4 mars 2021

Accord

Concernant l'adoption de Règlements techniques harmonisés de l'ONU applicables aux véhicules à roues et aux équipements et pièces susceptibles d'être montés ou utilisés sur les véhicules à roues et les conditions de reconnaissance réciproque des homologations délivrées conformément à ces Règlements**

(Révision 3, comprenant les amendements entrés en vigueur le 14 septembre 2017)

Additif 154 − Règlement ONU nº 155

Date d'entrée en vigueur en tant qu'annexe à l'Accord de 1958 : 22 janvier 2021

Prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne la cybersécurité et le système de gestion de la cybersécurité

Le présent document est communiqué uniquement à titre d'information. Le texte authentique, juridiquement contraignant, est celui du document ECE/TRANS/WP.29/2020/79 (tel que modifié par les documents ECE/TRANS/WP.29/2020/94 et ECE/TRANS/WP.29/2020/97).

Nations Unies

* Nouveau tirage pour raisons techniques (20 décembre 2022).

** Anciens titres de l'Accord :
Accord concernant l'adoption de conditions uniformes d'homologation et la reconnaissance réciproque de l'homologation des équipements et pièces de véhicules à moteur, en date, à Genève, du 20 mars 1958 (version originale) ;
Accord concernant l'adoption de prescriptions techniques uniformes applicables aux véhicules à roues, aux équipements et aux pièces susceptibles d'être montés ou utilisés sur un véhicule à roues et les conditions de reconnaissance réciproque des homologations délivrées conformément à ces prescriptions, en date, à Genève, du 5 octobre 1995 (Révision 2).

Règlement ONU nº 155

Prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne la cybersécurité et le système de gestion de la cybersécurité

Table des matières

1. Champ d'application

1.1 Le présent Règlement s'applique aux véhicules des catégories M et N en ce qui concerne la cybersécurité.

Il s'applique également aux véhicules de la catégorie O s'ils sont équipés d'au moins un module de gestion électronique.

1.2 Le présent Règlement s'applique également aux véhicules des catégories L_6 et L_7, s'ils sont équipés de fonctions de conduite automatisée de niveau 3 ou plus, telles que spécifiées dans le Document de référence proposant des définitions de la conduite automatisée dans le cadre du WP.29 et des principes généraux pour l'élaboration d'un Règlement ONU sur les véhicules automatisés (ECE/TRANS/WP.29/1140).

1.3 Le présent Règlement s'entend sans préjudice des autres Règlements ONU et textes législatifs régionaux ou nationaux régissant l'accès des parties autorisées au véhicule et à ses données, fonctions et ressources et les conditions de cet accès. Il s'entend également sans préjudice de l'application de la législation nationale et régionale sur la vie privée et la protection des personnes physiques en ce qui concerne le traitement de leurs données personnelles.

1.4 Le présent Règlement s'entend sans préjudice des autres Règlements ONU et textes législatifs nationaux ou régionaux régissant la conception et l'installation ou l'intégration de pièces et d'éléments de rechange, physiques et numériques, en ce qui concerne la cybersécurité.

2. Définitions

Aux fins du présent Règlement, on entend par :

2.1 « *Type de véhicule* », l'ensemble des véhicules qui ne présentent pas entre eux de différences, au moins au regard des critères de base suivants :

a) La désignation du type de véhicule donnée par le constructeur ;

b) Les aspects essentiels de l'architecture électrique/électronique et des interfaces externes en ce qui concerne la cybersécurité.

2.2 « *Cybersécurité* », la protection des véhicules routiers et de leurs fonctions contre les cyberattaques visant les composants électriques ou électroniques.

2.3 « *Système de gestion de la cybersécurité (CSMS)* », une approche systématique fondée sur les risques et définissant, au niveau organisationnel, les processus, les responsabilités et les mesures de gouvernance dont l'objet est de traiter les risques associés aux cybermenaces visant les véhicules et de protéger ceux-ci contre les cyberattaques.

2.4 « *Système* », un ensemble de composants et/ou de sous-systèmes qui assurent une ou plusieurs fonctions.

2.5 « *Phase de développement* », la période précédant l'homologation de type d'un type de véhicule.

2.6 « *Phase de production* », la durée de production d'un type de véhicule.

2.7 « *Phase de postproduction* », la période pendant laquelle un type de véhicule n'est plus produit, jusqu'à la fin de vie de tous les véhicules de ce type. Les véhicules conformes à un type de véhicule donné restent opérationnels pendant cette phase mais ne sont plus produits. La phase prend fin lorsque plus aucun véhicule d'un type donné n'est opérationnel.

2.8 « *Mesure d'atténuation* », une mesure qui réduit les risques.

2.9 « *Risque* », la possibilité qu'une menace donnée exploite les vulnérabilités d'un véhicule et cause ainsi un préjudice à l'entreprise ou à une personne.

2.10 « *Appréciation des risques* », 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 et/ou leur importance sont acceptables ou tolérables (évaluation des risques).

2.11 « *Gestion des risques* », les activités coordonnées visant à diriger et à piloter une entreprise vis-à-vis des risques.

2.12 « *Menace* », la source potentielle d'événements indésirables susceptibles de nuire à un système, à une entreprise ou à une personne.

2.13 « *Vulnérabilité* », un point faible d'un élément ou d'une mesure d'atténuation, qui l'expose à une ou plusieurs menaces.

3. Demande d'homologation

3.1 La demande d'homologation d'un type de véhicule en ce qui concerne la cybersécurité doit être présentée par le constructeur du véhicule ou par son représentant dûment accrédité.

3.2 Elle doit être accompagnée des pièces mentionnées ci-après, en triple exemplaire, et des informations suivantes :

3.2.1 Une description du type de véhicule en ce qui concerne les points mentionnés à l'annexe 1 du présent Règlement ;

3.2.2 Dans les cas où il est indiqué que les informations font l'objet de droits de propriété intellectuelle, ou qu'elles constituent un savoir-faire spécifique du constructeur ou de ses fournisseurs, le constructeur ou les fournisseurs doivent fournir des éléments d'information suffisants pour permettre d'effectuer convenablement les vérifications mentionnées dans le présent Règlement. Ces éléments d'information doivent être utilisés de façon confidentielle ;

3.2.3 Le certificat de conformité du CSMS, conformément aux dispositions du paragraphe 6 du présent Règlement.

3.3 La documentation doit être fournie en deux parties :

a) Le dossier d'information officiel aux fins de l'homologation, contenant les renseignements énumérés à l'annexe 1, à présenter à l'autorité d'homologation ou à son service technique au moment du dépôt de la demande d'homologation de type. Ce dossier d'information doit être utilisé par l'autorité d'homologation ou son service technique comme référence de base pour la procédure d'homologation. L'autorité d'homologation ou son service technique doit faire en sorte que ce dossier d'information reste disponible pendant au moins 10 ans à compter de la date de l'arrêt définitif de la production du type de véhicule considéré ;

b) Les autres éléments d'information pertinents au regard des prescriptions du présent Règlement, qui peuvent être conservés par le constructeur mais doivent pouvoir faire l'objet d'une inspection au moment de l'homologation de type. Le constructeur doit faire en sorte que toute information pouvant faire l'objet d'une inspection au moment de l'homologation de type reste disponible pendant au moins 10 ans à compter de la date de l'arrêt définitif de la production du type de véhicule considéré.

4. Marquage

4.1 Sur tout véhicule conforme à un type de véhicule homologué en application du présent Règlement doit être apposée de manière visible, en un endroit facilement accessible et indiqué sur la fiche d'homologation, une marque d'homologation internationale composée :

4.1.1 D'un cercle à l'intérieur duquel est placée la lettre « E » suivie du numéro distinctif du pays ayant délivré l'homologation ;

4.1.2 Du numéro du présent Règlement, suivi de la lettre « R », d'un tiret et du numéro d'homologation, à la droite du cercle prévu au paragraphe 4.1.1 ci-dessus.

4.2 Si le véhicule est conforme à un type de véhicule homologué en application d'un ou de plusieurs autres Règlements annexés à l'Accord dans le pays qui a accordé l'homologation en application du présent Règlement, il n'est pas nécessaire de répéter le symbole prescrit au paragraphe 4.1.1 ci-dessus ; dans un tel cas, les numéros de règlement et d'homologation et les symboles additionnels pour tous les Règlements en application desquels l'homologation a été accordée dans le pays qui l'a accordée en application du présent Règlement doivent être inscrits l'un au-dessous de l'autre à droite du symbole prescrit au paragraphe 4.1.1.

4.3 La marque d'homologation doit être nettement lisible et indélébile.

4.4 Elle doit être placée sur la plaque signalétique du véhicule apposée par le constructeur, ou à proximité.

4.5 On trouvera à l'annexe 3 du présent Règlement des exemples de marques d'homologation.

5. Homologation

5.1 Les autorités d'homologation accordent, selon qu'il convient, l'homologation de type en ce qui concerne la cybersécurité, uniquement aux types de véhicules qui satisfont aux prescriptions du présent Règlement.

5.1.1 L'autorité d'homologation ou son service technique doit vérifier les documents attestant que le constructeur a fait le nécessaire, en fonction du type de véhicule, pour :

a) Recueillir et contrôler, tout au long de la chaîne d'approvisionnement, les informations prescrites par le présent Règlement de façon à démontrer que les risques liés aux fournisseurs sont répertoriés et gérés ;

b) Rendre compte de l'appréciation des risques (qui a lieu pendant la phase de développement ou rétrospectivement), des résultats des essais effectués et des mesures d'atténuation prises pour le type de véhicule en question, notamment en fournissant des informations sur la conception à l'appui de l'appréciation des risques ;

c) Mettre en œuvre des mesures de cybersécurité appropriées dans le cadre de la conception du type de véhicule ;

d) Détecter les menaces de cyberattaque et y réagir ;

e) Consigner des données à l'appui de la détection des cyberattaques et disposer des capacités de traitement de données permettant d'analyser les tentatives de cyberattaque et les cyberattaques.

5.1.2 L'autorité d'homologation ou son service technique doit vérifier, en soumettant un véhicule du type concerné aux essais voulus, que le constructeur a bien mis en œuvre les mesures de cybersécurité dont il a fait état. Ces essais

doivent être réalisés par l'autorité d'homologation ou par son service technique ou bien en collaboration avec le constructeur sur la base d'un échantillonnage. L'échantillonnage doit cibler, sans s'y limiter, les risques définis comme élevés pendant l'appréciation des risques.

5.1.3 L'autorité d'homologation ou son service technique doit refuser d'accorder l'homologation de type en ce qui concerne la cybersécurité si le constructeur du véhicule n'a pas satisfait à l'une ou à plusieurs des prescriptions énoncées au paragraphe 7.3, notamment :

a) Si le constructeur n'a pas suivi toutes les étapes de l'appréciation des risques, telle que décrite au paragraphe 7.3.3, par exemple s'il n'a pas tenu compte de tous les risques relatifs aux menaces mentionnées dans la partie A de l'annexe 5 ;

b) Si le constructeur n'a pas protégé le type de véhicule contre les risques répertoriés dans le cadre de son appréciation des risques ou si les mesures d'atténuation proportionnées prescrites au paragraphe 7 n'ont pas été mises en œuvre ;

c) Si le constructeur n'a pas pris les mesures appropriées et proportionnées pour sécuriser les environnements du type du véhicule prévus (le cas échéant) pour le stockage et l'exécution des logiciels, services, applications ou données du marché secondaire ;

d) Si le constructeur n'a pas effectué, avant l'homologation, des essais appropriés et suffisants afin de s'assurer de l'efficacité des mesures de sécurité mises en œuvre.

5.1.4 L'autorité d'homologation en charge de l'évaluation doit également refuser d'accorder l'homologation de type en ce qui concerne la cybersécurité si ni elle ni son service technique n'ont reçu d'informations suffisantes de la part du constructeur pour évaluer la cybersécurité du type de véhicule.

5.2 L'homologation ou l'extension ou le refus d'homologation d'un type de véhicule en application du présent Règlement doit être notifié aux Parties à l'Accord de 1958 appliquant ledit Règlement au moyen d'une fiche conforme au modèle de l'annexe 2 du présent Règlement.

5.3 Les autorités d'homologation ne doivent pas délivrer d'homologation de type sans s'assurer que le constructeur a mis en place des dispositions et des procédures satisfaisantes pour gérer convenablement les aspects de la cybersécurité dont il est question dans le présent Règlement.

5.3.1 L'autorité d'homologation et ses services techniques s'assurent, en sus des critères établis dans l'annexe 2 de l'Accord de 1958 :

a) Qu'ils disposent d'un personnel compétent doté des compétences appropriées en cybersécurité et de connaissances spécifiques en matière d'évaluation des risques dans le secteur automobile[1] ;

b) Qu'ils ont mis en œuvre les procédures relatives à l'évaluation uniforme conformément au présent Règlement.

5.3.2 Chaque Partie contractante appliquant le présent Règlement doit notifier et informer les autorités d'homologation des autres Parties contractantes appliquant le présent Règlement ONU, par l'intermédiaire de son autorité d'homologation, de la méthode et des critères servant de base à cette dernière pour évaluer le caractère approprié des mesures prises conformément au présent Règlement et en particulier aux paragraphes 5.1, 7.2 et 7.3.

[1] Voir par exemple les normes ISO 26262-2018, ISO/PAS 21448 et ISO/SAE 21434.

Ces renseignements doivent être communiqués a) avant la délivrance de la première homologation, seulement, conformément au présent Règlement, et b) chaque fois que la méthode ou les critères d'évaluation sont mis à jour.

Ces renseignements sont destinés à être partagés en vue de la compilation et l'analyse des meilleures pratiques et dans l'optique d'une application convergente des dispositions par toutes les autorités d'homologation qui appliquent le présent Règlement.

5.3.3 Les renseignements visés au paragraphe 5.3.2 doivent être téléchargés en anglais dans la base de données électronique sécurisée DETA[2], établie par la Commission économique pour l'Europe, en temps voulu et au plus tard 14 jours avant la délivrance de la première homologation en application des méthodes et critères d'évaluation pertinents. Les renseignements doivent être suffisants pour permettre de comprendre quels objectifs minimaux l'autorité d'homologation a adoptés pour chaque prescription mentionnée au paragraphe 5.3.2, ainsi que les processus et mesures qu'elle applique pour vérifier que ces objectifs minimaux sont atteints[3].

5.3.4 Lorsqu'elles reçoivent les renseignements visés au paragraphe 5.3.2, les autorités d'homologation peuvent soumettre des observations à l'autorité d'homologation émettrice en les téléchargeant dans la DETA dans un délai de 14 jours suivant la notification.

5.3.5 Si l'autorité d'homologation accordant une homologation ne peut pas tenir compte des observations formulées en vertu du paragraphe 5.3.4, les autorités d'homologation qui les ont transmises et l'autorité d'homologation accordant une homologation doivent demander des éclaircissements en application de l'annexe 6 de l'Accord de 1958. Le groupe de travail subsidiaire[4] du Forum mondial de l'harmonisation des Règlements concernant les véhicules (WP.29) chargé du présent Règlement doit convenir d'une interprétation commune des méthodes et critères d'évaluation[5]. Cette interprétation commune doit être appliquée et toutes les autorités d'homologation doivent délivrer des homologations de type en conséquence, au titre du présent Règlement.

5.3.6 Chaque autorité d'homologation qui délivre une homologation de type en application du présent Règlement doit en notifier les autres autorités d'homologation. L'homologation de type et les documents justificatifs doivent être téléchargés dans la DETA, en anglais, par l'autorité d'homologation, dans les 14 jours suivant la délivrance de ladite homologation[6].

5.3.7 Les Parties contractantes peuvent étudier les homologations délivrées sur la base des renseignements téléchargés en vertu du paragraphe 5.3.6. Toutes divergences de vues éventuelles entre les Parties contractantes doivent être réglées conformément à l'article 10 et à l'annexe 6 de l'Accord de 1958. Les Parties contractantes doivent également informer le groupe de travail subsidiaire compétent du Forum mondial de l'harmonisation des Règlements concernant les véhicules (WP.29) des interprétations divergentes au sens de l'annexe 6 de l'Accord de 1958. Le groupe de travail compétent doit contribuer au règlement des divergences de vues et peut, au besoin, consulter le WP.29 à cet effet. »

---

[2] https://www.unece.org/trans/main/wp29/datasharing.html.

[3] Des lignes directrices concernant les renseignements (méthode, critères et objectifs minimaux, par exemple) à télécharger et le format à utiliser doivent être données dans le document d'interprétation que le groupe de travail informel de la cybersécurité et des questions de sûreté des transmissions sans fil (CS/OTA) prépare pour la septième session du GRVA.

[4] Groupe de travail des véhicules automatisés/autonomes et connectés (GRVA).

[5] Cette interprétation doit être prise en compte dans le document d'interprétation mentionné dans la note de bas de page du paragraphe 5.3.3.

[6] Des renseignements complémentaires sur les prescriptions minimales concernant les documents seront préparés par le GRA durant sa septième session.

5.4 Aux fins du paragraphe 7.2 du présent Règlement, le constructeur doit veiller à ce que les aspects de la cybersécurité dont il est question dans le présent Règlement soient mis en œuvre.

6. Certificat de conformité du système de gestion de la cybersécurité

6.1 Les Parties contractantes doivent désigner une autorité d'homologation chargée de procéder à l'évaluation du constructeur et de délivrer le certificat de conformité du CSMS.

6.2 La demande de certificat de conformité du système de gestion de la cybersécurité doit être présentée par le constructeur du véhicule ou par son représentant dûment accrédité.

6.3 Elle doit être accompagnée des pièces mentionnées ci-après, en triple exemplaire, et des informations suivantes :

6.3.1 Une description du système de gestion de la cybersécurité ;

6.3.2 Une déclaration signée conforme au modèle de l'appendice 1 de l'annexe 1.

6.4 Dans le cadre de l'évaluation, le constructeur doit déclarer, à l'aide du modèle de l'appendice 1 de l'annexe 1, et démontrer à la satisfaction de l'autorité d'homologation ou de son service technique qu'il a mis en place les procédures requises pour satisfaire à toutes les prescriptions en matière de cybersécurité énoncées dans le présent Règlement.

6.5 Si les résultats de cette évaluation sont satisfaisants, et à réception d'une déclaration signée par le constructeur conforme au modèle de l'appendice 1 de l'annexe 1, un certificat appelé « certificat de conformité du CSMS » tel que décrit à l'annexe 4 du présent Règlement est délivré au constructeur.

6.6 L'autorité d'homologation ou son service technique doit établir le certificat de conformité du CSMS en suivant le modèle de l'annexe 4 du présent Règlement.

6.7 Le certificat de conformité du CSMS a une durée de validité de trois ans au maximum à compter de la date de sa délivrance, à moins qu'il ne soit retiré.

6.8 L'autorité d'homologation qui a délivré le certificat de conformité du CSMS peut à tout moment vérifier que les conditions de sa validité restent remplies. L'autorité d'homologation doit retirer le certificat de conformité du CSMS si les prescriptions énoncées dans le présent Règlement ne sont plus respectées.

6.9 Le constructeur doit informer l'autorité d'homologation ou son service technique de toute modification ayant une incidence sur la validité du certificat de conformité du CSMS. Après avoir consulté le constructeur, l'autorité d'homologation ou son service technique doit déterminer s'il convient de procéder à de nouvelles vérifications.

6.10 Le constructeur doit demander un nouveau certificat de conformité du CSMS ou une prolongation du certificat existant en temps voulu, de façon à permettre à l'autorité d'homologation d'achever son évaluation avant la fin de la période de validité du certificat de conformité du CSMS. Sous réserve d'une évaluation favorable, l'autorité d'homologation doit délivrer un nouveau certificat de conformité du CSMS ou prolonger la validité du certificat périmé pour une nouvelle période de trois ans. L'autorité d'homologation doit vérifier que le CSMS est toujours conforme aux prescriptions du présent Règlement. L'autorité d'homologation doit délivrer un nouveau certificat lorsque des modifications ont été portées à son attention ou à celle de son service technique et que ces modifications ont fait l'objet d'une réévaluation favorable.

6.11 L'expiration ou le retrait du certificat de conformité du CSMS accordé au constructeur doit faire l'objet d'un examen compte tenu du type de véhicules pour lesquels le CSMS concerné était pertinent, en tant que modification de l'approbation, comme indiqué au paragraphe 8, ce qui peut impliquer le retrait de l'homologation si les conditions d'octroi ne sont plus remplies.

7. Spécifications

7.1 Spécifications générales

7.1.1 Les prescriptions du présent Règlement ne limitent pas les dispositions ou prescriptions d'autres Règlements ONU.

7.2 Prescriptions relatives au système de gestion de la cybersécurité

7.2.1 Aux fins de l'évaluation, l'autorité d'homologation ou son service technique doit vérifier que le constructeur du véhicule dispose d'un système de gestion de la cybersécurité et que celui-ci est conforme au présent Règlement.

7.2.2 Le système de gestion de la cybersécurité doit couvrir les aspects suivants :

7.2.2.1 Le constructeur du véhicule doit démontrer à l'autorité d'homologation ou à son service technique que son système de gestion de la cybersécurité s'applique aux phases suivantes :

a) Phase de développement ;

b) Phase de production ;

c) Phase de postproduction.

7.2.2.2 Le constructeur du véhicule doit démontrer que les processus mis en œuvre dans le cadre de son système de gestion de la cybersécurité garantissent que la sécurité est dûment prise en compte, notamment au regard des risques et mesures d'atténuation énumérés à l'annexe 5. Ces processus comprennent :

a) Les processus mis en œuvre en interne par le constructeur pour gérer la cybersécurité ;

b) Les processus mis en œuvre pour répertorier les risques auxquels chaque type de véhicule est exposé. Dans le cadre de ces processus, les menaces énumérées dans la partie A de l'annexe 5 et les autres menaces pertinentes doivent être prises en compte ;

c) Les processus mis en œuvre pour apprécier, catégoriser et traiter les risques répertoriés ;

d) Les processus en place pour vérifier que les risques répertoriés sont correctement gérés ;

e) Les processus mis en œuvre pour contrôler la cybersécurité d'un type de véhicule ;

f) Les processus mis en œuvre pour garantir que l'appréciation des risques est actualisée ;

g) Les processus mis en œuvre, s'agissant de chaque type de véhicule, pour surveiller et détecter les cyberattaques, les cybermenaces et les vulnérabilités et y réagir, et les processus mis en œuvre pour évaluer si les mesures de cybersécurité prises sont toujours efficaces à la lumière des nouvelles cybermenaces et vulnérabilités qui ont été répertoriées ;

h) Les processus mis en œuvre pour recueillir les données utiles à l'analyse des tentatives de cyberattaque et des cyberattaques.

7.2.2.3 Le constructeur du véhicule doit démontrer que les processus mis en œuvre dans le cadre de son système de gestion de la cybersécurité garantissent que,

sur la base des catégories mentionnées aux alinéas c) et g) du paragraphe 7.2.2.2, les cybermenaces et les vulnérabilités auxquelles il doit réagir sont atténuées dans un délai raisonnable.

7.2.2.4 Le constructeur du véhicule doit démontrer que les processus mis en œuvre dans le cadre de son système de gestion de la cybersécurité garantissent que la surveillance mentionnée à l'alinéa g) du paragraphe 7.2.2.2 est permanente. Cette surveillance doit :

a) Commencer dès la première immatriculation du véhicule ;

b) Permettre 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 conformément au paragraphe 1.3 et dans le respect des droits des propriétaires ou des conducteurs des véhicules en matière de vie privée, en particulier s'agissant du consentement.

7.2.2.5 Le constructeur du véhicule doit montrer comment son système de gestion de la cybersécurité gérera les dépendances pouvant exister avec ses fournisseurs, ses prestataires de services ou ses sous-entités en ce qui concerne les prescriptions du paragraphe 7.2.2.2.

7.3 Prescriptions relatives aux types de véhicules

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 1er juillet 2024, si le constructeur 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.

7.3.2 Le constructeur du véhicule doit répertorier et gérer, pour le type de véhicule à homologuer, les risqués liés aux fournisseurs.

7.3.3 Le constructeur doit répertorier les éléments critiques du type de véhicule concerné, procéder à une appréciation des risques complète pour ce type de véhicule et traiter ou gérer correctement les risques répertoriés. L'appréciation des risques doit tenir compte de chaque élément du type de véhicule et des interactions entre ces éléments. Elle doit également porter sur les interactions avec tout système externe. 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 5 ainsi que de tout autre risque pertinent.

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 1er juillet 2024, 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.

7.3.5 Le constructeur du véhicule doit mettre en œuvre des mesures appropriées et proportionnées pour sécuriser les environnements du type du véhicule prévus

(le cas échéant) pour le stockage et l'exécution des logiciels, services, applications ou données du marché secondaire.

7.3.6 Le constructeur du véhicule doit effectuer, avant l'homologation de type, des essais appropriés et suffisants afin de s'assurer de l'efficacité des mesures de sécurité mises en œuvre.

7.3.7 Le constructeur du véhicule doit mettre en œuvre des mesures correspondant au type de véhicule pour :

a) Détecter et prévenir les cyberattaques contre les véhicules de ce type ;

b) Renforcer ses capacités de surveillance aux fins de la détection des menaces, vulnérabilités et cyberattaques qui concernent ce type de véhicule ;

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

7.3.8 Les modules cryptographiques utilisés aux fins du présent Règlement doivent être conformes aux normes consensuelles. Dans le cas contraire, le constructeur du véhicule doit justifier leur utilisation.

7.4 Dispositions relatives à la communication de l'information

7.4.1 Le constructeur du véhicule doit rendre compte, au moins une fois par an et, si nécessaire, plus fréquemment, à l'autorité d'homologation ou à son service technique des résultats de ses activités de surveillance, telles que définies à l'alinéa g) du paragraphe 7.2.2.2, notamment en communiquant des informations relatives aux nouvelles cyberattaques. Le constructeur doit également confirmer à l'autorité d'homologation ou à son service technique que les mesures d'atténuation des cyberattaques mises en œuvre pour les types de véhicules concernés demeurent efficaces, et l'informer des mesures supplémentaires éventuellement prises.

7.4.2 L'autorité d'homologation ou son service technique doit vérifier les informations communiquées et, si nécessaire, demander au constructeur du véhicule de remédier aux faiblesses éventuellement détectées.

Si les informations communiquées ou la réponse apportée ne suffisent pas, l'autorité d'homologation peut décider de retirer le certificat de conformité du CSMS en application du paragraphe 6.8.

8. Modification du type de véhicule et extension de l'homologation de type

8.1 Toute modification du type de véhicule ayant une incidence sur ses caractéristiques techniques en ce qui concerne la cybersécurité et/ou sur la documentation prescrite dans le présent Règlement doit être portée à la connaissance de l'autorité d'homologation ayant délivré l'homologation correspondante. Cette dernière peut alors :

8.1.1 Soit considérer que le véhicule ainsi modifié est toujours conforme aux prescriptions et à la documentation correspondant à l'homologation de type existante ;

8.1.2 Soit réaliser une évaluation complémentaire nécessaire en vertu du paragraphe 5 et exiger, le cas échéant, un nouveau procès-verbal du service technique chargé des essais.

8.1.3 La confirmation, l'extension ou le refus de l'homologation, faisant mention des modifications apportées, doit être notifié au moyen d'une fiche de communication conforme au modèle de l'annexe 2 du présent Règlement. L'autorité d'homologation qui délivre une extension d'homologation doit attribuer un numéro de série à ladite extension et en informer les autres Parties

à l'Accord de 1958 appliquant le présent Règlement au moyen d'une fiche de communication conforme au modèle de l'annexe 2 dudit Règlement.

9. Conformité de la production

9.1 Les procédures relatives à la conformité de la production doivent correspondre à celles qui sont énoncées dans l'annexe 1 de l'Accord de 1958 (E/ECE/TRANS/505/Rev.3) et satisfaire aux prescriptions suivantes :

9.1.1 Le titulaire de l'homologation doit veiller à ce que les résultats des essais de contrôle de la conformité de la production soient enregistrés et que les documents annexés restent disponibles pour une période fixée en accord avec l'autorité d'homologation ou son service technique. Cette période ne doit pas excéder 10 ans à partir de la date de l'arrêt définitif de la production ;

9.1.2 L'autorité qui a accordé l'homologation de type peut à tout moment vérifier les méthodes de contrôle de la conformité appliquées dans chaque unité de production. La fréquence normale de ces vérifications est d'une fois tous les trois ans.

10. Sanctions pour non-conformité de la production

10.1 L'homologation délivrée pour un type de véhicule en application du présent Règlement peut être retirée si les prescriptions énoncées dans ledit Règlement ne sont pas respectées ou si les véhicules prélevés ne satisfont pas auxdites prescriptions.

10.2 Lorsqu'une autorité d'homologation retire une homologation qu'elle avait accordée, elle doit en aviser immédiatement les Parties contractantes appliquant le présent Règlement par l'envoi d'une fiche de communication conforme au modèle de l'annexe 2 dudit Règlement.

11. Arrêt définitif de la production

11.1 Si le titulaire d'une homologation cesse définitivement la production d'un type de véhicule homologué conformément au présent Règlement, il doit en informer l'autorité qui a délivré l'homologation, laquelle, à son tour, avise les Parties à l'Accord appliquant ledit Règlement, au moyen d'une copie de la fiche d'homologation portant à la fin, en gros caractères, la mention signée et datée « PRODUCTION ARRÊTÉE ».

12. Noms et adresses des services techniques chargés des essais d'homologation et des autorités d'homologation de type

12.1 Les Parties à l'Accord appliquant le présent Règlement communiquent au Secrétariat de l'Organisation des Nations Unies les noms et adresses des services techniques chargés des essais d'homologation et des autorités d'homologation de type qui délivrent les homologations et auxquelles doivent être envoyées les fiches d'homologation ou d'extension, de refus ou de retrait d'homologation émises dans les autres pays.

Annexe 1

Fiche de renseignements

Les renseignements ci-dessous doivent, s'il y a lieu, être fournis en triple exemplaire et être accompagnés d'une table des matières. Les schémas, s'il y en a, doivent être fournis à l'échelle appropriée, au format A4 ou pliés à ce format, et être suffisamment détaillés. Les photographies, s'il y en a, doivent être suffisamment détaillées.

1. Marque (raison sociale du constructeur) : .....

2. Type et dénomination(s) commerciale(s) générale(s) : .....

3. Moyen d'identification du type, s'il est indiqué sur le véhicule : .....

4. Emplacement de cette marque : .....

5. Catégorie(s) du véhicule : .....

6. Nom et adresse du constructeur ou de son représentant : .....

7. Nom(s) et adresse(s) de l'atelier (des ateliers) de montage : .....

8. Photographie(s) ou dessin(s) d'un véhicule type : .....

9. Cybersécurité

9.1 Caractéristiques générales de conception du type de véhicule, y compris :

a) Les systèmes du véhicule qui sont pertinents pour la cybersécurité du type de véhicule ;

b) Les composants de ces systèmes qui sont pertinents pour la cybersécurité ;

c) Les interactions de ces systèmes avec d'autres systèmes du type de véhicule et les interfaces externes.

9.2 Représentation schématique du type de véhicule

9.3 Numéro du certificat de conformité du CSMS : .....

9.4 Documents relatifs au type de véhicule à homologuer décrivant les résultats de l'appréciation des risques et les risques répertoriés : .....

9.5 Documents relatifs au type de véhicule à homologuer décrivant les mesures d'atténuation qui ont été mises en œuvre sur les systèmes énumérés ou sur le type de véhicule, et la façon dont elles permettent de gérer les risques répertoriés : .....

9.6 Documents relatifs au type de véhicule à homologuer décrivant la protection des environnements prévus pour les logiciels, services, applications ou données du marché secondaire : .....

9.7 Documents relatifs au type de véhicule à homologuer décrivant les essais qui ont été effectués pour vérifier la cybersécurité du type de véhicule et de ses systèmes et les résultats de ces essais : .....

9.8 Description de la prise en compte de la chaîne d'approvisionnement en ce qui concerne la cybersécurité : .....

Annexe 1 − Appendice 1

Modèle de déclaration de conformité du CSMS à établir par le constructeur

Déclaration du constructeur s'agissant de la conformité du système de gestion de la cybersécurité aux prescriptions y relatives

Nom du constructeur : .....

Adresse du constructeur : .....

..... (*nom du constructeur*) atteste que les processus nécessaires pour satisfaire aux prescriptions relatives au système de gestion de la cybersécurité énoncées au paragraphe 7.2 du Règlement ONU nº 155 sont en place et qu'ils seront maintenus.

Fait à : …… (*lieu*)

Le : .....

Nom du signataire : .....

Fonction du signataire : .....

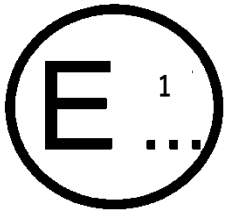
.....

(*Cachet et signature du représentant du constructeur*)

Annexe 2

Fiche de communication

(Format maximal : A4 (210 x 297 mm))



Émanant de : Nom de l'administration :
.....
.....
.....

concernant[8] : Délivrance d'une homologation
Extension d'homologation
Retrait d'homologation avec effet au jj/mm/aaaa
Refus d'homologation
Arrêt définitif de la production

d'un type de véhicule, conformément au Règlement ONU nº 155.

Nº d'homologation : .....

Nº d'extension : .....

Motif de l'extension : .....

1. Marque (raison sociale du constructeur) : .....
2. Type et dénomination(s) commerciale(s) générale(s) : .....
3. Moyen d'identification du type, s'il est indiqué sur le véhicule : .....

3.1 Emplacement de cette marque : .....

4. Catégorie(s) du véhicule : .....
5. Nom et adresse du constructeur ou de son représentant : .....
6. Nom(s) et adresse(s) de l'atelier (des ateliers) de montage : .....
7. Numéro du certificat de conformité du système de gestion de la cybersécurité : .....
8. Service technique chargé des essais : .....
9. Date du procès-verbal d'essai : .....
10. Numéro du procès-verbal d'essai : .....
11. Remarques (le cas échéant) : .....
12. Lieu : .....
13. Date : .....
14. Signature : .....
15. On trouvera en annexe la liste des documents du dossier d'homologation déposé auprès de l'autorité d'homologation, qui peut être obtenu sur demande.

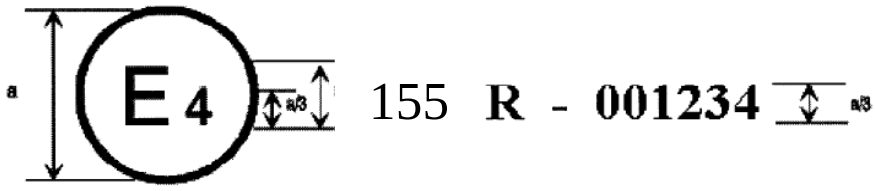
[7] Numéro distinctif du pays qui a accordé/étendu/refusé/retiré l'homologation (voir les dispositions du présent Règlement relatives à l'homologation).

[8] Biffer la mention inutile.

Annexe 3

Exemple de marque d'homologation

Modèle A
(Voir le paragraphe 4.2 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 (E 4), en application du Règlement nº 155, sous le numéro d'homologation 001234. Les deux premiers chiffres du numéro d'homologation (00) signifient que l'homologation a été délivrée conformément aux prescriptions dudit Règlement sous sa forme originale.

Annexe 4

Modèle de certificat de conformité du CSMS

Certificat de conformité du
système de gestion de la cybersécurité

avec le Règlement ONU nº [*le présent Règlement*]

Numéro de certificat [*numéro de référence*]

[……. *autorité d'homologation*]

Certifie que

Nom du constructeur : .....

Adresse du constructeur : .....

est en conformité avec les dispositions du paragraphe 7.2 du Règlement nº 155.

Des contrôles ont été effectués le : .....

par (nom et adresse de l'autorité d'homologation ou du service technique) : .....

Numéro du procès-verbal : .....

Le présent certificat est valable jusqu'au : [… *date*]

Fait à : [……*lieu*]

Le : […….*date*]

[…….*signature*]

Pièces jointes : description du système de gestion de la cybersécurité établie par le constructeur.

Annexe 5

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 des 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)

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			*Exemple de vulnérabilité ou de méthode d'attaque*	
	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)
	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	6.1	Acceptation d'informations provenant d'une **source non fiable**
			6.2	**Attaque de l'homme du milieu**/détournement de session

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			*Exemple de vulnérabilité ou de méthode d'attaque*	
		de session ou aux attaques par rejeu	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
	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

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			*Exemple de vulnérabilité ou de méthode d'attaque*	
			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
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 permettant des opérations 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)

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			*Exemple de vulnérabilité ou de méthode d'attaque*	
			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
			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	**Fabrication du logiciel** du système de commande ou d'information du véhicule
	24	Perturbation des systèmes ou des opérations	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	26	Les technologies cryptographiques peuvent être	26.1	L'utilisation de courtes **clefs cryptographiques** ayant une longue période de validité permet à l'attaquant de casser le cryptage

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			*Exemple de vulnérabilité ou de méthode d'attaque*	
exploitées si elles ne sont pas suffisamment protégées ou réduites		compromises ou ne sont pas suffisamment appliquées	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
	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 aux fins de la protection des données ou du 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		
7.1	Interception de l'information/rayonnements brouilleurs/surveillance des communications	M12	Les données confidentielles reçues et transmises par le véhicule doivent être protégées.

Référence du tableau A1	*Menace liée aux voies de communication des véhicules*	*Réf.*	*Mesure d'atténuation*
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 s'en remettre 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 s'en remettre 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		

Référence du tableau A1	*Menace liée au processus de mise à jour*	*Réf.*	*Mesure d'atténuation*
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.

Référence du tableau A1	*Menace liée à la connectivité et aux connexions externes*	*Réf.*	*Mesure d'atténuation*
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 des modules de sécurité.

Référence du tableau A1	*Menace liée aux cibles ou motivations potentielles d'une attaque*	*Réf.*	*Mesure d'atténuation*
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 afin que les données ou le code du système soient protégés. 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.
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 afin que les données ou le code du système soient protégés. Pour des exemples de contrôles de sécurité, voir OWASP.
23.1	Fabrication 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 s'en remettre 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 afin que les données ou le code du système soient protégés. 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.
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.

Référence du tableau A1	*Menace liée aux serveurs dorsaux*	*Réf.*	*Mesure d'atténuation*
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.

3. Mesures d'atténuation − « Perte physique de données »

Les mesures d'atténuation des menaces liées à la perte physique de données sont indiquées dans le tableau C3.

Tableau C3
Mesures d'atténuation des menaces liées à la perte physique de données

Référence du tableau A1	*Menace liée à la perte physique de données*	*Réf.*	*Mesure d'atténuation*
30.1	Dommages causés par un tiers. Des données sensibles peuvent être perdues ou compromises en raison de dommages matériels subis en cas d'accident de la circulation ou de vol.	M24	Les meilleures pratiques de protection de l'intégrité et de la confidentialité des données doivent être suivies pour le stockage des données personnelles. Pour

30.2	Perte due à des conflits de gestion des droits numériques (DRM). Les données de l'utilisateur peuvent être effacées en raison de problèmes de DRM.		des exemples de contrôles de sécurité, voir ISO/SC27/WG5.
30.3	Des données sensibles (ou leur intégrité) peuvent être perdues en raison de l'usure des composants informatiques, ce qui peut entraîner des problèmes en cascade (en cas de modification des clefs, par exemple)		