduire au minimum les risques associés à l'informatique en nuage. Pour des exemples de contrôles de sécurité, voir OWASP et les orientations NCSC sur l'informatique en nuage.
3.5	Atteinte à la sécurité de l'information due au partage involontaire de données (par exemple, erreurs administratives, stockage des données sur des serveurs situés dans des garages)	M5	Des contrôles de sécurité doivent être réalisés sur les systèmes dorsaux pour éviter les atteintes à la sécurité des données. Pour des exemples de contrôles de sécurité, voir OWASP.

2. Exemples de mesures d'atténuation − « Voies de communication des véhicules »

Des exemples de mesures d'atténuation des menaces liées aux « voies de communication des véhicules » sont donnés dans le tableau B2.

Tableau B2
Exemples de mesures d'atténuation des menaces liées aux « voies de communication des véhicules »

Référence du tableau 1	*Menaces liées aux « voies de communication des véhicules »*	*Réf.*	*Mesure d'atténuation*
4.1	Simulation de messages (par exemple, 802.11p V2X en cas de circulation en peloton, messages GNSS, etc.) par usurpation d'identité	M10	Le véhicule doit vérifier l'authenticité et l'intégrité des messages qu'il reçoit.
4.2	Attaque Sybil (visant à simuler d'autres véhicules pour faire croire qu'il y en a beaucoup sur la route)	M11	Des contrôles de sécurité doivent être mis en œuvre pour le stockage des clefs cryptographiques.
5.1	Les voies de communication permettent l'injection de code dans les données ou le code du véhicule, par exemple un code binaire altéré peut être injecté dans le flux de communication	M10	Le véhicule doit vérifier l'authenticité et l'intégrité des messages qu'il reçoit.
		M6	Les systèmes doivent mettre en œuvre des mesures de sécurité dès la conception afin de réduire au minimum les risques.
5.2	Les voies de communication permettent de manipuler les données ou le code du véhicule	M7	Des techniques et des conceptions de contrôle de l'accès doivent être utilisées pour protéger les données ou le code du système.
5.3	Les voies de communication permettent d'écraser les données ou le code du véhicule		
5.4 21.1	Les voies de communication permettent d'effacer les données ou le code du véhicule		
5.5	Les voies de communication permettent l'introduction de données ou de code dans les systèmes du véhicule (écriture de données ou de code)		
6.1	Acceptation d'informations provenant d'une source non fiable	M10	Le véhicule doit vérifier l'authenticité et l'intégrité des messages qu'il reçoit.
6.2	Attaque de l'homme du milieu/ détournement de session.	M10	Le véhicule doit vérifier l'authenticité et l'intégrité des messages qu'il reçoit.
6.3	Attaque par rejeu, par exemple une attaque contre une passerelle de communication permettant à l'attaquant d'installer une version antérieure du logiciel d'une unité de commande électronique (UCE) ou du microprogramme de la passerelle		
7.1	Interception de l'information/rayonnements brouilleurs/surveillance des communications	M12	Les données confidentielles reçues et transmises par le véhicule doivent être protégées.
7.2	Obtention d'un accès non autorisé à des fichiers ou des données	M8	La conception du système et le contrôle de l'accès devraient empêcher que des personnes non autorisées puissent accéder à des données personnelles ou des données critiques du système. Pour des exemples de contrôles de sécurité, voir OWASP.

Référence du tableau 1	*Menaces liées aux « voies de communication des véhicules »*	*Réf.*	*Mesure d'atténuation*
8.1	Envoi d'un grand nombre de données parasites au système d'information du véhicule, de sorte qu'il soit incapable de fournir des services de manière normale	M13	Des mesures visant à détecter une attaque par déni de service et à s'en remettre doivent être mises en œuvre.
8.2	Attaque par trou noir, perturbation de la communication entre les véhicules en bloquant le transfert de messages vers d'autres véhicules	M13	Des mesures visant à détecter une attaque par déni de service et à s'en remettre doivent être mises en œuvre.
9.1	Un utilisateur sans privilèges peut obtenir un accès privilégié, par exemple un accès racine	M9	Des mesures doivent être prises pour empêcher et détecter les accès non autorisés.
10.1	Un virus introduit dans les moyens de communication infecte les systèmes du véhicule	M14	Des mesures de protection des systèmes contre les virus/logiciels malveillants intégrés devraient être envisagées.
11.1	Messages internes malveillants (par exemple, bus CAN)	M15	Des mesures de détection des messages ou activités internes malveillant(e)s devraient être envisagées.
11.2	Messages V2X malveillants, par exemple, messages d'infrastructure à véhicule ou de véhicule à véhicule (CAM, DENM, etc)	M10	Le véhicule doit vérifier l'authenticité et l'intégrité des messages qu'il reçoit.
11.3	Messages de diagnostic malveillants		
11.4	Messages propriétaires malveillants (par exemple, ceux normalement envoyés par les fabricants d'équipement d'origine OEM ou les fournisseurs de composants/systèmes/fonctions)		

2. Exemples de mesures d'atténuation − « Processus de mise à jour »

Des exemples de mesures d'atténuation des menaces liées au « processus de mise à jour » sont donnés dans le tableau B3.

Tableau B3

Exemples de mesures d'atténuation des menaces liées au « processus de mise à jour »

Référence du tableau 1	*Menaces liées au « processus de mise à jour »*	*Réf.*	*Mesure d'atténuation*
12.1	Compromission des procédures de mise à jour logicielle sans fil, y compris la fabrication du programme ou du microprogramme de mise à jour du système	M16	Des procédures sécurisées de mise à jour logicielle doivent être utilisées.
12.2	Compromission des procédures de mise à jour logicielle locales/physiques, y compris la fabrication du programme ou du microprogramme de mise à jour du système		
12.3	Le logiciel est manipulé avant le processus de mise à jour (et est donc corrompu), bien que le processus de mise à jour soit intact		

Référence du tableau 1	*Menaces liées au « processus de mise à jour »*	*Réf.*	*Mesure d'atténuation*
12.4	Compromission des clefs cryptographiques du fournisseur du logiciel pour permettre une mise à jour non valide	M11	Des contrôles de sécurité doivent être mis en œuvre pour le stockage des clefs cryptographiques.
13.1	Attaque par déni de service contre le serveur ou le réseau de mise à jour pour empêcher le déploiement de mises à jour logicielles critiques et/ou le déverrouillage de fonctionnalités spécifiques au client	M3	Des contrôles de sécurité doivent être réalisés sur les systèmes dorsaux. Lorsque les serveurs dorsaux sont essentiels à la prestation des services, des mesures de rétablissement sont disponibles en cas de panne du système. Pour des exemples de contrôles de sécurité, voir OWASP.

3. Exemples de mesures d'atténuation − « Actions humaines non intentionnelles »

Des exemples de mesures d'atténuation des menaces liées aux « actions humaines non intentionnelles » sont donnés dans le tableau B4.

Tableau B4
Exemples de mesures d'atténuation des menaces liées aux « actions humaines non intentionnelles »

Référence du tableau 1	*Menaces liées à des « actions humaines involontaires »*	*Réf.*	*Mesure d'atténuation*
14.1	Mauvaise configuration de l'équipement par la communauté de maintenance ou le propriétaire lors de l'installation, la réparation ou l'utilisation, avec des conséquences imprévues	M17	Des mesures doivent être mises en œuvre pour définir et contrôler les procédures de maintenance.
14.2	Utilisation ou administration erronée de dispositifs et de systèmes (y compris les mises à jour sans fil)		
15.1	Victime innocente (par exemple, propriétaire, opérateur ou ingénieur de maintenance) amenée par la ruse et à son insu à charger un logiciel malveillant ou à permettre une attaque	M18	Des mesures doivent être mises en œuvre pour définir et contrôler les rôles des utilisateurs et les privilèges d'accès, en se fondant sur le principe du moindre privilège.
15.2	Les procédures de sécurité définies ne sont pas suivies	M19	Les organisations doivent s'assurer que les procédures de sécurité sont définies et suivies.

4. Exemples de mesures d'atténuation − « Connectivité et connexions externes »

Des exemples de mesures d'atténuation des menaces liées à « la connectivité et aux connexions externes » sont donnés dans le tableau B5.

Tableau B5
Exemples de mesures d'atténuation des menaces liées à « la connectivité et aux connexions externes »

Référence du tableau 1	*Menaces liées à la « connectivité externe »*	*Réf.*	*Mesure d'atténuation*
16.1	Manipulation des fonctions conçues pour commander à distance des systèmes du véhicule, tels qu'une clef à distance, un dispositif d'immobilisation et une pile de chargement	M20	Des contrôles de sécurité doivent être réalisés sur les systèmes qui ont un accès à distance.

Référence du tableau 1	*Menaces liées à la « connectivité externe »*	*Réf.*	*Mesure d'atténuation*
16.2	Manipulation de la télématique du véhicule (par exemple, manipulation de la mesure de la température de biens sensibles, déverrouillage à distance des portes de chargement)		
16.3	Interférence avec des systèmes ou capteurs sans fil à courte portée		
17.1	Utilisation d'applications corrompues, ou dont la sécurité logicielle est déficiente, pour attaquer des systèmes du véhicule	M21	Les logiciels doivent faire l'objet d'une évaluation de sécurité, être authentifiés et leur intégrité doit être protégée. Des contrôles de sécurité doivent être réalisés pour réduire au minimum le risque lié aux logiciels tiers destinés à être installés sur le véhicule ou vraisemblablement susceptibles de l'être.
18.1	Interfaces externes telles que les ports USB ou autres utilisées comme point d'attaque, par exemple par injection de code	M22	Des contrôles de sécurité doivent être réalisés sur les interfaces externes.
18.2	Support infecté par des virus connecté au véhicule		
18.3	Accès diagnostique (par exemple, dongles dans le port OBD) utilisé pour faciliter une attaque, comme la manipulation (directe ou indirecte) des paramètres du véhicule	M22	Des contrôles de sécurité doivent être réalisés sur les interfaces externes.

5. Exemples de mesures d'atténuation − « Cibles ou motivations potentielles d'une attaque »

Des exemples de mesures d'atténuation des menaces liées aux « cibles ou motivations potentielles d'une attaque » sont donnés dans le tableau B6.

Tableau B6
Exemples de mesures d'atténuation des menaces liées aux « cibles ou motivations potentielles d'une attaque »

Référence du tableau 1	*Menaces liées aux « cibles ou motivations potentielles d'une attaque »*	*Réf.*	*Mesure d'atténuation*
19.1	Extraction de logiciels soumis à des droits d'auteur ou exclusifs des systèmes du véhicule (piratage de produits/logiciel volé)	M7	Des techniques et des conceptions de contrôle de l'accès doivent être utilisées pour protéger les données ou le code du système. Pour des exemples de contrôles de sécurité, voir OWASP.
19.2	Accès non autorisé aux données personnelles du propriétaire, notamment concernant son identité, son compte de paiement, son carnet d'adresses, sa localisation, l'identifiant électronique du véhicule, etc.	M8	La conception du système et le contrôle de l'accès devraient empêcher que des personnes non autorisées puissent accéder à des données personnelles ou des données critiques du système. Pour des exemples de contrôles de sécurité, voir OWASP.
19.3	Extraction de clefs cryptographiques	M11	Des contrôles de sécurité doivent être mis en œuvre pour le stockage des clefs cryptographiques.

Référence du tableau 1	*Menaces liées aux « cibles ou motivations potentielles d'une attaque »*	*Réf.*	*Mesure d'atténuation*
20.1	Modifications illicites/non autorisées de l'identifiant électronique du véhicule	M7	Des techniques et des conceptions de contrôle de l'accès doivent être utilisées pour protéger les données ou le code du système. Pour des exemples de contrôles de sécurité, voir OWASP.
20.2	Usurpation d'identité. Par exemple, si un utilisateur souhaite afficher une autre identité lorsqu'il communique avec les systèmes de péage, le système dorsal du constructeur		
20.3	Mesure visant à contourner les systèmes de surveillance (par exemple, piratage/ altération/ blocage de messages tels que les données ODR Tracker ou le nombre de passages)	M7	Des techniques et des conceptions de contrôle de l'accès doivent être utilisées pour protéger les données ou le code du système. Pour des exemples de contrôles de sécurité, voir OWASP.
20.4	Manipulation des données visant à falsifier les données de conduite du véhicule (kilométrage, vitesse de conduite, itinéraire, etc.)		
20.5	Modifications non autorisées des données de diagnostic du système		
21.1	Effacement/manipulation non autorisé(e) des journaux d'événements du système	M7	Des techniques et des conceptions de contrôle de l'accès doivent être utilisées pour protéger les données ou le code du système. Pour des exemples de contrôles de sécurité, voir OWASP.
22.2	Introduire un logiciel malveillant ou une activité logicielle malveillante	M7	Des techniques et des conceptions de contrôle de l'accès doivent être utilisées pour protéger les données ou le code du système. Pour des exemples de contrôles de sécurité, voir OWASP.
23.1	Fabrication du logiciel du système de commande ou d'information du véhicule		
24.1	Déni de service pouvant, par exemple, être déclenché sur le réseau interne en inondant un bus CAN, ou en provoquant des pannes sur une UCE en envoyant un grand nombre de messages	M13	Des mesures visant à détecter une attaque par déni de service et à s'en remettre doivent être mises en œuvre
25.1	Accès non autorisé visant à falsifier les paramètres de configuration des fonctions critiques du véhicule, telles que les données de freinage, le seuil de déploiement de l'airbag, etc.	M7	Des techniques et des conceptions de contrôle de l'accès doivent être utilisées pour protéger les données ou le code du système. Pour des exemples de contrôles de sécurité, voir OWASP.
25.2	Accès non autorisé visant à falsifier les paramètres de charge, tels que la tension de charge, la puissance de charge, la température de la batterie, etc.		

6. Exemples de mesures d'atténuation − « Vulnérabilités potentielles susceptibles d'être exploitées si elles ne sont pas suffisamment protégées ou réduites »

Des exemples de mesures d'atténuation des menaces liées aux « vulnérabilités potentielles susceptibles d'être exploitées si elles ne sont pas suffisamment protégées ou réduites » sont donnés dans le tableau B7.

Tableau B7
Exemples de mesures d'atténuation des menaces liées aux « vulnérabilités potentielles susceptibles d'être exploitées si elles ne sont pas suffisamment protégées ou réduites »

Référence du tableau 1	*Menaces liées aux « vulnérabilités potentielles susceptibles d'être exploitées si elles ne sont pas suffisamment protégées ou réduites »*	*Réf.*	*Mesure d'atténuation*
26.1	L'utilisation de courtes clefs cryptographiques ayant une longue période de validité permet à l'attaquant de casser le cryptage	M23	Les meilleures pratiques de cybersécurité doivent être suivies lors du développement des logiciels et du matériel. Pour des exemples de contrôles de sécurité, voir SAE J3061.
26.2	Recours insuffisant aux algorithmes cryptographiques pour protéger les systèmes sensibles		
26.3	Utilisation d'algorithmes cryptographiques obsolètes		
27.1	Matériel ou logiciel modifié pour permettre une attaque ou ne répondant pas aux critères de conception permettant de bloquer une attaque	M23	Les meilleures pratiques de cybersécurité doivent être suivies lors du développement des logiciels et du matériel.
28.1	La présence de bogues logiciels peut être la cause de vulnérabilités potentiellement exploitables. Ceci est particulièrement vrai si le logiciel n'a pas été testé pour vérifier l'absence de mauvais code ou de bogues connus et pour réduire le risque de leur présence.	M23	Les meilleures pratiques de cybersécurité doivent être suivies lors du développement des logiciels et du matériel.
28.2	L'utilisation des restes de la phase de développement (ports de débogage, ports JTAG, microprocesseurs, certificats de développement, mots de passe des développeurs, etc.) peut permettre à un attaquant d'accéder aux UCE ou d'obtenir des privilèges plus élevés		
29.1	Ports Internet superflus laissés ouverts, permettant l'accès aux systèmes réseau		
29.2	Contourner la séparation réseau pour en prendre le contrôle. Par exemple, en utilisant des passerelles non protégées, ou des points d'accès (tels que les passerelles camion-remorque), pour contourner les protections et accéder à d'autres segments du réseau pour commettre des actes malveillants, comme l'envoi de messages arbitraires du bus CAN	M23	Les meilleures pratiques de cybersécurité doivent être suivies lors du développement des logiciels et du matériel.

7. Exemples de mesures d'atténuation − « Perte de données/atteinte à la sécurité des données du véhicule »

Des exemples de mesures d'atténuation des menaces liées à « la perte de données/l'atteinte à la sécurité des données du véhicule » sont donnés dans le tableau B8.

Tableau B8
Exemples de mesures d'atténuation des menaces liées à « la perte de données/l'atteinte à la sécurité des données du véhicule »

Référence du tableau 1	*Menaces liées à « la perte de données/l'atteinte à la sécurité des données du véhicule »*	*Réf.*	*Mesure d'atténuation*
30.1	Dommages causés par un tiers. Des données sensibles peuvent être perdues ou compromises en raison de dommages matériels subis en cas d'accident de la circulation ou de vol	M24	Les meilleures pratiques de protection des données doivent être suivies pour le stockage des données privées et sensibles. Pour des exemples de contrôles de sécurité, voir ISO/SC27/WG5.
30.2	Perte due à des conflits de gestion des droits numériques (DRM). Les données de l'utilisateur peuvent être effacées en raison de problèmes de DRM		
30.3	Des données sensibles (ou leur intégrité) peuvent être perdues en raison de l'usure des composants informatiques, ce qui peut entraîner des problèmes en cascade (en cas de modification des clefs, par exemple)		
31.1	Atteinte à la sécurité de l'information. Des données privées ou sensibles peuvent être divulguées lorsque la voiture change de main (par exemple, en cas de vente ou d'utilisation comme véhicule de location par de nouveaux clients)		

8. Exemples de mesures d'atténuation − « Manipulation physique des systèmes en vue de permettre une attaque »

Des exemples de mesures d'atténuation des menaces liées à la « manipulation physique des systèmes en vue de permettre une attaque » sont donnés dans le tableau B9.

Tableau B9
Exemples de mesures d'atténuation des menaces liées à la « manipulation physique des systèmes en vue de permettre une attaque »

Référence du tableau 1	*Menaces liées à la « manipulation physique des systèmes en vue de permettre une attaque »*	*Réf.*	*Mesure d'atténuation*
32.1	Manipulation du matériel OEM, par exemple ajout de matériel non autorisé à un véhicule pour permettre une attaque de l'homme du milieu	M9	Des mesures doivent être prises pour empêcher et détecter les accès non autorisés.

Annexe C

Exemples de contrôles de sécurité liés aux mesures d'atténuation

1. Introduction

1.1 La présente annexe a un caractère informatif.

1.2 La présente annexe peut être consultée par les services techniques et d'autres parties prenantes, si nécessaire, pour les aider à mieux comprendre les contrôles de sécurité.

1.3 Les exemples de contrôles de sécurité donnés dans la présente annexe ne doivent pas être considérés comme obligatoires dans le cadre de l'évaluation d'un système. Ces exemples ne sont pas nécessairement exhaustifs ou appropriés à tous les systèmes ou toutes les conceptions de véhicules.

1.4 De nouveaux contrôles de sécurité devraient être envisagés pour suivre les progrès de la technologie. La présente annexe pourrait également être actualisée à intervalles réguliers, pour s'assurer que son contenu reflète l'état de la technique.

2. Établissement de correspondances entre les mesures d'atténuation de haut niveau indiquées à l'annexe B et des exemples plus détaillés de contrôles de sécurité

2.1 Le tableau ci-dessous fournit des détails supplémentaires sur des exemples de contrôles de sécurité relatifs aux « mesures d'atténuation ». La liste des contrôles de sécurité figurant dans ce tableau n'est pas exhaustive. De même, tous les contrôles de sécurité recensés ne sont pas nécessairement requis. Leur sélection doit reposer sur une appréciation du risque et sur toute prescription juridique, contractuelle ou réglementaire pertinente dans un environnement spécifique de systèmes de transport intelligents / conduite automatisée.

Identifiant	*Mesure d'atténuation*	*Contrôles de sécurité potentiellement pertinents, illustrés d'exemples informatifs*
M1	Des contrôles de sécurité doivent être réalisés sur les systèmes dorsaux afin de réduire au minimum le risque d'attaques d'initié	3.1 Politiques de sécurité 3.2 Sécurité organisationnelle 3.3 Sécurité des ressources humaines et sensibilisation à la sécurité 3.4 Gestion du matériel 3.5 Contrôle d'accès : • Principe du double contrôle appliqué • Contrôles d'accès basés sur les rôles (« besoin d'en connaître », « séparation des tâches ») et formation appropriée du personnel 3.6 Sécurité cryptographique 3.7 Sécurité physique et environnementale 3.8 Surveillance • Mécanismes d'enregistrement ou de suivi des activités du personnel • Informations de sécurité et gestion des événements

Identifiant	*Mesure d'atténuation*	*Contrôles de sécurité potentiellement pertinents, illustrés d'exemples informatifs*
		3.10 Sécurité des logiciels 3.12 Gestion des incidents de sécurité 3.13 Échange d'informations
M2	Des contrôles de sécurité doivent être réalisés sur les systèmes dorsaux afin de réduire au minimum les accès non autorisés	3.5 Contrôle d'accès et authentification 3.6 Sécurité cryptographique 3.7 Sécurité physique et environnementale 3.8 Surveillance • Surveillance des systèmes serveurs et des communications 3.9 Conception du système • Configuration sécurisée des serveurs (par exemple, renforcement du système) • Protection des connexions Internet externes, y compris l'authentification ou la vérification des messages reçus et fourniture de voies de communication cryptées • Gestion des risques et de la sécurité des serveurs en nuage (le cas échéant) 3.10 Sécurité des logiciels 3.12 Gestion des incidents de sécurité • Informations de sécurité et gestion des événements 3.13 Échange d'informations
M3	Des contrôles de sécurité doivent être réalisés sur les systèmes dorsaux. Lorsque les serveurs dorsaux sont essentiels à la prestation des services, des mesures de rétablissement sont disponibles en cas de panne du système	3.5 Contrôle d'accès • Contrôles d'accès basés sur les rôles pour le personnel 3.8 Surveillance 3.9 Conception du système • Appliquer des techniques de minimisation des données pour réduire l'impact de leur éventuelle perte • Renforcer les systèmes pour empêcher et réduire au minimum tout accès physique non autorisé • Adopter des mesures proportionnées de protection physique et de surveillance 3.10 Sécurité des logiciels 3.12 Gestion des incidents de sécurité 3.13 Échange d'informations
M4	Des contrôles de sécurité doivent être réalisés pour réduire au minimum les risques associés à l'informatique en nuage	3.1 Politiques de sécurité 3.2 Sécurité organisationnelle 3.3 Sécurité des ressources humaines et sensibilisation à la sécurité 3.4 Gestion du matériel 3.5 Contrôle d'accès 3.6 Sécurité cryptographique 3.7 Sécurité physique et environnementale 3.8 Surveillance • Surveillance des systèmes serveurs

Identifiant	*Mesure d'atténuation*	*Contrôles de sécurité potentiellement pertinents, illustrés d'exemples informatifs*
		3.9 Conception du système • Gérer les risques et la sécurité des serveurs en nuage • Appliquer des techniques de minimisation des données pour réduire l'impact de leur éventuelle perte 3.10 Sécurité des logiciels 3.11 Sécurité des relations avec les fournisseurs 3.12 Gestion des incidents de sécurité • Informations de sécurité et gestion des événements 3.13 Échange d'informations
M5	Des contrôles de sécurité doivent être réalisés sur les systèmes dorsaux pour éviter les atteintes à la sécurité des données	3.1 Politiques de sécurité 3.2 Sécurité organisationnelle 3.3 Sécurité des ressources humaines et sensibilisation à la sécurité • Procédures appropriées de manipulation, de transfert et de cession des données • Formation appropriée du personnel, en particulier du personnel chargé de la manipulation des données 3.4 Gestion du matériel 3.5 Contrôle d'accès 3.6 Sécurité cryptographique 3.7 Sécurité physique et environnementale 3.8 Surveillance 3.9 Conception du système • Appliquer des techniques de minimisation des données pour réduire l'impact de leur éventuelle perte 3.10 Sécurité des logiciels 3.12 Gestion des incidents de sécurité 3.13 Échange d'informations
M6	Le principe d'intégration de la sécurité dès la conception doit être adopté pour réduire au minimum l'impact d'une attaque sur l'écosystème du véhicule	3.1 Politiques de sécurité 3.5 Contrôle d'accès • Procédures de contrôle d'accès et de lecture/écriture définies pour les fichiers et données du véhicule 3.6 Sécurité cryptographique 3.7 Sécurité physique et environnementale 3.8 Surveillance • Surveillance du système 3.9 Conception du système • Vérification de l'intégrité et de l'authentification des messages • Renforcement du système d'exploitation par exemple • Protection active de la mémoire • Segmentation du réseau et mise en œuvre de limites de confiance

Identifiant	*Mesure d'atténuation*	*Contrôles de sécurité potentiellement pertinents, illustrés d'exemples informatifs*
		3.10 Sécurité des logiciels • Techniques de vérification de l'intégrité des logiciels 3.12 Gestion des incidents de sécurité 3.13 Échange d'informations
M7	Des techniques et des conceptions de contrôle de l'accès doivent être utilisées pour protéger les données ou le code du système	3.5 Contrôle d'accès • Procédures de contrôle d'accès et de lecture/écriture définies pour les fichiers et données du véhicule 3.6 Sécurité cryptographique 3.7 Sécurité physique et environnementale 3.8 Surveillance • Surveillance du système 3.9 Conception du système • Protection active de la mémoire • Segmentation du réseau et mise en œuvre de limites de confiance • Validation des entrées en fonction de l'application (type de données/entrées attendues par l'application concernée) • Stockage sécurisé des informations sensibles 3.10 Sécurité des logiciels • Techniques de vérification de l'intégrité des logiciels • Test des logiciels 3.12 Gestion des incidents de sécurité 3.13 Échange d'informations
M8	La conception du système et le contrôle de l'accès devraient empêcher que des personnes non autorisées puissent accéder à des données personnelles ou des données critiques du système	3.5 Contrôle d'accès • Contrôles d'accès basés sur les rôles 3.6 Sécurité cryptographique 3.8 Surveillance 3.9 Conception du système • Renforcer les systèmes pour empêcher et réduire au minimum tout accès non autorisé • Adopter des mesures proportionnées de protection physique et de surveillance 3.10 Sécurité des logiciels 3.13 Échange d'informations
M9	Des mesures doivent être prises pour empêcher et détecter les accès non autorisés	3.5 Contrôle d'accès • Authentification multifactorielle pour les applications nécessitant un accès racine • Appliquer les « contrôles d'accès avec les moindres privilèges », par exemple en séparant les comptes administratifs 3.8 Surveillance • Surveillance du système

Identifiant	*Mesure d'atténuation*	*Contrôles de sécurité potentiellement pertinents, illustrés d'exemples informatifs*
		3.9 Conception du système • Établir des limites de confiance et des contrôles d'accès • Éviter les réseaux plats (assurer la sécurité en profondeur et la séparation des réseaux) 3.10 Sécurité des logiciels 3.13 Échange d'informations
M10	Le véhicule doit vérifier l'authenticité et l'intégrité des messages qu'il reçoit	3.5 Contrôle d'accès • Procédures de contrôle d'accès et de lecture/écriture définies pour les fichiers et données du véhicule 3.6 Sécurité cryptographique • Cryptage des communications contenant des données sensibles 3.8 Surveillance • Surveillance du système • Limiter et surveiller le contenu des messages et les protocoles 3.9 Conception du système • Authentification de tous les messages reçus • Vérification de l'intégrité et de l'authentification des messages • Tests de cohérence à l'aide d'autres capteurs du véhicule (température, radar, etc.) • Utilisation de techniques de vérification de l'intégrité, telles que le hachage, les protocoles sécurisés et le filtrage des paquets • Recours aux techniques de protection contre les attaques par rejeu, telles que l'horodatage et l'utilisation de valeurs sur l'ancienneté des données • Politiques de gestion de sessions pour éviter leur détournement • Renforcement du système d'exploitation • Protection active de la mémoire • Utilisation conjuguée de passerelles, de pare-feu, de mécanismes de prévention ou de détection des intrusions et de surveillance pour protéger les systèmes • Segmentation du réseau et mise en œuvre de limites de confiance 3.10 Sécurité des logiciels • Techniques de vérification de l'intégrité des logiciels 3.13 Échange d'informations
M11	Des contrôles de sécurité doivent être mis en œuvre pour le stockage des clefs cryptographiques	3.6 Sécurité cryptographique • Gérer et protéger activement les clefs cryptographiques • Envisager l'utilisation de modules de sécurité matérielle (HSM), de techniques de détection de manipulations frauduleuses et d'authentification des dispositifs pour réduire les vulnérabilités
M12	Les données confidentielles reçues et transmises par le véhicule doivent être protégées	3.6 Sécurité cryptographique • Cryptage des communications contenant des données sensibles 3.9 Conception du système • Techniques de minimisation des données appliquées aux communications

Identifiant	*Mesure d'atténuation*	*Contrôles de sécurité potentiellement pertinents, illustrés d'exemples informatifs*
		3.10 Sécurité des logiciels • Les logiciels et les systèmes utilisés pour protéger les informations confidentielles sont soumis à des tests de vulnérabilité
M13	Des mesures visant à détecter une attaque par déni de service et à s'en remettre doivent être mises en œuvre	3.8 Surveillance 3.9 Conception du système • Vérifier que la taille des données reçues correspond aux valeurs attendues • Authentification des données • Horodatage des messages et définition de leurs date et heure d'expiration • Mise en œuvre de mesures de limitation du débit en fonction du contexte • Définition de messages d'accusé de réception pour les messages V2X (actuellement non normalisés) • Stratégie de repli en cas de perte de communication 3.10 Sécurité des logiciels 3.12 Gestion des incidents de sécurité 3.13 Échange d'informations
M14	Des mesures de protection des systèmes contre les virus/logiciels malveillants intégrés devraient être envisagées	3.8 Surveillance • Surveillance du système 3.9 Conception du système • Authentification des messages et vérification de leur intégrité • Validation des entrées pour tous les messages • Établir des limites de confiance et des contrôles d'accès • Éviter les réseaux plats (assurer la sécurité en profondeur et la séparation des réseaux) 3.10 Sécurité des logiciels 3.12 Gestion des incidents de sécurité 3.13 Échange d'informations
M15	Des mesures de détection des messages ou activités internes malveillant(e)s devraient être envisagées	3.8 Surveillance • Surveillance du système 3.9 Conception du système • Authentification des messages et vérification de leur intégrité • Validation des entrées pour tous les messages • Établir des limites de confiance et des contrôles d'accès • Éviter les réseaux plats (assurer la sécurité en profondeur, l'isolement des composants et la séparation des réseaux) 3.10 Sécurité des logiciels 3.12 Gestion des incidents de sécurité 3.13 Échange d'informations

Identifiant	*Mesure d'atténuation*	*Contrôles de sécurité potentiellement pertinents, illustrés d'exemples informatifs*
M16	Des procédures sécurisées de mise à jour logicielle doivent être utilisées	3.6 Sécurité cryptographique • Gestion et protection efficaces des clefs cryptographiques utilisées 3.8 Surveillance 3.9 Conception du système 3.10 Sécurité des logiciels • Établir des procédures sécurisées, y compris des modèles et politiques de configuration • Utiliser des communications sécurisées pour les mises à jour • Assurer l'authenticité des mises à jour • Enregistrement de la version et de l'horodatage des mises à jour • Assurer la protection et la signature cryptographiques des mises à jour logicielles • Assurer le contrôle de la configuration et la possibilité d'annuler les mises à jour 3.13 Échange d'informations
M17	Des mesures doivent être mises en œuvre pour définir et contrôler les procédures de maintenance	3.3 Sécurité des ressources humaines et sensibilisation à la sécurité • Formation appropriée du personnel de maintenance 3.8 Surveillance 3.9 Conception du système • Assurer l'utilisation de modèles et de politiques de configuration • Vérifier la configuration des dispositifs • Autoriser uniquement la transmission à un véhicule d'un jeu d'instructions sûr • Appliquer les techniques d'authentification des messages et des dispositifs • Assurer des contrôles appropriés des données 3.10 Sécurité des logiciels 3.12 Gestion des incidents de sécurité 3.13 Échange d'informations
M18	Des mesures doivent être mises en œuvre pour définir et contrôler les rôles des utilisateurs et les privilèges d'accès, en se fondant sur le principe du moindre privilège	3.1 Politiques de sécurité 3.2 Sécurité organisationnelle 3.3 Sécurité des ressources humaines et sensibilisation à la sécurité 3.4 Gestion du matériel 3.5 Contrôle d'accès et authentification
M19	Les organisations doivent s'assurer que les procédures de sécurité sont définies et suivies	3.1 Politiques de sécurité 3.2 Sécurité organisationnelle 3.3 Sécurité des ressources humaines et sensibilisation à la sécurité • Existence d'un programme de sécurité définissant les procédures • Établir un processus de développement et de maintenance de la sécurité, y compris aux étapes de l'examen, de la contre-vérification et de l'approbation

Identifiant	*Mesure d'atténuation*	*Contrôles de sécurité potentiellement pertinents, illustrés d'exemples informatifs*
		• Les besoins spécifiques de sensibilisation et de formation à la cybersécurité sont déterminés selon les rôles, notamment en matière de conception et d'ingénierie, puis mis en œuvre
M20	Des contrôles de sécurité doivent être réalisés sur les systèmes qui ont un accès à distance	3.5 Contrôle d'accès • Droits de contrôle d'accès définis et mis en œuvre pour les systèmes d'accès à distance au véhicule 3.8 Surveillance • Surveillance du système axée sur les messages/comportements inattendus 3.9 Conception du système • Appliquer les techniques d'authentification des messages et des dispositifs • Autoriser uniquement la transmission à un véhicule d'un jeu d'instructions sûr • Utilisation de techniques de vérification de l'intégrité des messages, telles que le hachage, les protocoles sécurisés et le filtrage des paquets • Recours aux techniques de protection contre les attaques par rejeu, telles que l'horodatage et l'utilisation de valeurs sur l'ancienneté des données • Séparation du réseau mise en œuvre 3.10 Sécurité des logiciels • Tests logiciels et matériels pour réduire les vulnérabilités 3.12 Gestion des incidents de sécurité 3.13 Échange d'informations
M21	Les logiciels doivent faire l'objet d'une évaluation de sécurité, être authentifiés et leur intégrité doit être protégée	3.8 Surveillance 3.9 Conception du système 3.10 Sécurité des logiciels 3.13 Échange d'informations
M22	Des contrôles de sécurité doivent être réalisés sur les interfaces externes	3.8 Surveillance • Surveillance du système axée sur les messages/comportements inattendus 3.9 Conception du système • Appliquer les techniques d'authentification des messages et des dispositifs • Autoriser uniquement la transmission à un véhicule d'un jeu d'instructions sûr • Assurer la protection des limites de confiance et le contrôle d'accès entre les interfaces externes et les autres systèmes du véhicule • Les systèmes sont renforcés pour limiter l'accès 3.10 Sécurité des logiciels 3.12 Gestion des incidents de sécurité 3.13 Échange d'informations

Identifiant	*Mesure d'atténuation*	*Contrôles de sécurité potentiellement pertinents, illustrés d'exemples informatifs*
M23	Les meilleures pratiques de cybersécurité doivent être suivies lors du développement des logiciels et du matériel	3.2 Sécurité de l'organisation • Un programme actif est en place pour déceler les vulnérabilités critiques • Les organisations planifient les moyens d'assurer la sécurité de leurs systèmes pendant toute leur durée de vie 3.6 Sécurité cryptographique 3.7 Sécurité physique et environnementale 3.9 Conception du système • Adopter des pratiques de codage sécurisées pour la segmentation du réseau • Les risques de sécurité sont évalués et gérés de manière appropriée et proportionnée, y compris ceux propres à la chaîne d'approvisionnement • Méthodologies de conception sécurisées, y compris l'assurance que les impératifs de conception du réseau sont respectés par les mises en œuvre correspondantes 3.10 Sécurité des logiciels • Cryptage du code logiciel • Autoriser uniquement les applications soumises à un niveau de test accepté pour réduire les vulnérabilités • Les logiciels et leur configuration doivent faire l'objet d'une évaluation de sécurité, être authentifiés et leur intégrité doit être protégée 3.11 Sécurité des relations avec les fournisseurs • Il est possible de vérifier et de valider l'authenticité et l'origine des fournitures • Les organisations, y compris les fournisseurs, peuvent fournir des assurances sur leurs processus de sécurité et leurs produits 3.13 Échange d'informations
M24	Les meilleures pratiques de protection des données doivent être suivies pour le stockage des données privées et sensibles	3.6 Sécurité cryptographique 83. Surveillance 3.9 Conception du système • Les systèmes sont conçus de façon que les utilisateurs finaux puissent accéder, effacer et gérer leurs données personnelles de manière efficace et appropriée • Définir des mesures pour assurer l'effacement sécurisé des données des utilisateurs en cas de changement de propriétaire 3.10 Sécurité des logiciels 3.13 Échange d'informations
M25	Les systèmes devraient être conçus de manière à réagir de façon appropriée en cas de détection d'une attaque contre un véhicule	3.8 Surveillance 3.9 Conception du système • Les risques de sécurité sont évalués et gérés de manière appropriée et proportionnée • Redondances ou sauvegardes intégrées, en cas de panne du système

Identifiant	*Mesure d'atténuation*	*Contrôles de sécurité potentiellement pertinents, illustrés d'exemples informatifs*
		• Les systèmes critiques pour la sécurité sont protégés en cas de défaillance • Des mesures pour garantir la disponibilité des données sont recommandées 3.10 Sécurité des logiciels 3.12 Gestion des incidents de sécurité 3.13 Échange d'informations

3. Informations complémentaires sur les contrôles de sécurité

Des informations ou suggestions complémentaires concernant les exemples de contrôles de sécurité fournis dans le tableau ci-dessus sont données ci-après.

Le choix des contrôles de sécurité appropriés et l'application des orientations de mise en œuvre fournies dépendront de la conception du véhicule, définie par son type, de son appréciation du risque et de tout facteur juridique, contractuel ou réglementaire pertinent.

3.1 Politiques de sécurité

3.1.1 Les orientations relatives aux politiques de sécurité spécifiées dans la norme ISO/SAE 21434 peuvent s'appliquer.

3.1.2 Les points suivants peuvent également s'appliquer :

Les politiques de cybersécurité doivent être définies et approuvées par la direction et communiquées aux employés ;

Les politiques doivent être revues à intervalles réguliers ou en cas de changements importants, pour s'assurer de leur pertinence, de leur validité et de leur efficacité.

3.2 Sécurité organisationnelle

Les points suivants peuvent s'appliquer :

Les rôles et responsabilités en matière de cybersécurité doivent être définis et à attribués ;

Séparation des tâches afin de réduire les possibilités de modification ou d'utilisation abusive non autorisée ou non intentionnelle du matériel de l'organisation ;

Des contacts appropriés doivent être établis avec les autorités compétentes en cas d'activités de gestion des incidents de sécurité ou autres ;

Les contacts avec les groupes d'intérêt, les forums spécialisés en matière de sécurité et les associations professionnelles doivent être maintenus pour assurer une gestion efficace des connaissances en matière de cybersécurité.

3.3 Sécurité des ressources humaines et sensibilisation à la sécurité

3.3.1 Les points suivants peuvent s'appliquer :

Les besoins spécifiques de sensibilisation et de formation à la cybersécurité sont déterminés selon les rôles, notamment en matière de conception et d'ingénierie, puis mis en œuvre ;

Existence d'un programme de sécurité définissant les procédures ;

Formation appropriée du personnel, en particulier du personnel chargé de la manipulation des données ;

Formation appropriée du personnel de maintenance ;

Mécanismes d'enregistrement et de suivi des activités du personnel ;

Établir un processus de développement et de maintenance de la sécurité, y compris aux étapes de l'examen, de la contre-vérification et de l'approbation.

3.3.2 Points spécifiques relatifs aux « facteurs à prendre en compte en fin de vie » :

Procédures appropriées de manipulation, de transfert et de cession des données ;

Définir des mesures pour assurer l'effacement sécurisé des données des utilisateurs en cas de changement de propriétaire.

3.4 Gestion du matériel

3.4.1 Les points suivants peuvent s'appliquer :

Les éléments des systèmes du véhicule doivent être répertoriés et leur inventaire doit être dressé et tenu à jour ;

L'affectation des éléments figurant dans l'inventaire doit être connue ;

Les règles régissant l'utilisation acceptable des systèmes du véhicule et des éléments associés doivent être définies, expliquées et appliquées ;

Lorsqu'un élément est devenu inutile, il convient de s'en défaire de manière sécurisée, selon des procédures officielles.

3.5 Contrôle d'accès

3.5.1 Les points suivants peuvent s'appliquer :

3.5.1.1 Points liés aux « mécanismes de contrôle d'accès » :

- Établir des limites de confiance et des contrôles d'accès ;
- Appliquer le principe du moindre privilège pour réduire au minimum les risques ;
- Les contrôles d'accès basés sur les rôles (« besoin d'en connaître », « séparation des tâches ») sont en place et appliqués ;
- Procédures de contrôle d'accès et de lecture/écriture définies pour les fichiers, systèmes et données du véhicule ;
- Droits de contrôle d'accès définis et mis en œuvre pour les systèmes d'accès à distance au véhicule ;
- Assurer la protection des limites de confiance et le contrôle d'accès entre les interfaces externes et les autres systèmes du véhicule ;
- Assurer la protection des limites de confiance et le contrôle d'accès entre les logiciels hébergés (applications) et les autres systèmes du véhicule ;
- Principe du double contrôle appliqué ;
- Authentification multifactorielle pour les applications nécessitant un accès racine ;
- Contrôle d'accès au système et aux applications ;

a) Restriction de l'accès aux informations ;

b) Procédures de connexion sécurisées ;

c) Système de gestion des mots de passe pour les utilisateurs/ conducteurs ;

d) Utilisation d'utilitaires privilégiés ;

f) Contrôle d'accès au code source du véhicule.

3.5.1.2 Points liés à l'« authentification des dispositifs et des applications » :

- Appliquer les techniques d'authentification des dispositifs ;
- Authentification des dispositifs et équipements ;
- Vérifier la configuration des dispositifs ;
- Établir des procédures concernant les applications autorisées, ce qu'elles peuvent faire et dans quelles conditions.

3.5.1.3 Points liés à l'« autorisation » :

- S'assurer que des mécanismes d'autorisation sont en place concernant les rôles d'accès au véhicule ;
- S'assurer que l'application embarquée a clairement défini les types d'utilisateurs et les droits de ces derniers ;
- Veiller à l'application d'une approche du moindre privilège ;
- S'assurer que les mécanismes d'autorisation fonctionnent correctement, échouent de manière sécurisée et ne peuvent être contournés.

3.6 Sécurité cryptographique

3.6.1 Les points suivants peuvent s'appliquer :

3.6.1.1 Points liés à la « gestion des clés cryptographiques » :

- Gérer et protéger activement les clés cryptographiques ;
- Gestion et protection efficaces des clés cryptographiques utilisées.

3.6.1.2 Points liés au « cryptage des communications et des logiciels » :

- Cryptage des communications contenant des données sensibles, y compris les mises à jour logicielles ;
- Cryptage du code logiciel ;
- S'assurer qu'aucune donnée sensible n'est transmise en clair, que ce soit en interne ou en externe ;
- S'assurer que l'application utilise de bonnes méthodes cryptographiques connues.

3.7 Sécurité physique et environnementale

3.7.1 Aucun autre point signalé.

3.8 Surveillance

3.8.1 Les orientations relatives à la surveillance sur le terrain spécifiées dans la norme ISO/SAE 21434 peuvent s'appliquer.

3.8.2 Les points suivants peuvent également s'appliquer :

- Surveillance du système axée sur les messages/comportements inattendus ;
- Adoption de mesures proportionnées de protection physique et de surveillance ;
- Surveillance des systèmes serveurs et des communications ;
- Systèmes de détection et de riposte en cas de simulation de capteurs ;
- Politiques de gestion de sessions pour éviter leur détournement ;
- Protection contre les logiciels malveillants ;
- Enregistrement et surveillance ;
- Contrôle des logiciels opérationnels ;
- Considérations relatives à l'audit des systèmes d'information.

3.9 Conception du système

3.9.1 Les points suivants peuvent s'appliquer :

3.9.1.1 Points liés à la « conception du réseau » :

- Éviter les réseaux plats (assurer la sécurité en profondeur, l'isolement des composants et la séparation des réseaux) ;
- Segmentation du réseau et mise en œuvre de limites de confiance ;
- Protection des connexions Internet externes, y compris l'authentification ou la vérification des messages reçus et fourniture de voies de communication cryptées ;
- Environnement sécurisé pour l'exécution protégée de logiciels tiers ;
- Utilisation conjuguée de passerelles, de pare-feu, de mécanismes de prévention ou de détection des intrusions et de surveillance pour protéger les systèmes ;
- S'assurer que toutes les connexions internes et externes (utilisateur et entité) soient soumises à un mécanisme d'authentification approprié et adéquat. Veiller à ce que ce contrôle ne puisse pas être contourné ;
- S'assurer que les authentifiants ne sont pas transmis en clair.

3.9.1.2 Points liés au « contrôle des données stockées dans les véhicules et les serveurs et communiquées depuis ceux-ci » :

a) Généralités :

- Assurer des contrôles appropriés des données ;
- S'assurer que les informations sensibles ne sont pas compromises ;
- Appliquer des techniques de minimisation des données pour réduire l'impact de leur éventuelle perte ;
- Techniques de minimisation des données appliquées aux communications ;
- Les systèmes sont conçus de façon que les utilisateurs finaux puissent accéder, effacer et gérer leurs données personnelles de manière efficace et appropriée ;
- Appliquer des techniques pour éviter la manipulation frauduleuse de données système critiques ;
- Appliquer des permissions d'écriture et des mesures d'authentification strictes pour la mise à jour et l'accès aux paramètres du véhicule ;
- S'assurer que l'indicateur de sécurité est défini de sorte à éviter toute transmission accidentelle dans le réseau du véhicule ;

b) Recours au chiffrement :

- Élaboration et application d'orientations concernant l'utilisation de moyens de contrôle cryptographiques pour protéger l'information. Cela comprend la mise en évidence des données présentes et de la protection requise ;
- Stockage sécurisé des informations sensibles ;
- Cryptage des données sensibles et soin apporté à la gestion appropriée et sécurisée des clés de chiffrement ;
- Protection active de la mémoire ;

- Utilisation de modules de sécurité matérielle (HSM), de techniques de détection de manipulations frauduleuses et d'authentification des dispositifs à envisager pour réduire les vulnérabilités ;

c) Authentification :

- S'assurer que, lors de la transmission d'authentifiants ou de toute autre information sensible, les données sont uniquement acceptées si elles utilisent des protocoles et des canaux d'information sécurisés empruntant la voie de communication du véhicule ;
- S'assurer que toutes les pages exigent l'authentification des informations sensibles ;

d) Cookies :

- Déterminer si toutes les transitions d'état dans le code de l'application vérifient correctement les cookies et imposent leur utilisation ;
- S'assurer que des activités non autorisées ne peuvent pas être exécutées en manipulant des cookies ;
- S'assurer que les cookies contiennent le moins d'informations privées (utilisateur/conducteur) possible ;
- S'assurer que l'intégralité des cookies est cryptée s'ils contiennent des données sensibles ;
- Définir tous les cookies utilisés par l'application, leur nom, et leur raison d'être ;

e) Validation des données :

- S'assurer que les données de la session sont validées ;
- Veiller à l'existence d'un mécanisme de validation des données ;
- S'assurer que toutes les entrées qui peuvent être modifiées par un utilisateur malveillant comme les en-têtes HTTP, les champs de saisie, les champs cachés, les listes déroulantes et les autres composants Web sont correctement validées ;
- Veiller à l'existence de contrôles de longueur appropriés sur toutes les entrées ;
- S'assurer que tous les champs, cookies, en-têtes/corps de requêtes http et champs de formulaire sont validés ;
- S'assurer que les données sont bien formées et ne contiennent que des caractères acceptables et connus si possible ;
- S'assurer que la validation des données s'effectue côté serveur ;
- Déterminer à quel endroit a lieu la validation des données et si un modèle centralisé ou décentralisé est utilisé ;
- Veiller à l'absence de portes dérobées dans le modèle de validation des données ;
- Règle d'or : toutes les entrées externes, quelles qu'elles soient, doivent être examinées et validées.

3.9.1.3 Points relatifs aux « contrôles portant sur les messages » :

a) Autoriser uniquement la transmission à un véhicule d'un jeu d'instructions sûr ;

b) Authentification des messages et vérification de leur intégrité :

- Authentification des données ;

- Vérifier que la taille des données reçues correspond aux valeurs attendues ;
- Limiter et surveiller le contenu des messages et les protocoles ;
- Mettre en œuvre des mesures de limitation du débit en fonction du contexte ;
- Validation des entrées pour tous les messages ;

c) Validation des entrées en fonction de l'application (type de données/entrées attendues par l'application concernée) ;

d) Tests de cohérence à l'aide d'autres capteurs du véhicule (température, radar, etc.) ;

e) Définition de messages d'accusé de réception pour les messages V2X (actuellement non normalisés) ;

f) Techniques de prévention des attaques par rejeu, telles que l'horodatage et l'utilisation de valeurs sur l'ancienneté des données ;

g) Horodatage des messages et définition de leurs date et heure d'expiration ;

e) S'assurer que, lors de la transmission d'authentifiants ou de toute autre information sensible, les données sont uniquement acceptées si elles utilisent la méthode HTTP « POST » et non la méthode HTTP « GET » ;

g) Toute page qui, de l'avis de l'entreprise ou de l'équipe de développement, n'entre pas dans le cadre de l'authentification devrait être examinée afin d'évaluer toute possibilité de violation de la sécurité.

3.10 Sécurité des logiciels système − acquisition, développement et maintenance

3.10.1 Les points suivants peuvent s'appliquer :

- Utiliser des communications sécurisées pour les mises à jour ;
- Assurer la protection et la signature cryptographiques des mises à jour logicielles ;
- Assurer l'utilisation de modèles et de politiques de configuration ;
- Assurer le contrôle de la configuration et la possibilité d'annuler les mises à jour ;
- Enregistrement de la version et de l'horodatage des mises à jour ;
- Assurer l'authenticité des mises à jour ;
- Établir des procédures sécurisées de mise à jour, y compris des modèles et politiques de configuration ;
- Pour les mises à jour, les applications doivent être examinées et testées pour s'assurer qu'elles n'ont pas d'impact négatif sur la sécurité du véhicule ou de l'organisation.

3.10.1.1 Points liés au « développement de logiciels sécurisés » :

a) Adopter des pratiques de codage sécurisées :

- Veiller à l'absence de portes dérobées de développement/débogage dans le code de production ;
- S'assurer qu'aucune erreur système ne peut être renvoyée à l'utilisateur, au conducteur ou à l'interface homme-machine ;
- S'assurer que toutes les décisions logiques sont assorties d'une clause par défaut ;

- S’assurer que les répertoires de compilation ne contiennent aucun kit d’environnement de développement ;
- Gestion de la mémoire ;
- Validation des entrées ;
- Codage de sortie ;
- Prévention de la modification du code ;

b) Traitement des erreurs :

- Traitement des erreurs, traitement des exceptions et journalisation ;
- S’assurer que l’application échoue de manière sécurisée et que des options de redondance sont disponibles en cas de défaillance ;
- S’assurer que les ressources sont libérées en cas d’erreur ;
- S’assurer qu’aucune information sensible n’est enregistrée en cas d’erreur ;
- Rechercher tous les appels vers le système d’exploitation sous-jacent ou les appels d’ouverture de fichiers et examiner les possibilités d’erreur ;
- S’assurer que les erreurs des applications sont enregistrées ;

c) Appliquer des techniques de test des logiciels et de vérification de l’intégrité :

- Détecter la présence dans l’application d’une fonction d’enregistrement de débogage susceptible d’enregistrer des données sensibles ;
- Examiner la structure des fichiers. Y a-t-il des composants qui ne devraient pas être directement accessibles à l’utilisateur ?
- Examiner toutes les allocations/désallocations de mémoire ;
- Détecter la présence de SQL dynamique dans l’application et déterminer si elle est vulnérable aux attaques par injection de commandes SQL ;
- Rechercher la présence de code ou de code de test mis en commentaire susceptible de contenir des informations sensibles ;

d) Gestion de session :

- Examiner les invalidations de session ;
- Examiner comment et quand une session est créée pour un utilisateur et comment elle est authentifiée et désauthentifiée ;
- Examiner l’identifiant de la session et vérifier s’il est suffisamment complexe pour assurer la sécurité exigée ;
- Déterminer les actions déclenchées par l’application en cas d’identifiant de session non valide ;
- Déterminer les modalités de gestion des sessions multitraitement/multiutilisateurs ;
- Déterminer le délai d’inactivité des sessions HTTP ;
- Déterminer le mode de fonctionnement de la fonctionnalité de déconnexion.

3.10.1.2 Points liés aux « tests des logiciels sécurisés » :

- Les fonctionnalités de sécurité doivent être testées pendant la phase de développement ;

- Des programmes de tests de réception et des critères connexes devraient être mis en place pour les nouveaux systèmes, les mises à jour et les nouvelles versions de logiciels

3.11 Sécurité des relations avec les fournisseurs

3.11.1 Les orientations relatives au développement distribué spécifiées dans la norme ISO/SAE 21434 peuvent s'appliquer.

3.11.2 Les points suivants peuvent également s'appliquer :

- Les prescriptions de cybersécurité visant à atténuer les risques posés par les produits/systèmes du fournisseur pour les produits/systèmes du constructeur doivent être convenues avec le fournisseur et documentées ;
- Toutes les prescriptions de cybersécurité pertinentes doivent être définies et convenues avec chaque fournisseur susceptible de traiter, stocker, communiquer ou fournir des infrastructures destinées aux constructeurs, ou d'y accéder ;
- Les accords conclus avec les fournisseurs doivent comprendre des prescriptions visant les risques de cybersécurité associés aux services de technologie de l'information et de la communication et à la chaîne d'approvisionnement des produits ;
- Le constructeur doit régulièrement surveiller, examiner et auditer la prestation de services des fournisseurs ;
- Les modifications apportées à la prestation de services par les fournisseurs, y compris l'actualisation et l'amélioration des politiques, procédures et contrôles existants en matière de cybersécurité, doivent être gérées en tenant compte de la criticité des informations, systèmes, composants et processus concernés et de la réévaluation des risques.

3.12 Gestion des incidents de sécurité

3.12.1 Des orientations relatives à la gestion des incidents de cybersécurité au niveau des véhicules spécifiés dans la norme ISO/SAE 21434 peuvent s'appliquer.

3.12.1 Les points suivants peuvent également s'appliquer :

- Les responsabilités et les procédures de gestion devraient être définies afin d'assurer des interventions rapides, efficaces et ordonnées en cas d'incident de cybersécurité ;
- Les incidents de cybersécurité devraient être signalés le plus rapidement possible par les voies hiérarchiques appropriées.

3.13 Échange d'informations

3.13.1 Les orientations relatives à l'échange structuré d'informations figurent dans la série UIT-T X.1500 pour les techniques d'échange structuré d'informations sur la cybersécurité (CYBEX).

3.13.2 Les références suivantes de la série UIT-T X.1500 peuvent être utilisées pour échanger des informations structurées sur la cybersécurité afin d'améliorer la cybersécurité grâce à un échange d'informations cohérent, complet, mondial, opportun et sûr sur les vulnérabilités, les failles, les schémas d'attaque, etc. :

- X.1520 Vulnérabilités et expositions courantes (CVE) ;
- X.1521 Système d'évaluation des vulnérabilités courantes (CVSS) ;
- X.1524 Liste des failles courantes (CWE) ;
- X.1525 Système d'évaluation des failles courantes (CWSS) ;
- X.1544 Liste et classification des schémas d'attaque courants (CAPEC).

Annexe D

Liste des documents de référence

La liste suivante contient des références aux documents qui ont été utilisés lors de la rédaction du présent document :

Rapport de l'ENISA « Cyber Security and Resilience of Smart Cars »	TFCS-03-09
Principes de sécurité du Ministère britannique des transports	TFCS-03-07
Directive de la NHTSA sur la cybersécurité	TFCS-03-08
IPA « Approaches for Vehicle Information Security » (Japon)	TFCS-04-05
Directive de la CEE sur la cybersécurité (ITS/AD)	ECE/TRANS/WP.29/2017/46

SAE J 3061

ISO/SAE 21434 Véhicules routiers − Ingénierie de la cybersécurité (en cours d'élaboration)

ISO/IEC 19790

Série ISO/IEC 27000

ISO/IEC 26262

ISO/IEC 19790 « Exigences de sécurité pour les modules cryptographiques »

US Auto ISAC (rapport préparé par Booz Allen Hamilton)
https://www.automotiveisac.com/best-practices

OWASP

GSMA CLP.11 : Lignes directrices de sécurité IoT et CLP.17 : Évaluation de la sécurité IoT