Nations Unies ECE/TRANS/WP.29/GRSG/2015/16

Conseil économique et social

Distr. générale
20 février 2015
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 dispositions générales de sécurité

108e session
Genève, 4-8 mai 2015
Point 3 de l'ordre du jour provisoire
Règlement no 39 (Indicateur de vitesse)

Proposition de projet de série 01 d'amendements au Règlement no 39 (Indicateur de vitesse)

Communication de l'expert de la Fédération internationale de l'automobile*

Le texte reproduit ci-après, établi par l'expert de la Fédération internationale de l'automobile (FIA), vise à ajouter d'autres amendements à la proposition soumise par l'expert de la Belgique concernant les prescriptions applicables à l'installation des compteurs kilométriques sur les véhicules (ECE/TRANS/WP.29/GRSG/2015/15). Les modifications qu'il est proposé d'apporter au document ECE/TRANS/WP.29/GRSG/2015/15 sont signalées en caractères gras pour les ajouts ou biffés pour les suppressions.

* Conformément au programme de travail du Comité des transports intérieurs pour la période 2012-2016 (ECE/TRANS/224, par. 94 et ECE/TRANS/2012/12, activité 02.4), le Forum mondial a pour mission d'élaborer, d'harmoniser et de mettre à jour les Règlements en vue d'améliorer les caractéristiques fonctionnelles des véhicules. Le présent document est soumis en vertu de ce mandat.

GE.15-03206 (F) 200315 240315
1503206

Merci de recycler

I. Proposition

Titre du Règlement, modifier comme suit:

«PRESCRIPTIONS UNIFORMES RELATIVES À L'HOMOLOGATION DES VÉHICULES EN CE QUI CONCERNE L'APPAREIL INDICATEUR DE VITESSE **ET LE COMPTEUR KILOMÉTRIQUE**, Y COMPRIS ~~SON~~ **LEUR** INSTALLATION».

Table des matières, annexes, modifier comme suit:

«Annexes

…

Annexe 3 − Mesure de la précision de l'indicateur de vitesse **et du compteur kilométrique** pour contrôle de conformité de la production

Annexe 4 − Essai de protection contre les tentatives de manipulation du compteur kilométrique pour contrôle de conformité de la production

Annexe 5 − Profil de protection contre la fraude au kilométrage sur la base des Critères communs.».

Paragraphe 1, modifier comme suit (y compris la note de bas de page[1]):

«1. DOMAINE D'APPLICATION

Le présent Règlement s'applique à l'homologation des véhicules des catégories L, M et N[1].

[1] Selon la définition ~~de l'annexe 7~~ de la Résolution d'ensemble sur la construction des véhicules (R.E.3) (document ~~TRANS/WP.29/78/Rev.1/Amend.2~~ **ECE/TRANS/WP.29/78/Rev.3, par. 2. − www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29resolutions.html.**».

Paragraphes 2.1 à 2.6, modifier comme suit:

«2.1 "*Homologation du véhicule*", l'homologation d'un type de véhicule en ce qui concerne l'appareil indicateur de vitesse **et le compteur kilométrique**, y compris ~~son~~ **leur** installation.

2.2 "*Type de véhicule en ce qui concerne l'indicateur de vitesse* ***et le compteur kilométrique***", les véhicules ne présentant pas entre eux de différences essentielles, ces différences pouvant porter notamment sur les points suivants:

2.2.1 Les dimensions des pneumatiques choisies dans la gamme des pneumatiques de monte normale;

2.2.2 Le rapport global de transmission, y compris les réducteurs éventuels, à l'indicateur de vitesse;

2.2.3 Le type d'indicateur de vitesse caractérisé par:

2.2.3.1 Les tolérances de son mécanisme de mesure;

2.2.3.2 La constante technique de l'indicateur de vitesse;

2.2.3.3 La gamme de vitesses affichées.

2.2.4 Le type de compteur kilométrique caractérisé par:

2.2.4.1 La constante technique du compteur kilométrique;

2.2.4.2 Le nombre de chiffres affichés.

2.3 "*Pneumatiques de monte normale*", le ou les types de pneumatiques prévus par le constructeur pour le type de véhicule considéré; les pneumatiques neige ne seront pas considérés comme des pneumatiques de monte normale;

2.4 "*Pression normale de marche*", la pression de gonflage à froid préconisée par le constructeur, augmentée de 0,2 bar;

2.5 "*Indicateur de vitesse*", la partie de l'appareil indicateur de vitesse destinée à indiquer au conducteur la vitesse instantanée de son véhicule[2];

2.5.1 "*Tolérances du mécanisme de mesure de l'indicateur de vitesse*", la précision de l'appareil indicateur de vitesse proprement dit, exprimée par les limites supérieure et inférieure de l'indicateur de vitesse pour une gamme de vitesses affichées;

2.5.2 "*Constante technique de l'indicateur de vitesse*", le rapport entre le nombre de tours à l'entrée ou d'impulsions par minute et une certaine vitesse affichée;

2.6 "*Compteur kilométrique*", la partie du système d'information destinée à indiquer au conducteur le nombre de kilomètres effectivement parcourus par son véhicule du fait de toute opération de conduite, et comprenant les instruments (physiques) de mesure, le calculateur, l'unité de stockage et des solutions d'affichage de rechange.

2.6.1 "*Constante technique du compteur kilométrique*", le rapport entre le nombre de tours à l'entrée ou d'impulsions et la distance parcourue par le véhicule.

2.~~6~~**7** "*Véhicule à vide*", le véhicule en ordre de marche, avec le plein de carburant, de liquide de refroidissement et de lubrifiant, les outils de bord et une roue de secours (si elle est fournie de série par le constructeur du véhicule), avec un conducteur d'un poids de 75 kg, sans convoyeur, ni accessoires en option ni chargement.».

Paragraphes 3.1 à 3.2.1, modifier comme suit:

«3.1 La demande d'homologation d'un type de véhicule en ce qui concerne l'appareil indicateur de vitesse **et le compteur kilométrique**, y compris ~~son~~ **leur** installation, est présentée par le constructeur du véhicule ou par son représentant dûment accrédité.

…

3.2.1 description du type de véhicule en ce qui concerne les points mentionnés aux paragraphes 2.2, 2.3, 2.4**,** ~~et~~ 2.5 **et 2.6** ci-dessus; le type de véhicule doit être indiqué.».

[2] Il ne comprend pas la partie d'un tachygraphe indiquant la vitesse et la distance parcourue, si celui-ci satisfait à des prescriptions d'homologation de type, qui définissent un rapport précis entre la vitesse réelle et la vitesse affichée (voir par. 5.3 ci-après).

Paragraphe 4, modifier comme suit:

«4.1 Lorsque le type de véhicule présenté à l'homologation en application du présent Règlement satisfait aux prescriptions dudit Règlement en ce qui concerne l'appareil indicateur de vitesse **et le compteur kilométrique**, y compris ~~son~~ **leur** installation, l'homologation pour ce type de véhicule est accordée.».

Ajouter un nouveau paragraphe, ainsi conçu:

«**5.1 Un indicateur de vitesse et un compteur kilométrique conformes aux prescriptions du présent Règlement doivent être installés à bord du véhicule à homologuer.**».

Les paragraphes 5.1 à 5.3 deviennent les paragraphes 5.2 à 5.4.

Ajouter de nouveaux paragraphes, ainsi conçus:

«**5.5 L'afficheur du compteur kilométrique doit être visible ou accessible pour le conducteur. Il doit pouvoir afficher un nombre entier à six chiffres au moins pour les véhicules des catégories M et N, et à cinq chiffres au moins pour les véhicules de la catégorie L. Les autorités d'homologation de type peuvent néanmoins admettre un nombre entier à cinq chiffres pour les véhicules des catégories M et N aussi, pourvu que l'usage prévu pour le véhicule justifie ce choix. Si le compteur atteint son maximum (par exemple 999 999 km), le défilement de l'afficheur s'arrête.**

5.5.1 **Sur les véhicules destinés à être vendus dans des pays utilisant les unités de mesure anglo-saxonnes, le compteur kilométrique peut être gradué en miles. Le kilométrage total affiché par le compteur kilométrique ne doit pas différer de plus de ± 4 % par rapport au kilométrage réel.**

5.5.2 Les données des compteurs kilométriques doivent être protégées contre les tentatives de manipulation tout au long de la chaîne de traitement (mesure, calcul, stockage, affichage). Les données réelles de kilométrage doivent être stockées de manière sécurisée − conformément aux exigences de sécurité qui figurent dans le profil de protection décrit dans l'annexe 5 − à l'intérieur du véhicule et évaluées conformément à la version 3.1 des Critères communs d'évaluation de la sécurité des technologies de l'information (ci-après «Critères communs»), publiée en septembre 2012. Les Critères communs et leurs modalités d'essai sont acceptés partout dans le monde, accessibles à tout un chacun (voir www.commoncriteriaportal.org) et publiés dans les normes ISO/CEI 15408 et ISO/CEI 18045. Il faut faire en sorte que les manipulations du compteur nécessitent tellement de temps et d'argent qu'elles ne soient plus rentables par rapport à la plus-value escomptée sur le prix de vente, aux risques mortels encourus ou aux dégradations de l'environnement susceptibles d'être causées par un véhicule tout au long de son cycle de vie. Les données relatives au kilométrage contenues dans ces modules de gestion électronique (ECU) doivent être lisibles à partir de la prise de diagnostic embarqué (OBD) à 16 broches installée sur le véhicule, tout en étant protégées en écriture, contre l'écrasement et contre la modification des valeurs. Ces données doivent être accessibles à toutes les parties intéressées, comme les ateliers, les vendeurs de véhicules d'occasion, les automobile clubs ou les autorités. Toute différence entre le kilométrage affiché et le kilométrage stocké dans l'espace sécurisé de l'ECU doit être

signalée au conducteur sur le tableau de bord, par exemple sous la forme d'un message d'erreur ou par l'allumage d'un témoin de défaillance.

5.5.3 **Le kilométrage affiché après une opération de réparation ou de remplacement du compteur kilométrique ou d'un de ses composants doit être identique à celui qui était affiché avant ladite opération, ou additionné, tout au plus, d'un déplacement sur une courte distance. En pareil cas, des contre-mesures à l'efficacité prouvée doivent également être en place pour éviter toute modification ou falsification des valeurs. La constante technique du compteur kilométrique ne peut être modifiée après réparation; le kilométrage réel est stocké à l'intérieur du véhicule de manière sécurisée et protégé contre les tentatives de manipulation. La valeur en question doit être aisément lisible au moyen de dispositifs de diagnostic embarqué, afin de pouvoir la comparer avec la valeur affichée.**».

Ajouter de nouveaux paragraphes, ainsi conçus:

«**10.** **DISPOSITIONS TRANSITOIRES**

10.1 **À compter de la date officielle d'entrée en vigueur de la série 01 d'amendements au présent Règlement, aucune Partie contractante appliquant le présent Règlement ne pourra refuser d'accorder ou refuser d'accepter des homologations de type accordées au titre du présent Règlement modifié par la série 01 d'amendements.**

10.2 **À compter du 1er septembre 2017, les Parties contractantes appliquant le présent Règlement ne pourront accorder de nouvelles homologations de type que si le type du véhicule à homologuer satisfait aux prescriptions du présent Règlement modifié par la série 01 d'amendements.**

10.3 **Les Parties contractantes appliquant le présent Règlement ne doivent pas refuser d'accorder des extensions d'homologations de type à des types existants ayant été homologués au titre d'une précédente série d'amendements au présent Règlement.**

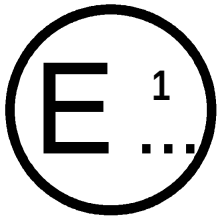
10.4 **À compter de la date d'entrée en vigueur de la série 01 d'amendements au présent Règlement, les Parties contractantes appliquant le présent Règlement devront continuer d'accepter les homologations de type accordées au titre d'une précédente série d'amendements au présent Règlement.**».

Annexes 1 et 2, modifier comme suit:

«Annexe 1

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'appareil indicateur de vitesse **et le compteur kilométrique**, y compris ~~son~~ **leur** installation en application du Règlement n° 39.

N° d'homologation ..... N° d'extension .....

1. Marque de fabrique ou de commerce du véhicule .....
2. Type du véhicule.....
3. Nom et adresse du constructeur .....
4. Le cas échéant, nom et adresse du représentant du constructeur .....
5. Description de l'appareil indicateur de vitesse .....
5.1 Caractéristiques des pneumatiques de monte normale.....
5.2 Caractéristiques des pneus montés pendant l'essai .....
5.3 Rapport d'entraînement de l'appareil indicateur de vitesse .....
6. **Description du compteur kilométrique, preuves d'évaluation incluses**.....
~~6.~~**7.** Masse du véhicule lors de l'essai et répartition de cette masse entre les essieux .....
~~7.~~**8.** Variantes .....
~~8.~~**9.** Véhicule présenté à l'homologation le.....
~~9.~~**10.** Service technique chargé des essais d'homologation.....
~~10.~~**11.** Date du procès-verbal délivré par ce service .....
~~11.~~**12.** Numéro du procès-verbal délivré par ce service .....
~~12.~~**13.** L'homologation est accordée/refusée/étendue/retirée[2].....
~~13.~~**14.** Emplacement, sur le véhicule, de la marque d'homologation.....

~~14.~~**15.** Lieu .....

~~15.~~**16.** Date .....

~~16.~~**17.** Signature .....

---

[1] Numéro distinctif du pays qui a délivré/étendu/refusé/retiré l'homologation (voir les dispositions du Règlement relatives à l'homologation).

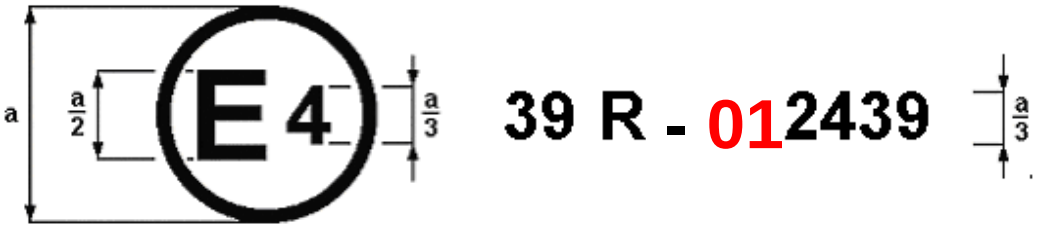
[2] Biffer les mentions inutiles.

Annexe 2

Exemples de marque d'homologation

Modèle A

(voir le paragraphe 4.4 du présent Règlement)

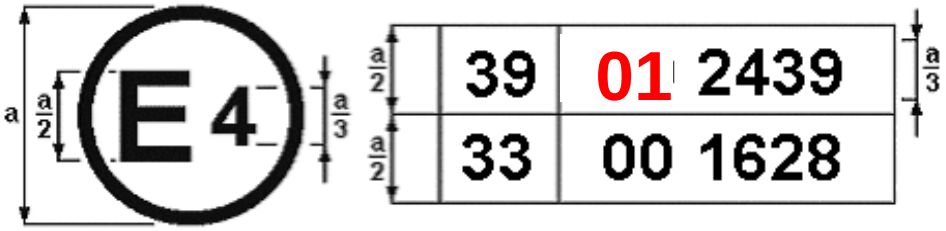


a = 8 mm min.

La marque d'homologation ci-dessus, apposée sur un véhicule, indique que le type de ce véhicule a été homologué aux Pays-Bas (E4), en application du Règlement n° 39. Le numéro d'homologation indique que l'homologation a été accordée conformément aux prescriptions du Règlement n° 39 ~~dans sa forme initiale~~ **modifié par la série 01 d'amendements**.

Modèle B

(voir le paragraphe 4.5 du présent Règlement)



a = 8 mm min.

La marque d'homologation ci-dessus, apposée sur un véhicule, indique que le type de ce véhicule a été homologué aux Pays-Bas (E4), en application des Règlements n^{os} 39 et 33[1]. Les numéros d'homologation indiquent qu'aux dates auxquelles les homologations respectives ont été accordées, le~~s~~ Règlement~~s~~ n^{os} 39 ~~et 33~~ **avait été modifié par la série 01 d'amendements et le Règlement n° 33** étai~~en~~t encore sous ~~leur~~ **sa** forme initiale.

[1] Ce dernier numéro n'est donné qu'à titre d'exemple.».

Ajouter de nouvelles annexes, ainsi conçues:

«Annexe 4

Essai de protection contre les tentatives de manipulation du compteur kilométrique pour contrôle de conformité de la production

(à élaborer)

Annexe 5

Profil de protection contre la fraude au kilométrage sur la base des critères communs

1. Objectif

1.1 La notion de sécurité en ce qui concerne la fraude au kilométrage repose sur un profil de protection qui doit être élaboré par les parties prenantes conformément à la version 3.1 des Critères communs, publiée en septembre 2012 dans la norme ISO/CEI 15408[3].

1.2 Le présent profil de protection a pour objectif de garantir à tout conducteur, acheteur, vendeur, réparateur ou autorité que le kilométrage affiché est bien conforme au kilométrage réel du véhicule résultant de toute opération de conduite.

1.3 Pour atteindre un équilibre économique entre la protection contre la fraude au kilométrage et les avantages à retirer d'une telle fraude, un constructeur peut choisir, pour ses véhicules, le niveau de protection adapté en définissant un objectif de sécurité, sur la base du présent profil de protection. Enfin, un groupe réunira, tous les 24 mois, l'ensemble des parties prenantes pour décider d'une éventuelle actualisation du présent profil de protection en fonction de l'évolution technique.

2. Cible d'évaluation: généralités

Le profil de protection couvre la totalité du système de mesure du kilométrage concerné par la fraude au kilométrage et tout cas pertinent d'utilisation constatée pendant le cycle de vie du véhicule. La cible d'évaluation (TOE) comprend donc plusieurs sous-systèmes qui sont pris en compte dans le présent profil de protection. On peut distinguer quatre sous-systèmes pertinents dans le cadre de la fraude au kilométrage.

2.1 Calcul du kilométrage

Ce sous-système comprend l'ensemble des ECU et des capteurs qui interviennent dans le calcul du kilométrage du véhicule. Les tentatives visant à interrompre la comptabilisation des kilomètres au compteur lors de la conduite, par exemple en falsifiant les signaux transmis aux calculateurs par les

[3] Voir également http://www.commoncriteriaportal.org/.

capteurs des roues, constituent une menace toute particulière qu'il convient de contrer par les mesures imposées dans le cadre du présent profil de protection.

2.2 Stockage des données de kilométrage

Ce sous-système comprend des ECU ou des unités de ces modules dans lesquels est stocké le kilométrage réel. Tant que les exigences fonctionnelles de sécurité et les exigences d'assurance de sécurité du présent profil de protection sont respectées, les constructeurs de véhicules ont toute latitude pour choisir leurs modalités d'application. Ils peuvent décider de stocker le kilométrage dans un ECU prévu à cet effet ou opter pour une stratégie de répartition du stockage et/ou de stockage multiple dans plusieurs ECU afin d'être en mesure de détecter plus facilement toute agression contre un ECU en particulier.

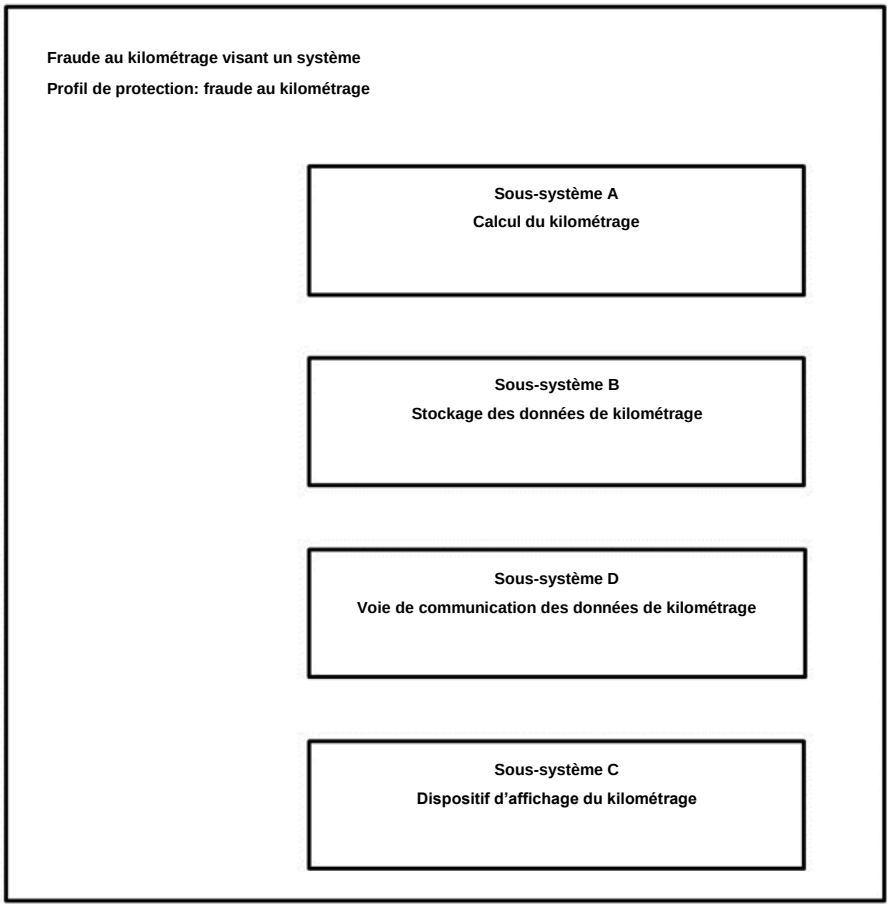
2.3 Dispositif d'affichage du kilométrage

Ce sous-système comprend le dispositif d'affichage utilisé par une partie intéressée pour extraire et afficher le kilométrage réel du véhicule. Il peut s'agir d'un dispositif extérieur agréé utilisé par un atelier et/ou d'un afficheur de bord. Tant que ce sous-système satisfait aux prescriptions du présent profil de protection, chacune de ces options est valable. Du point de vue de la sécurité, il est toutefois bien plus aisé pour un éventuel fraudeur de chercher à manipuler altérer un afficheur intégré directement accessible que de s'attaquer aux valeurs transmises depuis un véhicule vers un dispositif extérieur dont les données ne peuvent être manipulées en amont.

2.4 Voie de communication des données de kilométrage

Ce sous-système comprend la voie de communication et le processus de communication qui servent à transmettre le kilométrage réel au dispositif d'affichage. En tant que quatrième sous-système pertinent dans le dispositif d'ensemble de lutte contre la fraude, cette voie de communication doit également être protégée au titre du présent profil de protection afin de prévenir les fraudes au niveau intermédiaire. Par exemple, si le kilométrage est parfaitement exact et stocké de manière sécurisée dans le véhicule mais que la communication entre l'unité de stockage et le dispositif d'affichage transite par message chiffré via la prise OBD, un fraudeur peut aisément utiliser une solution matérielle à l'intérieur du véhicule pour accéder au bus, intercepter la demande d'extraction des données de kilométrage et falsifier la réponse communiquée au dispositif d'affichage. Les technologies de chiffrement les plus modernes seront donc mises en œuvre dans le cadre du présent profil de protection afin d'assurer la communication entre l'unité de stockage (sous-système B) et le dispositif d'affichage (sous-système C).

Figure 1
Cible d'évaluation (vue d'ensemble du système)



3. Fonctionnement

3.1 Une fois l'unité de stockage des données de kilométrage installée et essayée lors du montage du véhicule, tout déplacement des roues du véhicule, sur la route ou sur un banc d'essai (par exemple lors d'un contrôle technique périodique) fait toujours augmenter le kilométrage stocké dans le sous-système concerné. La valeur enregistrée dans l'unité de stockage ne peut jamais diminuer ou être réinitialisée avec le temps.

3.2 Même en cas de changement de la totalité du sous-système de stockage des données de kilométrage (ce qui peut supposer, selon les modalités d'application du présent profil de protection pour lesquelles le vendeur aura opté, de remplacer un ou plusieurs ECU), il ne faut pas que cette valeur puisse être falsifiée.

3.3 L'objectif global du profil de protection contre la fraude au kilométrage étant de faire en sorte que l'effort à fournir par un fraudeur excède les gains financiers à retirer d'une tentative de manipulation du compteur kilométrique, on pourrait l'atteindre en répartissant le stockage sécurisé des données de kilométrage dans un nombre si important d'ECU qu'il devienne, pour un fraudeur potentiel, inintéressant d'un point de vue économique de remplacer l'ensemble de ces modules, même dans le cas des véhicules haut de gamme.

3.4 Dès qu'un dispositif d'affichage agréé (sous-système C) transmet une commande d'extraction des données de kilométrage par l'intermédiaire de la voie de communication agréée (sous-système D), l'unité de stockage des données de kilométrage (sous-système B) communique le kilométrage réel, calculé et actualisé en permanence par le sous-système de calcul (sous-système A) à toute partie intéressée.

4. Revendication de conformité

4.1 Revendication de conformité

Le présent profil de protection est conforme aux Critères communs d'évaluation de la sécurité des technologies de l'information, (partie 1-3), version 3.1, révision 4 (2012).

4.2 Déclaration de conformité

Tout objectif de sécurité ou profil de protection se réclamant du présent profil de protection doit y être strictement conforme.

Note: en vertu de cette disposition, aucun document présenté par un constructeur automobile au titre d'un objectif de sécurité afin de justifier de l'application du présent profil de protection ne peut servir à imposer des exigences fonctionnelles de sécurité ou des exigences d'assurance de sécurité qui soient plus souples que celles du présent profil de protection.

5. Définition du problème de sécurité

5.1 Principal moyen d'information: kilométrage réel

Note: en raison de la conception du système − se rapporter à l'architecture globale d'un système comprenant quatre sous-systèmes en interaction − la protection de ce moyen d'information passe par la protection d'une série d'autres ressources par les sous-systèmes dont elles relèvent.

À titre d'exemple, l'unité de stockage des données de kilométrage doit protéger au moins les deux ressources suivantes:

a) Les données relatives au kilométrage réel (l'ensemble du système délègue cette fonction de protection à l'unité de stockage); et

b) La clef de chiffrement qu'elle utilise pour communiquer avec le dispositif d'affichage de manière fiable et sécurisée.

5.2 Utilisateurs et agents extérieurs

Une liste énumérant non seulement toutes les personnes qualifiées pour interagir en toute légitimité avec le système, comme les utilisateurs réguliers qui se servent du dispositif d'affichage pour extraire et afficher le kilométrage réel dans un atelier, mais aussi les fraudeurs qui tentent de nuire à l'intégrité du système doit être dressée. Dans le cadre du présent profil de protection, le sous-système de calcul du kilométrage comprend les capteurs des roues; aucun agent extérieur n'est donc décrit ici.

6. Menaces

Les menaces visant les diverses ressources sont libellées, dans le cadre d'un profil de protection, avec le préfixe "T." suivi d'une dénomination unique. Il appartient à l'auteur d'un profil de protection ou d'un objectif de sécurité d'attribuer à une menace le nom de son choix, pourvu qu'il soit unique. Pour le

profil de protection général “fraude au kilométrage”, il s’agit principalement de contrer les menaces suivantes:

6.1 T.Mileage_Corrupted

La valeur affichée par le dispositif d’affichage ne correspond pas au kilométrage réel du véhicule.

Note: cette menace se propage aux sous-systèmes d’un profil de protection sous des formes variées.

6.2 T.Fake_Mileage_Computing

Un fraudeur cherche à émuler et/ou à altérer la comptabilisation du kilométrage transmise par le sous-système “calcul du kilométrage” au sous-système “stockage des données de kilométrage” à des fins d’enregistrement.

6.3 T.Hardware_Memory_Loss

Des fraudeurs sont déjà parvenus à vider une mémoire morte programmable effaçable électriquement (EEPROM), ce qui a entraîné la diminution du kilométrage, puis à la reprogrammer avec une valeur fausse.

6.4 T.Intercepted_Communication

Le sous-système “dispositif d’affichage du kilométrage” est concerné par la menace.

7. Politiques de sécurité des organismes

Les politiques de sécurité sont les règles, procédures, pratiques ou lignes directrices en matière de sécurité qu’un organisme donné impose dans la conduite de ses opérations pour remplir des objectifs de sécurité. Elles peuvent régir la cible d’évaluation (TOE) ou son environnement. Le libellé de ces politiques se compose du préfixe “OSP.” suivi d’une dénomination unique.

7.1 OSP.Audit

Le sous-système “stockage des données de kilométrage” contrôle et signale les échecs d’authentification du dispositif d’affichage du kilométrage.

7.2 OSP.Crypto

Les autorités chargées d’émettre la clé de chiffrage nécessaire à la communication (les centres de gestion de la confidentialité) doivent veiller à ce que les clés destinées aux dispositifs d’affichage du kilométrage ne soient communiquées qu’aux utilisateurs autorisés.

8. Suppositions concernant l’environnement de la TOE

Établir un profil de protection nécessite en outre de dresser une liste de suppositions (préfixe “A.”) concernant l’environnement de la TOE.

8.1 A.System_Activation

Une fois le véhicule monté, les constructeurs du véhicule mettent toujours en service les sous-systèmes de calcul et de stockage des données de kilométrage.

Un tel postulat permet de réduire le nombre des possibilités de fraude qui doivent être prises en compte dans la TOE. L’exemple ci-dessus part du principe qu’il est extrêmement simple, si le sous-système en cause n’est pas mis en service, de conduire le véhicule sans que les kilomètres parcourus soient comptabilisés.

9. Objectifs de sécurité

La liste des objectifs de sécurité arrêtés dans le cadre de la TOE doit être exhaustive afin que chaque menace soit prise en compte par au moins un objectif de sécurité, ce qui permet de ne laisser aucune menace de côté. En outre, il convient de faire l'économie d'objectifs de sécurité superflus afin de limiter les coûts occasionnés et la charge du développement informatique. On utilisera, dans le cadre du profil de protection, une représentation matricielle du rapport m^x n entre les menaces et les objectifs de sécurité afin de tenir compte de ces deux variables. Seront notamment attribués au sous-système "stockage des données de kilométrage" les objectifs suivants.

9.1 O.Access

La TOE doit définir l'accès des utilisateurs aux diverses fonctions (mise en service du stockage des données de kilométrage) et données (kilométrage réel).

9.2 O.Audit

La TOE doit permettre de contrôler les tentatives d'atteinte à la sécurité du système.

9.3 O.Authentication

La TOE devrait permettre d'authentifier les entités en connexion, à savoir les sous-systèmes "calcul du kilométrage" et "dispositif d'affichage du kilométrage".

9.4 O.Integrity

La TOE doit permettre de préserver l'intégrité des données de kilométrage stockées.

9.5 O.Output

La TOE doit permettre de garantir que les données transmises au dispositif d'affichage des données de kilométrage correspondent précisément aux données stockées.

La TOE est protégée contre l'ensemble des menaces énumérées à la condition expresse qu'elle satisfasse à tous les objectifs de sécurité.

10. Exigences de sécurité

10.1 Les exigences de sécurité sont des bonnes pratiques détaillées dans le domaine du développement de systèmes informatiques sécurisés. Le Common Criteria Group a élaboré des séries d'exigences qu'il a classées selon la nomenclature suivante:

- **a) Classes fonctionnelles;**
- **b) Familles fonctionnelles;**
- **c) Composants fonctionnels;**
- **d) Éléments fonctionnels.**

10.2 Les classes fonctionnelles peuvent porter sur les domaines suivants:

- **a) FAU: Audit de sécurité;**
- **b) FDP: Protection des données;**
- **c) FCO: Communication.**

10.3 L'auteur d'un profil de protection peut ainsi aisément sélectionner des exigences de sécurité parmi celles qui sont décrites dans la partie 2 des Critères communs, les adapter à ses besoins et les appliquer. Tout comme il convient d'établir que les diverses menaces sont traitées par des objectifs de sécurité, il est nécessaire de démontrer, par l'intermédiaire d'une matrice, que chaque objectif de sécurité est pris en compte par au moins une des exigences fonctionnelles de sécurité qui figurent dans la liste.

Par exemple, on peut aborder l'objectif "O.Output" en utilisant la classe FCO_NRO.1 qui figure dans le catalogue de la partie 2 des Critères communs.

Le libellé FCO_NRO.1 signifie:

a) FCO (Nom de classe fonctionnelle): Communication;

b) NRO (Nom de famille fonctionnelle): Non-répudiation de l'origine;

c) 1 (Numéro attribué au composant fonctionnel au sein de la famille visée): "Preuve sélective de l'origine".

Si ce composant est sélectionné, le profil de protection impose à tout développeur de coder chacun des trois éléments fonctionnels issus du catalogue. On peut envisager, dans le cas du sous-système "stockage des données de kilométrage", l'exemple suivant:

FCO_NRO.1.1: La TOE doit pouvoir générer la preuve de l'origine du kilométrage réel transmis à la demande du dispositif d'affichage du kilométrage.

Cette fonction, associée aux exigences propres à la classe FCS (support cryptographique), permettra au dispositif d'affichage du kilométrage de se fier à la valeur communiquée par le sous-système de stockage des données de kilométrage et donc de transmettre une valeur correcte à l'utilisateur.

10.4 Les exigences de sécurité sont généralement réparties en deux classes:

a) Les exigences fonctionnelles de sécurité (pratiques optimales) de la partie 2 des Critères communs (ISO/CEI 15408) présentent certaines fonctionnalités de sécurité, comme la vérification des tentatives d'accès ou l'authentification des utilisateurs.

b) Les exigences d'assurance de sécurité, d'un autre côté, définissent les modalités de développement de ces fonctionnalités et la manière dont elles doivent être appliquées au système pour garantir l'élimination de tous les points faibles.

Dans le cadre des Critères communs, les exigences d'assurance sont classées en sept niveaux d'évaluation sécuritaire (EAL) qui déterminent le niveau de l'effort à fournir aux fins du développement informatique et des essais et la rigueur à mettre en œuvre.

En ce qui concerne le profil de protection "fraude au kilométrage", un niveau EAL 4 convient, ce qui suppose d'adopter une approche méthodique du développement et de procéder à des essais fonctionnels de type boîte blanche et boîte noire sans toutefois que pèse la charge du développement formel ou semi formel et des essais qui s'imposent pour les EAL plus élevés.

La protection de l'équipement de contrôle du kilométrage et sa résistance contre les tentatives de manipulation doivent être essayées conformément à la procédure d'évaluation arrêtée dans le cadre des Critères communs (ISO/CEI

15408) et décrite dans les spécifications détaillées concernant les procédures d'essai et d'évaluation, qui figurent dans la "Méthodologie pour l'évaluation de la sécurité des technologies de l'information" (publiée dans la norme ISO/CEI 18045). Y sont, entre autres, définies les modalités d'essai et d'évaluation des points faibles. L'évaluation devrait permettre de vérifier que les manipulations du compteur nécessitent tellement de temps et d'argent qu'elles ne sont plus rentables par rapport à la plus-value escomptée sur le prix de vente, aux risques mortels encourus ou aux dégradations de l'environnement susceptibles d'être causées par un véhicule tout au long de son cycle de vie. Ces méthodes d'essai et d'évaluation sont acceptées partout dans le monde; c'est pourquoi elles ont été normalisées dans ledit document ISO.».

II. Justification

1. La présente proposition vise à compléter le document ECE/TRANS/WP.29/GRSG/2015/15, soumis par l'expert de la Belgique.

2. La fraude au kilométrage provoque des défaillances inattendues qui peuvent être dangereuses, par exemple en produisant des pannes.

3. La fraude au kilométrage va à l'encontre des prescriptions juridiques concernant la durabilité des composants pertinents sur le plan écologique[1] et peut aggraver l'empreinte environnementale des véhicules.

4. La fraude au kilométrage entraîne pour les consommateurs européens un coût économique annuel estimatif compris entre 5,6 et 9,6 milliards d'euros[2]. Les pertes pour les consommateurs se traduisent non seulement par une surcote des véhicules d'occasion, mais aussi par des coûts supplémentaires de réparation et de maintenance. En protégeant les compteurs kilométriques contre les manipulations, on cherche globalement à rendre trop coûteuse la fraude au kilométrage tout au long du cycle de vie du véhicule. Les manipulations du compteur doivent nécessiter tellement de temps et coûter si cher qu'elles ne sont plus rentables par rapport au prix auquel le véhicule peut être vendu pendant sa durée de vie.

5. La fraude au kilométrage est un problème transfrontière qui concerne 5 à 12 % des ventes de voitures d'occasion et 30 à 50 % des transactions transfrontalières[2].

6. Il s'agit de protéger les données de kilométrage au moyen de la méthode fondée sur les Critères communs (norme ISO 15408) décrite dans l'annexe 5, ce qui permet aux autorités d'homologation de type de contrôler les diverses cibles de sécurité des constructeurs dans le cadre d'un profil de protection unique. Le profil de protection du système de contrôle du kilométrage doit être défini en premier lieu par les parties prenantes. Les principales étapes permettant d'élaborer le profil de protection sont décrites dans l'annexe 5, qui devrait servir de guide aux experts auxquels incombe cette tâche.

---

[1] Règlements (CE) n° 698/2008, annexe 1, par. 2.2 et n° 692/2008, annexe VII, par. 1.2 et 1.3.

[2] Dans 25 États membres de l'Union européenne, selon les statistiques de la Commission européenne: Roadworthiness Package, Impact Assessment, p. 17, Bruxelles, 13 juillet 2012.