Nations Unies ECE/TRANS/WP.29/GRVA/2021/21

Conseil économique et social

Distr. générale
12 juillet 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

Onzième session
Genève, 27 septembre-1er octobre 2021
Point 5 a) de l'ordre du jour provisoire
Véhicules connectés :
Cybersécurité et protection des données

Proposition d'amendements au Règlement ONU nº 155 (Cybersécurité et systèmes de gestion de la cybersécurité) et au document d'interprétation correspondant

Communication des experts du groupe de travail informel de la cybersécurité et des questions de sûreté des transmissions sans fil*

Le texte ci-après a été établi par les experts du groupe de travail informel de la cybersécurité et des questions de sûreté des transmissions sans fil. Il contient une proposition d'amendements au Règlement ONU nº 155, pour adoption comme complément 1 à la version initiale du Règlement. Les modifications qu'il est proposé d'apporter au Règlement ONU nº 155 et au document d'interprétation relatif à cet instrument (ECE/TRANS/WP.29/2021/59) figurent en caractères gras pour les ajouts et biffés pour les suppressions.

* Conformément au programme de travail du Comité des transports intérieurs pour 2021 tel qu'il figure dans le projet de budget-programme pour 2021 (A/75/6 (Sect. 20), par. 20.51), 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

A. Amendements au Règlement ONU nº 155

Paragraphe 7.3.1, lire :

« 7.3.1 Le constructeur doit disposer d'un certificat de conformité valide pour le système de gestion de la cybersécurité correspondant au type de véhicule à homologuer.

Toutefois, pour les homologations de type ~~antérieures au~~ **délivrées pour la première fois avant le** 1er juillet 2024 **et pour toutes les extensions de ces homologations**, s'il peut donner la preuve que le type de véhicule n'a pas pu être développé conformément au système de gestion de la cybersécurité, il doit démontrer que la cybersécurité a été dûment prise en compte pendant la phase de développement du type de véhicule en question. ».

Paragraphe 7.3.4, lire :

« 7.3.4 Le constructeur doit protéger le type de véhicule contre les risques répertoriés dans le cadre de son appréciation des risques et, à cette fin, prendre des mesures d'atténuation proportionnées. Celles-ci doivent comprendre toutes les mesures mentionnées dans les parties B et C de l'annexe 5 qui sont pertinentes au regard des risques répertoriés. Toutefois, si une mesure d'atténuation mentionnée dans la partie B ou C de l'annexe 5 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.

En particulier, pour les homologations de type ~~antérieures au~~ **délivrées pour la première fois avant le** 1er juillet 2024 **et pour toutes les extensions de ces homologations**, le constructeur du véhicule doit s'assurer qu'une mesure de remplacement appropriée est mise en œuvre si une mesure d'atténuation mentionnée dans la partie B ou C de l'annexe 5 n'est pas faisable d'un point de vue technique. Le cas échéant, le constructeur doit communiquer l'évaluation de la faisabilité technique à l'autorité d'homologation. ».

B. Amendements au document d'interprétation du Règlement ONU nº 155 (ECE/TRANS/WP.29/2021/59)

Partie A, 3, paragraphe Y, paragraphes 7.3 à 7.3.1, lire :

« 7.3.1 Le constructeur doit disposer d'un certificat de conformité valable pour le système de gestion de la cybersécurité correspondant au type de véhicule à homologuer.

Toutefois, ~~s'agissant des~~ **pour les** homologations de type ~~antérieures au~~ **délivrées pour la première fois avant le** 1er juillet 2024 **et pour toutes les extensions de ces homologations**, s'il peut donner la preuve que le type de véhicule n'a pas pu être développé conformément au système de gestion de la cybersécurité, il doit démontrer que la cybersécurité a été dûment prise en compte pendant la phase de développement du type de véhicule en question.

Explication de la prescription

Cette prescription vise à vérifier qu'il existe un certificat de conformité du CSMS qui permet d'homologuer tout nouveau type de véhicule et qu'il est approprié pour le type de véhicule considéré.

Il est possible que les architectures mises au point avant la certification du CSMS n'aient pas pu être développées en pleine conformité avec ce système.

Par conséquent, la disposition relative à la prise en compte adéquate de la cybersécurité est bien applicable aux homologations de type délivrées avant le 1er juillet 2024, mais exclusivement pendant la phase de développement. Les phases de production et de post-production des types concernés doivent être pleinement conformes au CSMS certifié.

Les autres modifications ou mises à jour techniques devant entraîner des extensions du type existant au-delà du 1er juillet 2024 doivent être effectuées, autant que possible, conformément aux processus définis dans le CSMS pour la phase de développement. Tout écart par rapport à ces processus doit être expliqué et justifié auprès du service technique ou de l'autorité d'homologation de type, et la direction du constructeur du véhicule doit en assumer la responsabilité, au niveau hiérarchique approprié.

En ce qui concerne les modifications ou les mises à jour, le service technique ou l'autorité d'homologation peuvent confirmer qu'il est possible d'accorder des extensions après le 1er juillet 2024, sur la base de la méthode et des critères publiés par la CEE, conformément au paragraphe 5 du Règlement ONU nº 155.

Précision à prendre en compte :

a) « Correspondant au type de véhicule à homologuer » signifie que le CSMS doit être applicable au type de véhicule à homologuer.

Exemples de documents ou de justificatifs à fournir

Les éléments suivants pourraient servir à mettre en évidence la validité du certificat du CSMS :

b) Le certificat de conformité du CSMS, pour prouver qu'il est encore valable ;

c) La confirmation que le CSMS est appliqué de manière appropriée au type de véhicule et toute autre information nécessaire pour en apporter l'assurance.

d) Des informations sur la manière dont les mises à jour ou les extensions sont gérées au sein du CSMS, pour toute mise à jour d'une homologation de type délivrée avant le 1er juillet 2024. ».

Partie A, 3, paragraphe AB, paragraphe 7.3.4, lire :

« 7.3.4 Le constructeur doit ... qu'une mesure de remplacement appropriée est mise en œuvre.

En particulier, pour les homologations de type ~~antérieures au~~ **délivrées pour la première fois avant le** 1er juillet 2024 **et pour toutes les extensions de ces homologations**, le constructeur du véhicule doit s'assurer qu'une mesure de remplacement appropriée est mise en œuvre si une mesure d'atténuation mentionnée dans la partie B ou C de l'annexe 5 n'est pas faisable d'un point de vue technique. Le cas échéant, le constructeur doit communiquer l'évaluation de la faisabilité technique à l'autorité d'homologation.

Explication de la prescription

Cette prescription vise à permettre de vérifier que le constructeur du véhicule applique les mesures d'atténuation qui s'imposent conformément aux résultats de son appréciation des risques.

Le fabricant ... qui interagissent avec le véhicule.

Les mesures techniques d'atténuation ... d'adopter des technologies de défense nouvelles ou améliorées.

Il est possible que les architectures conçues avant la mise en application du Règlement ONU nº 155 n'aient pas pu être développées de manière à ce que toutes les mesures d'atténuation des parties B et C de l'annexe 5 soient mises en œuvre. Par conséquent, pour les homologations délivrées pour la première fois avant le 1er juillet 2024, d'autres mesures d'atténuation appropriées sont admises pour contrer les risques de cybersécurité répertoriés.

Les autres modifications ou mises à jour techniques devant entraîner des extensions du type existant au-delà du 1er juillet 2024 doivent être effectuées, autant que possible, conformément à l'annexe 5. Il convient dans ce cadre d'étudier les risques et de vérifier qu'ils continuent à être maîtrisés ou réduits. Tout écart par rapport aux prescriptions de l'annexe 5 doit être expliqué et justifié.

En ce qui concerne les modifications ou les mises à jour, le service technique ou l'autorité d'homologation peuvent confirmer qu'ils jugent que les risques sont convenablement maîtrisés, y compris les éventuels écarts, et qu'il est possible d'accorder des extensions après le 1er juillet 2024, sur la base de la méthode et des critères publiés par la CEE, conformément au chapitre 5 du Règlement ONU nº 155.

Précisions à prendre en compte :

a) Les décisions prises par le constructeur au stade de la conception doivent être liées à la stratégie d'évaluation et de gestion des risques. Le constructeur doit être en mesure de justifier la stratégie mise en œuvre ;

b) Le qualificatif "proportionnée" doit être pris en considération lorsqu'on décide s'il faut mettre en œuvre une mesure d'atténuation et laquelle. Si le risque est négligeable, on peut faire valoir qu'aucune mesure ne s'impose ;

c) Protection contre un risque répertorié signifie atténuation de ce risque.

Exemples de documents ou de justificatifs à fournir

Les normes suivantes peuvent être applicables :

...

iii) La raison pour laquelle il est estimé que des mesures d'atténuation ne sont pas nécessaires. ».

II. Justification

1. Le groupe de travail informel de la cybersécurité et des questions de sûreté des transmissions sans fil a examiné, à sa vingt-deuxième session, une demande visant à préciser les dispositions transitoires énoncées aux paragraphes 7.3.1 et 7.3.4 en ce qui concerne les demandes d'extension présentées après le 1er juillet 2024 pour des homologations de type délivrées pour la première fois avant cette date.

2. Le groupe de travail informel a conclu qu'il convenait de modifier a) le Règlement ONU nº 155 (Cybersécurité et systèmes de gestion de la cybersécurité) − voir la partie A du présent document, et b) le document d'interprétation du Règlement ONU nº 155 (ECE/TRANS/WP.29/2021/59) − voir la partie B du présent document, afin de préciser dans quelles circonstances des extensions peuvent être accordées et quelles informations supplémentaires doivent être fournies par le constructeur du véhicule qui fait la demande.

3. En outre, les erreurs de numérotation des paragraphes Y et AB de la partie A, 3 du document d'interprétation du Règlement ONU nº 155 ont été corrigées.