Nations Unies ECE/TRANS/WP.29/2023/87

Conseil économique et social

Distr. générale
1er septembre 2023
Français
Original : anglais

Commission économique pour l'Europe

Comité des transports intérieurs

Forum mondial de l'harmonisation des Règlements concernant les véhicules

191e session
Genève, 14-16 novembre 2023
Point 2.3 de l'ordre du jour provisoire
Systèmes de transport intelligents et coordination des activités relatives aux véhicules automatisés

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

Communication du Groupe de travail des véhicules automatisés/autonomes et connectés*

Le texte ci-après, adopté par le Groupe de travail des véhicules automatisés/autonomes et connectés (GRVA) à sa seizième session (ECE/TRANS/WP.29/GRVA/16, par. 53), est fondé sur une proposition d'amendement au document ECE/TRANS/WP.29/2022/60, contenue dans le document informel GRVA-16-15. Il est soumis au Forum mondial de l'harmonisation des Règlements concernant les véhicules (WP.29) et au Comité d'administration de l'Accord de 1958 (AC.1) pour examen à leurs sessions de novembre 2023.

* Conformément au programme de travail du Comité des transports intérieurs pour 2023 tel qu'il figure dans le projet de budget-programme pour 2023 (A/77/6 (Sect. 20), par. 20.6), 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.

Partie I − Introduction, lire :

« 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 nos 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, ISO PAS 5112 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 no 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. ».

Annexe 1, partie A, tableau A1, paragraphe 4.3.2, point 4.1, lire :

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			*Exemple de vulnérabilité ou de méthode d'attaque*	
…	…	…	…	…
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 (messages V2X de prise de conscience coopérative (CAM) ou de coordination des manœuvres (MCM), messages GNSS, etc.)
			…	…
…	…	…	…	…

Annexe 1, partie B, tableau B1, point 4.1 des références du tableau A1, lire :

Référence du tableau A1	*Menace liée aux voies de communication des véhicules*	*Réf.*	*Mesure d'atténuation*
4.1	Simulation de messages par usurpation d'identité (messages V2X de prise de conscience coopérative (CAM) ou de coordination des manœuvres (MCM), messages GNSS, etc.)	M10	Le véhicule doit vérifier l'authenticité et l'intégrité des messages qu'il reçoit.
…	…	…	…