Berne, le 9 août 2024

Instructions relatives à la preuve de la protection contre les cyberattaques (art. 103, al. 5 et 6, OETV)

Vu l'art. 220, al. 4, de l'ordonnance du 19 juin 1995[2] concernant les exigences techniques requises pour les véhicules routiers (OETV), l'OFROU édicte les

instructions

suivantes:

I. Considérants

1. L'art. 103, al. 5 et 6, OETV prévoit que depuis le 1er avril 2024, les véhicules des catégories M et N doivent être conformes au règlement (UE) 2019/2144[3] pour ce qui est de la protection contre les cyberattaques lors de leur première immatriculation en Suisse. Selon l'art. 3*b*, al. 1, OETV, les délais transitoires fixés dans le règlement de l'UE sont applicables. Cela signifie qu'à partir du 7 juillet 2024 (date de l'importation ou de la construction en Suisse), les véhicules mentionnés doivent en principe disposer d'une homologation conforme au règlement CEE-ONU n° 155[4].
2. Selon l'art. 103, al. 5, OETV, un niveau de protection équivalent contre les cyberattaques peut être reconnu pour les véhicules des catégories M_1 et N_1, outre l'exception concernant les petites séries décrite dans la disposition.
3. Le règlement CEE-ONU n° 155, appliqué par plus de 60 États[5], et les réglementations nationales concernant certains marchés (par ex. les États-Unis), d'où proviennent un petit nombre de véhicules importés en Suisse, sont fondés sur la même norme ISO.
4. Les normes ISO sont des normes internationales qui fixent les standards de qualité et de sécurité, facilitant ainsi les échanges internationaux de marchandises et de prestations de service. Les directives de la CEE-ONU[6] pour l'application de son règlement n° 155 se réfèrent à la norme « ISO/SAE 21434:2021 Road vehicles – Cybersecurity engineering ». L'autorité

---

[2] RS **741.41**

[3] Règlement (UE) 2019/2144 du Parlement européen et du Conseil du 27 novembre 2019 relatif aux prescriptions applicables à la réception par type des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, en ce qui concerne leur sécurité générale et la protection des occupants des véhicules et des usagers vulnérables de la route, modifiant le règlement (UE) 2018/858 du Parlement européen et du Conseil et abrogeant les règlements (CE) nº 78/2009, (CE) nº 79/2009 et (CE) nº 661/2009 du Parlement européen et du Conseil et les règlements (CE) nº 631/2009, (UE) nº 406/2010, (UE) nº 672/2010, (UE) nº 1003/2010, (UE) nº 1005/2010, (UE) nº 1008/2010, (UE) nº 1009/2010, (UE) nº 19/2011, (UE) nº 109/2011, (UE) nº 458/2011, (UE) nº 65/2012, (UE) nº 130/2012, (UE) nº 347/2012, (UE) nº 351/2012, (UE) nº 1230/2012 et (UE) 2015/166 de la Commission, JO L 325 du 16.12.2019, p. 1 ; modifié en dernier lieu par le règlement délégué (UE) 2023/2590, JO L, 2023/2590, 22.11.2023

[4] Règlement CEE-ONU n°155 du 22 janvier 2021 sur les prescriptions uniformes concernant l'homologation des véhicules en ce qui concerne la cybersécurité et le système de gestion de la cybersécurité ; modifié par le complément 15, en vigueur depuis le 8 octobre 2022 (Add.154 Amend.1).

[5] ECE/TRANS/WP.29/343/Rev.32/Add.1

[6] Recommendations on uniform provisions concerning cyber security and software updates de la Commission économique pour l'Europe des Nations Unies (United Nations Economic Commission for Europe).

américaine NHTSA[7] a publié elle aussi des meilleures pratiques fondées sur la norme ISO/SAE 21434:2021 (Cybersecurity Best Practices for the Safety of Modern Vehicles, Updated 2022[8]). Si un constructeur de véhicules satisfait à la norme ISO/SAE 21434:2021, la protection contre les cyberattaques est équivalente à celle prévue par le règlement CEE-ONU n° 155.

5. On pouvait donc s'attendre à ce que la preuve d'un niveau de protection équivalent puisse être apportée.

6. Il s'est avéré que l'autorité américaine NHTSA, par exemple, ne contraint pas les constructeurs américains à faire savoir s'ils satisfont à la norme ISO/SAE 21434:2021. Il n'existe donc pas de possibilité d'accès public à l'information dans ce domaine.

7. Selon les informations les plus récentes, la preuve de la protection contre les cyberattaques pour les véhicules issus de marchés tiers hors Union européenne ne peut pas être apportée ou ne peut l'être que moyennant des coûts disproportionnés pour des véhicules individuels.

8. Lors de la révision partielle de l'OETV du 22 décembre 2023, le Conseil fédéral, conscient de certaines difficultés d'homologation, a édicté des dispositions transitoires permettant de dispenser les véhicules des catégories M_1 et N_1 qui ne bénéficient pas d'une réception générale UE de l'obligation de satisfaire à certaines exigences du règlement (UE) 2019/2144 jusqu'à fin 2026 (art. 222*s* OETV). Ces derniers n'ont par exemple pas encore l'obligation d'être équipés d'un système d'enregistrement des données d'événement, d'un système d'aide au freinage d'urgence, d'un système d'urgence de maintien de la trajectoire, d'un système d'alerte de somnolence et de perte d'attention du conducteur, d'un système d'alerte de distraction du conducteur, d'un système de surveillance de la pression des pneumatiques ou d'un système de détection en marche arrière (art. 222*s*, al. 5, OETV) ni de satisfaire à l'exigence de protection contre les mises à jour logicielles non autorisées (art. 222*s*, al. 6 OETV). La preuve de protection contre les cyberattaques n'est pas concernée par la disposition transitoire.

9. Dans les conditions précitées, l'obligation de prouver la protection contre les cyberattaques constitue un obstacle involontaire pour les véhicules issus de pays non européens (par ex. véhicules américains qui n'ont pas été construits pour le marché européen). L'importation et l'immatriculation de ces véhicules seraient de ce fait largement empêchées ou tout du moins entravées malgré les dispositions transitoires.

10. Les dispositions transitoires applicables jusqu'à fin 2026 serviront principalement à permettre aux acteurs économiques concernés de se préparer aux dispositions relatives à la sécurité introduites par le règlement (UE) 2019/2144. Durant cette période, l'immatriculation des véhicules des catégories M_1 et N_1 importés directement de pays non européens, qui n'ont pas été construits pour le marché européen et ne disposent pas d'une réception générale UE sera facilitée.

11. L'UE n'a pas encore adapté les prescriptions concernant la réception individuelle aux nouvelles exigences du règlement (UE) 2019/2144. Les prescriptions actuelles en la matière n'exigent notamment aucune preuve de la cybersécurité pour les véhicules des catégories M_1 et N_1. Les réceptions individuelles UE sont également reconnues en Suisse dans le cadre d'obligations internationales (ARM)[9] et les véhicules en bénéficiant peuvent être immatriculés et circuler en Suisse.

12. Les véhicules dispensés de la réception par type et pour lesquels aucune preuve de cybersécurité n'est apportée jusqu'à fin 2026 ne présentent pas un plus grand risque que les véhicules bénéficiant d'une réception individuelle UE qui sont immatriculés et circulent en

---

[7] National Highway Traffic Safety Administration, part of the U.S. Department of Transportation.

[8] https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022112024-tag.pdf (dernier accès le 11 juillet 2024).

[9] Accord entre la Confédération suisse et la Communauté européenne relatif à la reconnaissance mutuelle en matière d'évaluation de la conformité RS **0.946.526.81**

Suisse. Par ailleurs, la responsabilité individuelle du constructeur en matière de cybersécurité a également prévalu jusqu'ici, sans obligation de preuve.

13. Seront exclus de l'obligation de preuve tous les véhicules dispensés de la réception par type. Cela concerne les importations directes pour un usage personnel au sens de l'art. 4, al. 1, de l'ordonnance du 19 juin 1995[10] sur la réception par type des véhicules routiers (ORT) et, pour des raisons d'égalité de traitement, les véhicules construits en Suisse et dispensés de la réception par type au sens de l'art. 4, al. 3, ORT.

14. Outre les véhicules des catégories M_1 et N_1, ceux de la catégorie N_2 seront également dispensés de l'obligation de preuve de la cybersécurité, à la demande du milieu économique suisse. Il s'est avéré que la capacité des services de contrôle en la matière est également insuffisante dans l'UE. Les États-membres de l'UE sont en mesure de pallier l'engorgement en délivrant des réceptions nationales par type de petites séries, ce qui n'est pas possible en Suisse pour les véhicules dont le poids total dépasse 3,5 t.

15. Le problème de capacité des services de contrôle se pose également pour les trolleybus et les autocars. Les véhicules destinés au trafic de ligne soumis à concession sont tributaires de la concession de l'Office fédéral des transports (OFT) conformément à la loi sur le transport de voyageurs[11]. La concession permet un contrôle supplémentaire et durable du respect des prescriptions techniques. L'OFT doit donc pouvoir décider, au cas par cas, d'une autorisation transitoire.

16. L'art. 220, al. 4, OETV prévoit que l'OFROU peut édicter des instructions en vue de l'exécution de ladite ordonnance. Pour les raisons susmentionnées, les modalités d'exécution lors du contrôle de la preuve de la protection contre les cyberattaques sont fixées de manière uniforme.

II. Instructions à durée déterminée

1. Pour les raisons susmentionnées, il n'y a pas lieu d'exiger la **preuve** de la protection contre les cyberattaques pour l'admission à la circulation des véhicules qui :
   a. ne bénéficient pas d'une réception générale UE,
   b. ont été importés ou construits en Suisse avant le 1er janvier 2027, **et**
   c. remplissent l'une des conditions suivantes :
      i. véhicules des catégories M_1, N_1 et N_2 importés pour un usage personnel conformément à l'art. 4, al. 1, ORT ;
      ii. véhicules des catégories M_1, N_1 et N_2 dispensés de la réception par type conformément à l'art. 4, al. 3, ORT ;
      iii. véhicules destinés au trafic de ligne soumis à concession, pour lesquels l'OFT délivre une autorisation au cas par cas.

2. Les autres conditions d'admission ainsi que les exigences générales d'ordre juridique et technique, notamment celles qui concernent la sécurité du transport et des produits des véhicules ainsi que la protection des données restent applicables. **Les constructeurs et les importateurs sont tenus de garantir un niveau de protection équivalent des véhicules contre les cyberattaques (référence : règlement CEE-ONU n° 155). Ils n'ont simplement pas l'obligation d'en apporter la preuve.**

[10] RS **741.511**

[11] RS **745.1**

III. Entrée en vigueur et validité

1. Les présentes instructions entrent en vigueur rétroactivement au 7 juillet 2024.
2. Elles s'appliquent uniquement aux véhicules cités, qui ont été importés ou construits en Suisse avant le 1er janvier 2027.

Office fédéral des routes

Jürg Röthlisberger
Directeur