Nations Unies ECE/TRANS/WP.29/GRVA/2022/5

Conseil économique et social

Distr. générale
12 novembre 2021
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

Douzième session
Genève, 24-28 janvier 2021
Point 5 a) de l'ordre du jour provisoire
Véhicules connectés :
Cybersécurité et protection des données

Proposition de recommandations relatives à des prescriptions uniformes concernant la cybersécurité et les mises à jour logicielles

Communication des experts du groupe de travail informel de la cybersécurité et des questions de sûreté des transmissions sans fil (mises à jour logicielles)*

Le texte ci-après, établi par les experts du groupe de travail informel de la cybersécurité et des questions de sûreté des transmissions sans fil (mises à jour logicielles), est une proposition de recommandations relatives à des prescriptions uniformes concernant la cybersécurité et les mises à jour logicielles répondant aux besoins des Parties contractantes de l'Accord de 1998.

* Conformément au programme de travail du Comité des transports intérieurs pour 2022 tel qu'il figure dans le projet de budget-programme pour 2022 (A/76/6 (Sect. 20), par. 20.76), 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 en vertu de ce mandat.

I. Proposition de recommandations relatives à des prescriptions uniformes concernant la cybersécurité et les mises à jour logicielles des véhicules automobiles

A. Partie I − Introduction

1. Les personnes et les organisations qui participent à la conception, à la fabrication ou à l'assemblage des véhicules à moteur ont un rôle à jouer dans la cybersécurité de ces véhicules.

2. Le présent document donne aux Parties contractantes à l'Accord de 1998 des orientations pour l'élaboration de textes réglementaires ou législatifs relatifs à la cybersécurité des véhicules automobiles ou aux mises à jour logicielles et aux procédures de mise à jour des logiciels des véhicules. L'idée est de rendre possible une approche harmonisée en matière d'adoption de ce type de réglementation ou de législation. À ce titre, les prescriptions techniques énoncées dans le présent document sont aussi conformes que possible aux prescriptions des Règlements ONU n^{os} 155 et 156 qui s'appliquent aux Parties contractantes à l'Accord de 1958 en matière de cybersécurité et de mises à jour logicielles, respectivement. Des références ont été ajoutées entre parenthèses, qui renvoient à la ou aux parties correspondantes du Règlement concerné.

On trouvera dans le présent document des prescriptions techniques relatives au véhicule et aux systèmes de gestion. Les prescriptions techniques relatives aux systèmes de gestion portent sur des éléments extérieurs au véhicule mais nécessaires à la gestion efficace de sa cybersécurité pendant toute sa durée de vie et permettant que les mises à jour logicielles soient correctement évaluées et protégées avant de lui être envoyées.

Il est souhaitable que les prescriptions techniques relatives au véhicule soient à tout le moins adoptées en bloc lors de l'élaboration d'un Règlement ou d'une loi. Les prescriptions relatives au système de gestion devraient également être reprises, dans la mesure du possible. Lorsqu'il n'est pas possible de les reprendre dans un texte réglementaire ou législatif, il est proposé de les adopter en tant que directives nationales, auxquelles les constructeurs automobiles devront se conformer.

On ne trouvera pas dans le présent document de définition des critères d'acceptation ou de critères d'essai pour ces prescriptions.

Les phases du cycle de vie d'un véhicule évoquées dans le présent document ne sont pas définies ; c'est dans le texte réglementaire ou législatif qu'il conviendra de le faire. Ces phases sont régies par des normes internationales comme les normes ISO/SAE 21434 et ISO 24089, qui sont appliquées par l'industrie automobile. Il convient toutefois de noter que la « phase de post-production » désigne tout ce qui se passe après la production d'un véhicule, et que les deux principaux moments à prendre en compte alors sont la fin de vie du véhicule (également appelée « mise hors service ») et la fin de l'assistance qui lui est fournie en matière de cybersécurité. Étant donné que l'Accord de 1998 est destiné à s'appliquer à différents systèmes réglementaires et de mise en œuvre, le groupe de travail informel de la cybersécurité et des questions de sûreté des transmissions sans fil n'a pas défini dans le présent document de durée minimale pour ce qui est de l'assistance au véhicule en matière de cybersécurité.

Le présent document propose une méthode permettant de gérer et de comprendre les informations relatives aux configurations logicielles et matérielles figurant dans la réglementation et la législation, notamment pour ce qui est des systèmes d'un véhicule, eu égard à l'homologation de ce dernier. L'utilisation d'un identifiant spécifique (par exemple le code RxSWIN tel que défini dans le Règlement ONU n^{o} 156) désignant la configuration logicielle et matérielle d'un système donné permet de savoir si une mise à jour logicielle aura des conséquences sur la certification de ce système, car l'identifiant spécifique doit être modifié dans un tel cas. Pour que cette méthode fonctionne, un constructeur automobile doit être en mesure de fournir des informations sur le matériel et le logiciel désignés par un identifiant spécifique donné. Il doit être possible de déterminer de quel logiciel un véhicule donné est équipé afin de vérifier sa conformité à ce que désigne l'identifiant spécifique.

B. Partie II

1. Systèmes de gestion

1.1 Système de gestion de la cybersécurité

1.1.1 Le constructeur du véhicule doit mettre en place un système de gestion de la cybersécurité tout au long des phases suivantes : *(Règlement ONU nº 155, par. 7.2.2.1.)*

a) Phase de développement ;

b) Phase de production ;

c) Phase de postproduction.

1.1.2 Le système de gestion de la cybersécurité doit comprendre des processus visant à : (*Règlement ONU nº 155, par. 7.2.2.2*)

a) Gérer la cybersécurité au niveau de l'entreprise ;

b) Répertorier les risques auxquels les véhicules sont exposés, ce qui inclut la prise en compte des menaces énumérées dans la partie A de l'annexe 1 et d'autres menaces pertinentes ;

c) Apprécier, catégoriser et traiter les risques répertoriés ;

d) Vérifier que les risques répertoriés sont correctement gérés ;

e) Contrôler la cybersécurité d'un véhicule ;

f) S'assurer que l'évaluation des risques est actualisée ;

g) Surveiller et détecter les cyberattaques, les cybermenaces et les vulnérabilités du véhicule et les déjouer ;

h) Évaluer si les mesures mises en œuvre en matière de cybersécurité restent efficaces lorsque de nouvelles cybermenaces ou vulnérabilités sont détectées ;

i) Fournir des données permettant d'analyser les tentatives de cyberattaque et les cyberattaques.

1.1.3 Le système de gestion de la cybersécurité doit garantir que les cybermenaces et les vulnérabilités pour lesquelles une intervention du constructeur a été jugée nécessaire sont atténuées dans un délai raisonnable. (*Règlement ONU nº 155, par. 7.2.2.3*).

1.1.4 Les processus mis en œuvre dans le cadre du système de gestion de la cybersécurité doivent garantir que la surveillance mentionnée à l'alinéa g) du par. 1.1.2 g) est permanente et comprend : (*Règlement ONU nº 155, par. 7.2.2.4*)

a) Les véhicules en circulation ;

b) La capacité d'analyser et de détecter les cybermenaces, les vulnérabilités et les cyberattaques à partir des données et des journaux du véhicule. Cette capacité doit s'exercer dans le respect des droits des propriétaires ou des conducteurs des véhicules en matière de vie privée, en particulier s'agissant du consentement.

1.1.5 Le système de gestion de la cybersécurité doit gérer les relations de dépendance pouvant exister avec les fournisseurs, les prestataires de services ou les sous-entités du constructeur. (*Règlement ONU nº 155, par. 7.2.2.5*).

1.2 Système de gestion des mises à jour logicielles

1.2.1 Le système de gestion des mises à jour logicielles doit comprendre des processus visant à :

a) Étayer les informations relatives aux mises à jour logicielles (*Règlement ONU nº 156, par. 7.1.1.1*) ;

b) Conserver en toute sécurité les informations visées à l'alinéa a) du par. 1.2.1 (*Règlement ONU nº 156, par. 7.1.1.1*) ;

c) Mettre les informations visées à l'alinéa a) du par. 1.2.1 à la disposition des autorités compétentes qui en feront la demande (*Règlement ONU nº 156, par. 7.1.1.1*) ;

d) Doter d'un identifiant unique la version initiale et toutes les versions ultérieures d'un logiciel, y compris les données de validation de l'intégrité, et les composants matériels pertinents des systèmes du véhicule décrits dans la loi ou le règlement (*Règlement ONU nº 156, par. 7.1.1.2*) ;

e) Consulter et actualiser les informations concernant tout identifiant spécifique renvoyant à des informations relatives au logiciel d'un véhicule, avant et après une mise à jour, ce qui inclut la possibilité de mettre à jour les informations concernant les versions du logiciel et les données de validation de l'intégrité de tous les composants logiciels pertinents pour chaque identifiant spécifique utilisé (*Règlement ONU nº 156, par. 7.1.1.3*) ;

f) Vérifier que, lorsque des identifiants spécifiques sont utilisés pour accéder à des informations sur le logiciel d'un véhicule, la ou les versions du logiciel présent sur un composant pertinent du véhicule correspondent à celles qui sont associées à l'identifiant spécifique pertinent (*Règlement ONU nº 156, par. 7.1.1.4*) ;

g) Recenser les interdépendances du système mis à jour avec un ou plusieurs autres systèmes (*Règlement ONU nº 156, par. 7.1.1.5*) ;

h) Recenser les véhicules cibles aux fins d'une mise à jour logicielle (*Règlement ONU nº 156, par. 7.1.1.6*) ;

i) Confirmer la compatibilité d'une mise à jour logicielle avec la configuration du ou des véhicules cibles avant la mise à disposition de la mise à jour logicielle, notamment en évaluant la compatibilité entre la dernière configuration logicielle et matérielle connue du ou des véhicules cibles et la mise à jour logicielle à mettre à disposition (*Règlement ONU nº 156, par. 7.1.1.7*) ;

j) Déterminer si une mise à jour logicielle aura une incidence sur un système faisant l'objet d'un Règlement ou d'une loi, notamment sur l'un quelconque des paramètres utilisés pour définir les systèmes que la mise à jour est susceptible de concerner, ou si celle-ci modifiera tel ou tel paramètre visé par la loi ou le Règlement (*Règlement ONU nº 156, par. 7.1.1.8*) ;

k) Déterminer si une mise à jour logicielle ajoutera, modifiera ou activera une ou plusieurs fonctions qui n'étaient pas présentes ou activées lorsque le véhicule a été certifié conformément au texte réglementaire ou législatif, ou si une mise à jour modifiera ou désactivera tout autre paramètre ou fonction régis par la loi ou le Règlement, et préciser notamment si :

i) Les informations prescrites (par la loi ou le Règlement) concernant le véhicule devront être modifiées ;

ii) Les résultats des essais précédents effectués conformément au texte réglementaire ou législatif ne rendront plus compte du fonctionnement du véhicule après que la modification aura eu lieu ;

iii) Une éventuelle modification des fonctions du véhicule aura une incidence sur la certification du véhicule conformément au texte réglementaire ou législatif (*Règlement ONU nº 156, par. 7.1.1.9*) ;

l) Déterminer si une mise à jour logicielle aura une incidence sur tout autre système requis pour continuer d'utiliser le véhicule en toute sécurité, ou si la mise à jour ajoutera ou modifiera des fonctions propres au véhicule par rapport à la date où il a été certifié ; (*Règlement ONU nº 156, par. 7.1.1.10*) ;

m) Permettre à l'utilisateur du véhicule d'être averti lorsqu'une mise à jour logicielle est effectuée (*Règlement ONU nº 156, par. 7.1.1.11*).

1.2.2 Le constructeur du véhicule doit enregistrer et conserver les informations suivantes pour chaque mise à jour :

a) La documentation sur les processus qu'il met en œuvre pour effectuer les mises à jour logicielles et sur toute norme pertinente appliquée ; (*Règlement ONU nº 156, par. 7.1.2.1*) ;

b) La documentation décrivant la configuration de tout système régi par une loi ou un règlement, avant et après une mise à jour. Celle-ci doit comprendre des codes uniques pour les composants matériels et logiciels du système (y compris pour les différentes versions du logiciel) ainsi que tous les paramètres pertinents du véhicule ou du système. (*Règlement ONU nº 156, par. 7.1.2.2*) ;

c) Lorsque des identifiants spécifiques sont utilisés pour accéder à des informations sur le logiciel des systèmes de commande électronique contribuant aux systèmes ou aux fonctions d'un véhicule décrits dans une loi ou un Règlement, un registre vérifiable donnant des informations sur l'ensemble du logiciel auquel renvoie chaque identifiant spécifique avant et après une mise à jour est créé. Il s'agit notamment des informations sur les versions du logiciel et les données de validation de l'intégrité pour tous les logiciels pertinents. (*Règlement ONU nº 156, par. 7.1.2.3*) ;

d) La liste des véhicules cibles de la mise à jour et la confirmation de la compatibilité de la dernière configuration connue de ces véhicules avec la mise à jour. (*Règlement ONU nº 156, par. 7.1.2.4*) ;

e) La liste de toutes les mises à jour logicielles décrivant : (*Règlement ONU nº 156, par. 7.1.2.5*) :

i) Le but de la mise à jour ;

ii) Les systèmes ou les fonctions du véhicule concernés par la mise à jour ;

iii) Le(s) système(s) ou fonction(s) énumérés au point b) éventuellement exigés par la réglementation ou la législation ;

iv) Lorsque de tels systèmes ou fonctions sont requis, les éventuelles incidences de la mise à jour logicielle sur le respect des prescriptions de la loi ou du Règlement pertinents énumérés au paragraphe 3) ;

v) L'éventuelle incidence de la mise à jour logicielle sur un paramètre énoncé dans la réglementation ou la législation pour un véhicule ou un système de véhicule ;

vi) L'éventuelle demande d'homologation de la mise à jour à faire auprès de l'autorité nationale compétente ;

vii) Le mode et les conditions d'exécution de la mise à jour ;

viii) Les éléments permettant de confirmer que la mise à jour logicielle se fera en toute sécurité ;

ix) Les éléments permettant de confirmer que la mise à jour logicielle a fait l'objet de procédures de vérification et de validation qui ont été satisfaisantes.

1.2.3 Les informations visées au 1.2.2.3 et au 1.2.2.4 doivent être mises à disposition par le constructeur du véhicule (*Règlement ONU nº 156, par. 7.1.1.12*).

1.2.4 En ce qui concerne la sécurité des mises à jour logicielles, le constructeur du véhicule doit prévoir et mettre en œuvre des processus pour (*Règlement ONU nº 156, par. 7.1.3*) :

a) S'assurer de la protection raisonnable des mises à jour logicielles contre toute manipulation avant le lancement de la mise à jour (*Règlement ONU nº 156, par. 7.1.3.1*) ;

b) S'assurer que les processus de mise à jour sont raisonnablement protégés contre toute altération, y compris au stade de l'élaboration de la mise à jour du système (*Règlement ONU nº 156, par. 7.1.3.2*) ;

c) Vérifier que les fonctions et le code informatique du logiciel utilisés sur le véhicule sont appropriés et les valider (*Règlement ONU nº 156, par. 7.1.3.3*).

1.2.5 Pour les véhicules dont les mises à jour peuvent s'effectuer à distance, le constructeur du véhicule doit prévoir et mettre en œuvre des processus pour (*Règlement ONU nº 156, par. 7.1.4*) :

a) Évaluer les mises à jour à distance pour s'assurer qu'elles n'auront aucune incidence sur la sécurité, si elles se font pendant la conduite du véhicule (*Règlement ONU nº 156, par. 7.1.4.1*) ;

b) S'assurer que les mises à jour à distance qui supposent un travail complexe ou faisant appel à des compétences particulières (comme un réétalonnage de capteur post-programmation pour terminer une mise à jour), ne puissent avoir lieu que si elles sont effectuées en présence d'une personne qualifiée pour ce faire, ou sous son contrôle (*Règlement ONU nº 156, par. 7.1.4.2*).

2. Prescriptions applicables au véhicule

2.1 Prescriptions en matière de cybersécurité

2.1.1 Le constructeur doit répertorier les éléments critiques du véhicule concerné, procéder à une appréciation des risques complète pour ce véhicule et traiter ou gérer correctement les risques répertoriés (*Règlement ONU nº 155, par. 7.3.3*).

2.1.1.1 L'appréciation des risques doit tenir compte de chaque élément du véhicule et des interactions entre ces éléments.

2.1.1.2 L'appréciation des risques doit porter sur les interactions avec les systèmes externes.

2.1.1.3 Dans le cadre de l'appréciation des risques, le constructeur du véhicule doit tenir compte des risques liés à toutes les menaces visées dans la partie A de l'annexe 1 ainsi que de tout autre risque pertinent.

2.1.1.4 L'appréciation des risques doit prendre en compte tous les risques liés au fournisseur (*Règlement ONU nº 155, par. 7.3.2*).

2.1.2 Le constructeur doit protéger le véhicule contre les risques répertoriés lors de l'appréciation des risques *(Règlement ONU nº 155, par. 7.3.4.).*

2.1.2.1 Des mesures d'atténuation pertinentes et proportionnées doivent être appliquées pour protéger le véhicule.

2.1.2.2 Les mesures d'atténuation doivent comprendre toutes les mesures mentionnées dans les parties B et C de l'annexe 1 qui sont pertinentes au regard des risques répertoriés. Toutefois, si une mesure d'atténuation mentionnée dans la partie B ou C de l'annexe 1 n'est pas pertinente ou suffisante au regard du risque répertorié, le constructeur du véhicule doit s'assurer qu'une mesure de remplacement appropriée est mise en œuvre.

2.1.2.3 Le constructeur du véhicule doit effectuer des essais appropriés et suffisants afin de s'assurer de l'efficacité des mesures de sécurité mises en œuvre (*Règlement ONU nº 155, par. 7.3.6*).

2.1.3 Le constructeur du véhicule doit mettre en œuvre des mesures appropriées et proportionnées pour sécuriser les environnements du véhicule prévus (le cas échéant) pour le stockage et l'exécution des logiciels, services, applications ou données du marché secondaire (*Règlement ONU nº 155, par. 7.3.5).*

2.1.4 Le constructeur du véhicule doit mettre en œuvre des mesures adaptées au véhicule pour (*Règlement ONU nº 155, par. 7.3.7*) :

a) Détecter et prévenir les cyberattaques contre le véhicule ;

b) Renforcer ses propres capacités de surveillance afin de détecter les menaces, vulnérabilités et cyberattaques qui concernent le véhicule ;

c) Disposer des capacités de traitement des données permettant d'analyser les tentatives de cyberattaques et les cyberattaques.

2.1.5 Les modules cryptographiques doivent être conformes aux normes consensuelles. Dans le cas contraire, le constructeur du véhicule doit justifier leur utilisation (*Règlement ONU nº 155, par. 7.3.8*).

2.2 Prescriptions s'appliquant aux mises à jour logicielles

2.2.1 L'authenticité et l'intégrité des mises à jour logicielles doivent être protégées afin de prévenir de façon raisonnable l'altération des mises à jour et d'éviter les mises à jour non valables (*Règlement ONU nº 156, par. 7.2.1.1*).

2.2.2 Lorsque des identifiants spécifiques sont utilisés pour accéder à des informations sur le logiciel des systèmes de commande électronique contribuant aux systèmes ou aux fonctions présents sur un véhicule énoncés dans une loi ou dans un Règlement, chaque identifiant spécifique doit être unique. Lorsque le logiciel concerné est modifié par le constructeur du véhicule, l'identifiant spécifique doit être mis à jour si cela a des conséquences sur la certification du véhicule ou de ses systèmes (*Règlement ONU nº 156, par. 7.2.1.2.1*).

2.2.3 Les versions du logiciel des systèmes de commande électronique contribuant aux systèmes ou fonctions d'un véhicule énoncés dans une loi ou dans un Règlement, ou les identifiants spécifiques utilisés pour accéder à des informations relatives à ce logiciel, doivent être aisément lisibles de façon normalisée, au moyen d'une interface de communication électronique présente sur le véhicule. (*Règlement ONU nº 156, par. 7.2.1.2.2*).

2.2.4 Les informations relatives à la configuration du logiciel d'un véhicule doivent être protégées contre toute modification non autorisée. (*Règlement ONU nº 156, par. 7.2.1.2.3*).

2.2.5 Prescriptions additionnelles applicables aux mises à jour à distance (*Règlement ONU nº 156, par. 7.2.2*).

2.2.5.1 Le véhicule doit rétablir un système dans sa version précédente en cas d'échec ou d'interruption d'une mise à jour, ou doit être mis en mode sécurisé après qu'une mise à jour a échoué ou a été interrompue.

2.2.5.2 Les mises à jour logicielles ne peuvent être exécutées que lorsque le véhicule a une réserve d'énergie suffisante pour achever le processus de mise à jour (mais aussi pour un éventuel rétablissement de la version précédente ou pour mettre le véhicule en mode sécurisé).

2.2.5.3 Dans le cas où l'exécution d'une mise à jour peut avoir une incidence sur la sécurité du véhicule, l'état de ce véhicule doit permettre la mise à jour en toute sécurité.

2.2.5.4 L'utilisateur du véhicule doit pouvoir être averti d'une mise à jour avant que celle-ci soit exécutée. Les informations suivantes doivent lui être communiquées :

a) Le but de la mise à jour. L'information donnée peut se rapporter au degré d'importance de la mise à jour et indiquer si cette dernière est faite dans le cadre d'un rappel, ou pour des raisons de sécurité ou de sûreté ;

b) Toutes les modifications apportées aux fonctions du véhicule par cette mise à jour ;

c) Le temps prévu pour l'exécution de la mise à jour ;

d) Toutes les fonctions du véhicule susceptibles de ne pas être disponibles durant l'exécution de la mise à jour ;

e) Toutes les instructions pouvant aider l'utilisateur du véhicule à exécuter la mise à jour en toute sécurité.

Dans le cas de mises à jour groupées ayant un contenu semblable, une même information peut se rapporter à l'ensemble de ces mises à jour.

2.2.5.5 Dans le cas où l'exécution d'une mise à jour pendant la conduite peut comporter des risques, le véhicule doit :

a) Ne pas pouvoir être conduit durant l'exécution de la mise à jour ; ou

b) Empêcher le conducteur d'utiliser une fonction qui aurait une incidence sur la sécurité ou sur la bonne exécution de la mise à jour.

2.2.5.6 Dès que la mise à jour est achevée :

a) L'utilisateur du véhicule doit pouvoir être informé de la réussite (ou de l'échec) de la mise à jour ;

b) L'utilisateur du véhicule doit pouvoir être informé des modifications apportées et, si nécessaire, de l'existence d'une version actualisée du manuel d'utilisation du véhicule.

3. Définitions

3.1 Par « *cybersécurité* », on entend la protection des véhicules routiers et de leurs fonctions contre les cyberattaques visant les composants électriques ou électroniques.

3.2 Par « *exécution* », on entend, dans le contexte des mises à jour logicielles, le processus d'installation et d'activation d'une mise à jour qui a été téléchargée.

3.3 Par « *informations sur la configuration* », on entend les informations permettant de savoir quelles versions des logiciels sont présentes sur le véhicule. Il peut s'agit d'informations détaillées ou d'identifiants désignant spécifiquement des configurations données (le code R_XSWIN).

3.4 Par « *données de validation de l'intégrité* », on entend une représentation des données numériques sur la base de laquelle des comparaisons peuvent être établies pour détecter des erreurs ou des changements dans les données. Elles peuvent inclure des totaux de contrôle et des valeurs de hachage.

3.5 Par « *mesure d'atténuation* », on entend une mesure qui réduit un risque.

3.6 Par « *transmissions sans fil* », on entend toute méthode permettant d'effectuer des transferts de données sans fil au lieu d'utiliser un câble ou une autre connexion locale.

3.7 Par « *risque* », on entend la possibilité qu'une menace donnée exploite les vulnérabilités d'un véhicule et cause ainsi un préjudice à une entreprise ou à une personne.

3.8 Par « *appréciation des risques* », on entend le processus englobant la recherche, la reconnaissance et la description des risques (définition des risques), en vue d'en comprendre la nature et d'en déterminer le niveau (analyse des risques), et la comparaison des résultats de l'analyse des risques aux critères de risque afin de déterminer si les risques ou le niveau de risque sont acceptables ou tolérables (évaluation des risques).

3.9 Par « *mode sécurisé* », on entend un mode de fonctionnement en cas de défaillance d'un élément n'exposant pas à un risque déraisonnable.

3.10 Par « *logiciel* », on entend la partie d'un système de commande électronique constituée de données numériques et d'instructions.

3.11 Par « *mise à jour logicielle* », on entend le programme utilisé pour installer une nouvelle version d'un logiciel comportant une modification des paramètres de configuration.

3.12 Par « *système* », on entend un ensemble de composants ou de sous-systèmes qui assurent une ou plusieurs fonctions.

3.13 Par « *menace* », on entend la source potentielle d'événements indésirables susceptibles de nuire à un système, à une entreprise ou à une personne.

3.14 Par « *utilisateur du véhicule* », on entend une personne qui dirige ou conduit le véhicule, le propriétaire du véhicule, un représentant habilité ou un employé d'un gestionnaire de parc automobile, un représentant habilité ou un employé du constructeur du véhicule, ou un technicien habilité.

3.15 Par « *vulnérabilité* », on entend un point faible d'un élément ou d'une mesure d'atténuation, qui expose un système à une ou plusieurs menaces.

Annexe 1

Liste des menaces et des mesures d'atténuation correspondantes

1. La présente annexe se compose de trois parties. La partie A décrit l'état de référence pour les menaces, vulnérabilités et méthodes d'attaque. La partie B décrit les mesures d'atténuation des menaces visant les types de véhicule. La partie C décrit les mesures d'atténuation des menaces visant les zones situées en dehors des véhicules, par exemple les systèmes dorsaux.

2. Les parties A, B et C doivent être prises en compte dans le cadre de l'appréciation des risques et des mesures d'atténuation que les constructeurs de véhicules doivent mettre en œuvre.

3. 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 des parties B et C pour établir un lien entre chaque attaque ou vulnérabilité et les mesures d'atténuation correspondantes.

4. L'analyse des menaces doit également inclure un examen des éventuelles conséquences d'une attaque. Cet examen peut contribuer à déterminer le degré de risque et à 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 et altérer les performances ;

d) Modifier des logiciels sans avoir d'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.

Partie A
Vulnérabilités ou 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 A1.

Tableau A1
Liste 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 liés aux véhicules en circulation	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** (au moyen, par exemple, de clefs USB ou d'autres supports connectés au serveur)
	2	Services d'un serveur dorsal perturbés, entravant 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 liées aux véhicules stockées sur des serveurs dorsaux perdues ou compromises (« violation 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 fournisseurs de services en nuage tiers
			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** (au moyen, par exemple, de clef 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)
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 détournement de session 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'un module de gestion électronique ou du microprogramme de la passerelle
	7	Les informations peuvent être facilement divulguées. Par exemple, les communications peuvent être interceptées ou l'accès non autorisé à des fichiers ou dossiers sensibles peut être rendu possible	7.1	**Interception de l'information**/rayonnements brouilleurs/surveillance des communications
			7.2	Obtention d'un **accès non autorisé** à des fichiers ou à 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

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace				*Exemple de vulnérabilité ou de méthode d'attaque*
	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
	11	Des messages reçus par le véhicule (par exemple, messages X2V ou de diagnostic), ou transmis à l'intérieur de celui-ci, renferment 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 équipementiers 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** (il est donc corrompu), bien que le processus de mise à jour soit intact
			12.4	**Compromission** des clefs cryptographiques du fournisseur du logiciel **visant à 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 qui facilitent les cyberattaques	15	Des acteurs légitimes peuvent prendre des mesures sans avoir conscience que celles-ci sont susceptibles de faciliter 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 à leurs connexions externes	16	La manipulation de la connectivité des fonctions du véhicule permet une cyberattaque, les moyens utilisés comprenant : la télématique, les systèmes 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 marchandises qui y sont 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 Menaces pour les données ou le code du véhicule	19	Extraction des données ou du code du véhicule	19.1	Extraction de logiciels soumis à des droits d'auteur ou propriétaires 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

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace				*Exemple de vulnérabilité ou de méthode d'attaque*
			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**
	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	**Falsification du logiciel** du système de commande ou d'information du véhicule
	24	Perturbation des systèmes ou des opération	24.1	**Déni de service** que l'on peut, par exemple, déclencher sur le réseau interne en inondant un bus CAN, ou en provoquant des pannes sur un module de gestion électronique par l'envoi d'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 du coussin gonflable, 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 vulnérables
			26.3	Utilisation d'algorithmes cryptographiques obsolètes ou sur le point de l'être

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace				*Exemple de vulnérabilité ou de méthode d'attaque*
	27	Des pièces ou des fournitures pourraient être compromises afin que les véhicules puissent être attaqués	27.1	**Matériel ou logiciel que l'on modifie pour permettre une attaque** ou qui ne répond 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, en particulier si l'on n'a pas contrôlé le logiciel 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 modules de gestion électronique 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**, donnant 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 en vue de commettre des actes malveillants, comme l'envoi de messages arbitraires sur le bus CAN
	31	Le transfert involontaire de données est possible	31.1	Atteinte à la sécurité de l'information. Des données personnelles 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 électronique**, par exemple ajout de matériel non autorisé à un véhicule pour permettre une attaque de « l'homme du milieu » **Remplacement de matériel électronique autorisé** (par exemple capteurs) par du matériel électronique non autorisé **Manipulation des informations** recueillies par un capteur (par exemple utilisation d'un aimant pour altérer le capteur à effet Hall relié à la boîte de vitesses)

Partie B
Mesures d'atténuation des menaces visant les véhicules

1. Mesures d'atténuation − « Voies de communication des véhicules »

Les mesures d'atténuation des menaces liées aux voies de communication des véhicules sont indiquées dans le tableau B1.

Tableau B1
Mesures d'atténuation des menaces liées aux voies de communication des véhicules

Référence du tableau A1	*Menace liée 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 (par exemple au moyen de modules matériels de sécurité).
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 M6	Le véhicule doit vérifier l'authenticité et l'intégrité des messages qu'il reçoit. La sécurité doit être prise en compte dans la conception des systèmes afin que les risques soient réduits au minimum.
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'un module de gestion électronique ou du microprogramme de la passerelle		

Référence du tableau A1	*Menace liée aux voies de communication des véhicules*	*Réf.*	*Mesure d'atténuation*
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 à 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 à des données critiques du système. Pour des exemples de contrôles de sécurité, voir OWASP.
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 la surmonter doivent être mises en œuvre.
8.2	Attaque par trou noir, perturbation de la communication entre les véhicules par blocage du transfert de messages vers d'autres véhicules	M13	Des mesures visant à détecter une attaque par déni de service et à la surmonter doivent être mises en œuvre.
9.1	Un utilisateur sans privilèges peut obtenir un accès privilégié, par exemple un accès racine	M9	Des mesures visant à empêcher et à détecter les accès non autorisés doivent être mises en œuvre.
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 équipementiers ou les fournisseurs de composants/systèmes/fonctions)		

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

Les mesures d'atténuation des menaces liées au processus de mise à jour sont indiquées dans le tableau B2.

Tableau B2
Mesures d'atténuation des menaces liées au processus de mise à jour

Référence du tableau A1	*Menace liée 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 (il est donc corrompu), bien que le processus de mise à jour soit intact		
12.4	Compromission des clefs cryptographiques du fournisseur du logiciel visant à 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. Mesures d'atténuation − « Actions humaines non intentionnelles qui facilitent les cyberattaques »

Les mesures d'atténuation des menaces liées aux actions humaines non intentionnelles qui facilitent les cyberattaques sont indiquées dans le tableau B3.

Tableau B3
Mesures d'atténuation des menaces liées aux actions humaines non intentionnelles qui facilitent les cyberattaques

Référence du tableau A1	*Menace liée aux actions humaines non intentionnelles*	*Réf.*	*Mesure d'atténuation*
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 visant à définir et à contrôler les rôles des utilisateurs et les privilèges d'accès doivent être mises en œuvre selon le principe du moindre privilège.
15.2	Les procédures de sécurité définies ne sont pas suivies	M19	Les entreprises doivent s'assurer que les procédures de sécurité sont définies et suivies, notamment pour ce qui est du journal d'actions et des accès réservés à la gestion des fonctions de sécurité.

4. Mesures d'atténuation − « Connectivité et connexions externes »

Les mesures d'atténuation des menaces liées à la connectivité et aux connexions externes sont indiquées dans le tableau B4.

Tableau B4
Mesures d'atténuation des menaces liées à la connectivité et aux connexions externes

Référence du tableau A1	*Menace liée à la connectivité et aux connexions externes*	*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.
16.2	Manipulation de la télématique du véhicule (par exemple, manipulation de la mesure de la température de marchandises qui y sont 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, ils doivent être authentifiés et leur intégrité doit être protégée. Des contrôles de sécurité doivent être réalisés de façon à ce que le risque lié aux logiciels tiers destinés à être installés sur le véhicule ou vraisemblablement susceptibles de l'être soit réduit au minimum.
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. Mesures d'atténuation − « Cibles ou motivations potentielles d'une attaque »

Les mesures d'atténuation des menaces liées aux cibles ou motivations potentielles d'une attaque sont indiquées dans le tableau B5.

Tableau B5
Mesures d'atténuation des menaces liées aux cibles ou motivations potentielles d'une attaque

Référence du tableau A1	*Menace liée aux cibles ou motivations potentielles d'une attaque*	*Réf.*	*Mesure d'atténuation*
19.1	Extraction de logiciels soumis à des droits d'auteur ou propriétaires 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 à 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 (par exemple au moyen de modules matériels de sécurité).
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. Il est possible d'atténuer les attaques qui consistent à manipuler des données et ciblent des capteurs ou des données transmises grâce à un recoupement des données provenant de différentes sources d'information.
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.

Référence du tableau A1	*Menace liée aux cibles ou motivations potentielles d'une attaque*	*Réf.*	*Mesure d'atténuation*
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	Falsification du logiciel du système de commande ou d'information du véhicule		
24.1	Déni de service que l'on peut, par exemple, déclencher sur le réseau interne en inondant un bus CAN, ou en provoquant des pannes sur un module de gestion électronique par l'envoi d'un grand nombre de messages	M13	Des mesures visant à détecter une attaque par déni de service et à la surmonter 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 du coussin gonflable, 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. Mesures d'atténuation − « Vulnérabilités potentielles susceptibles d'être exploitées si elles ne sont pas suffisamment protégées ou réduites »

Les mesures d'atténuation des menaces liées aux vulnérabilités potentielles susceptibles d'être exploitées si elles ne sont pas suffisamment protégées ou réduites sont indiquées dans le tableau B6.

Tableau B6
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 A1	*Menace liée 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 dans le cadre du développement des logiciels et du matériel.
26.2	Recours insuffisant aux algorithmes cryptographiques pour protéger les systèmes vulnérables		
26.3	Utilisation d'algorithmes cryptographiques obsolètes		
27.1	Matériel ou logiciel que l'on modifie pour permettre une attaque ou qui ne répond pas aux critères de conception permettant de bloquer une attaque	M23	Les meilleures pratiques de cybersécurité doivent être suivies dans le cadre du développement des logiciels et du matériel.

Référence du tableau A1	*Menace liée aux vulnérabilités potentielles susceptibles d'être exploitées si elles ne sont pas suffisamment protégées ou réduites*	*Réf.*	*Mesure d'atténuation*
28.1	La présence de bogues logiciels peut être la cause de vulnérabilités potentiellement exploitables, en particulier si l'on n'a pas testé le logiciel 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. Les contrôles en matière de cybersécurité doivent avoir une portée suffisante.
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 modules de gestion électronique ou d'obtenir des privilèges plus élevés		
29.1	Ports Internet superflus laissés ouverts, donnant 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 en vue de commettre des actes malveillants, comme l'envoi de messages arbitraires sur le bus CAN	M23	Les meilleures pratiques de cybersécurité doivent être suivies lors du développement des logiciels et du matériel. Les meilleures pratiques de cybersécurité en matière de conception et d'intégration des systèmes doivent être suivies.

7. Mesures d'atténuation − « Perte de données/violation des données du véhicule »

Les mesures d'atténuation des menaces liées à la perte de données ou à la violation des données du véhicule sont indiquées dans le tableau B7.

Tableau B7
Mesures d'atténuation des menaces liées à la perte de données ou à la violation des données du véhicule

Référence du tableau A1	*Menace liée à la perte de données/ou à la violation des données du véhicule*	*Réf.*	*Mesure d'atténuation*
31.1	Atteinte à la sécurité de l'information. Des données personnelles ou confidentielles 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)	M24	Les meilleures pratiques de protection de l'intégrité et de la confidentialité des données doivent être suivies pour le stockage des données personnelles.

8. Mesures d’atténuation − « Manipulation physique des systèmes en vue de permettre une attaque »

Les mesures d’atténuation des menaces liées à la manipulation physique des systèmes en vue de permettre une attaque sont indiquées dans le tableau B8.

Tableau B8
Mesures d’atténuation des menaces liées à la manipulation physique des systèmes en vue de permettre une attaque

Référence du tableau A1	*Menace liée à la manipulation physique des systèmes en vue de permettre une attaque*	*Réf.*	*Mesure d’atténuation*
32.1	Manipulation du matériel électronique, par exemple ajout de matériel non autorisé à un véhicule pour permettre une attaque de l’homme du milieu	M9	Des mesures visant à empêcher et à détecter les accès non autorisés doivent être prises.

Partie C
Mesures d'atténuation des menaces visant les zones situées en dehors des véhicules

1. Mesures d'atténuation − « Serveurs dorsaux »

Les mesures d'atténuation des menaces liées aux serveurs dorsaux sont indiquées dans le tableau C1.

Tableau C1
Mesures d'atténuation des menaces liées aux serveurs dorsaux

Référence du tableau A1	*Menace liée 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 que le risque d'attaques d'initié soit réduit au minimum.
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 que les accès non autorisés soient réduits au minimum. Pour des exemples de contrôles de sécurité, voir OWASP.
1.3 et 3.4	Accès physique non autorisé au serveur (au moyen, par exemple, de 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.
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 doivent être 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 fournisseurs de services en nuage tiers	M4	Des contrôles de sécurité doivent être réalisés pour que les risques associés à l'informatique en nuage soient réduits au minimum. 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 visant à éviter les atteintes à la sécurité des données doivent être réalisés sur les systèmes dorsaux. Pour des exemples de contrôles de sécurité, voir OWASP.

2. Mesures d'atténuation − « Actions humaines non intentionnelles »

Les mesures d'atténuation des menaces liées aux actions humaines non intentionnelles sont indiquées dans le tableau C2.

Tableau C2
Mesures d'atténuation des menaces liées aux actions humaines non intentionnelles

Référence du tableau A1	*Menace liée aux actions humaines non intentionnelles*	*Réf.*	*Mesure d'atténuation*
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 visant à définir et à contrôler les rôles des utilisateurs et les privilèges d'accès doivent être mises en œuvre selon le principe du moindre privilège.
15.2	Les procédures de sécurité définies ne sont pas suivies	M19	Les entreprises doivent s'assurer que les procédures de sécurité sont définies et suivies, notamment pour ce qui est du journal d'actions et des accès réservés à la gestion des fonctions de sécurité.