Nations Unies ECE/TRANS/WP.29/GRVA/2022/18

Conseil économique et social

Distr. générale
15 juillet 2022
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

Quatorzième session
Genève, 26-30 septembre 2022
Point 5 a) de l'ordre du jour provisoire
Véhicules connectés :
Cybersécurité et protection des données

Proposition d'amendements au document d'interprétation pour le Règlement ONU nº 155 (Cybersécurité et système de gestion de la cybersécurité)

Communication des experts de SAE International*

Le texte ci-après a été établi par les experts de SAE International. Il propose d'apporter des modifications aux références aux normes ISO/SAE 21434:2021 et ISO PAS 5112, ainsi que de préciser l'interprétation de la prescription énoncée à la première ligne du tableau B1 dans l'annexe 5 du Règlement ONU nº 155, concernant l'authentification des messages du Système mondial de navigation par satellite (GNSS). Il est fondé sur le document informel GRVA-13-29 et sur le document ECE/TRANS/WP.29/2022/61.

* Conformément au programme de travail du Comité des transports intérieurs pour 2022 tel qu'il figure dans le projet de budget-programme pour 2022 (A/76/6 (Sect. 20), par. 20.76), 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.

A. Partie A

1. Préambule

1. La partie A du présent document a pour objet de contribuer à préciser les prescriptions des paragraphes 5, 7 et 8 ainsi que de l'annexe 1 du Règlement ONU énonçant des prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne la cybersécurité et de leurs systèmes de gestion de la cybersécurité (Règlement ONU nº 155) ainsi que de communiquer des informations sur les éléments qui peuvent servir à déterminer la mesure dans laquelle ces prescriptions sont satisfaites. Ce document s'adresse aux constructeurs de véhicules qui soumettent des systèmes à l'essai, ainsi qu'aux services techniques et autorités d'homologation chargés d'évaluer ces systèmes. Il devrait contribuer à harmoniser les essais entre les différents services techniques et autorités d'homologation.

2. Note concernant la démonstration du respect des prescriptions

2. Le présent document est purement indicatif. Il renseigne sur les données susceptibles d'être admises par les services techniques et les autorités compétentes et sur le niveau des informations à communiquer. Il n'a pas vocation à être exhaustif. Les normes citées ne le sont qu'à titre d'exemples ; elles ne sont pas obligatoires. Un contrôle de cohérence (voir la section 6, « Lien avec la norme ISO/SAE 21434:2021 ») a néanmoins montré que cette norme en particulier peut se révéler très utile pour appliquer les prescriptions concernant le système de gestion de la cybersécurité tout au long de la chaîne d'approvisionnement. En fonction du type de véhicule défini par le constructeur, ainsi que des pratiques et procédures auxquelles il a recours, des informations autres ou équivalentes peuvent être communiquées.

3. Le respect de toutes les prescriptions applicables au titre du Règlement peut être démontré au moyen de documents ou d'un exposé, ou encore d'un audit. Le type de documentation à fournir n'est pas imposé, mais devrait être convenu entre le constructeur du véhicule et le service technique ou l'autorité d'homologation avant les essais ou les audits. La démonstration peut être apportée par une présentation, des diagrammes et des données d'expérience. Il faut que les arguments à l'appui du respect des prescriptions soient logiques, compréhensibles et convaincants. Les documents ne doivent pas nécessairement être volumineux.

4. Le langage employé dans le présent document se veut conforme aux directives ISO/IEC, deuxième partie, Règles de structure et de rédaction des normes internationales (ISBN 978-92-67-10603-8), décrites à la section 7 de la huitième édition de 2018.

3. Orientations concernant les dispositions du Règlement énonçant des prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne la cybersécurité et de leurs systèmes de gestion de la cybersécurité (Règlement ONU nº 155)

Note : Les paragraphes cités ci-dessous se rapportent aux dispositions du Règlement énonçant des prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne la cybersécurité et de leurs systèmes de gestion de la cybersécurité.

A. Paragraphes 1 à 4 du Règlement

« 1. Champ d'application »

Le présent document ne comporte aucune indication concernant cette prescription.

« 2. Définitions »

Le présent document ne comporte aucune indication concernant cette prescription.

« 3. Demande d'homologation »

Le présent document ne comporte aucune indication concernant cette prescription.

« 4. Marquage »

Le présent document ne comporte aucune indication concernant cette prescription.

B. Paragraphes 5 à 5.3

« 5. Homologation »

« 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. »

Explication de la prescription

Outre les conditions visées au paragraphe 5.1, l'autorité d'homologation est tenue de vérifier si toutes les prescriptions mentionnées à la section 7 du Règlement ont été effectivement respectées. Il s'agit notamment du système de gestion de la cybersécurité mentionné aux paragraphes 7.2 et 7.3.1.

C. Paragraphe 5.3.1, alinéa a)

« 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 matière de cybersécurité et de connaissances spécifiques en matière d'évaluation des risques dans le secteur automobile ; »

Explication de la prescription

Cette prescription implique que l'autorité d'homologation ou le service technique (l'organisation) dispose en nombre suffisant des catégories de personnel suivantes :

a) Personnel compétent et expérimenté en matière de réglementation de la cybersécurité ainsi que de toutes règles, normes et procédures nationales ou émanant d'organisations qui permettent de mettre en œuvre cette cybersécurité. Les normes applicables pourraient être notamment les normes ISO/SAE 21434 et ISO 27001 pour le contenu et certains aspects des normes ISO 19011 et ISO PAS 5112 pour les procédures d'audit ;

b) Personnel compétent et expérimenté en matière d'application de méthodes d'essais en laboratoire, tels que des essais d'intrusion, à données aléatoires ou par canal auxiliaire, en relation avec la cybersécurité du véhicule.

Cette compétence doit être démontrée par des qualifications appropriées ou d'autres preuves de formation équivalentes.

Le Règlement n'impose aucune relation contractuelle particulière entre l'autorité d'homologation ou le service technique et le personnel concerné. Il peut s'agir de contrats de travail, de contrats de service, etc.

L'effectif du personnel concerné doit être proportionné à la charge de travail effective.

Les procédures internes de l'organisation doivent être telles que toutes les tâches au titre du Règlement soient effectuées ou supervisées par un personnel disposant des compétences requises.

D. Paragraphe 5.3.1, alinéa b)

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

Explication de la prescription

L'organisation doit avoir mis en place des procédures attestant que l'évaluation de chaque type de véhicule est menée selon le même schéma. En cas de besoin, l'évaluation peut comporter des variantes, à condition qu'elles soient appliquées selon des critères clairs et qu'elles soient expliquées dans la documentation interne de l'organisation.

Au cas où l'autorité d'homologation a désigné plusieurs services techniques, elle doit assurer l'uniformité d'évaluation entre eux, notamment en organisant des réunions régulières pour qu'ils échangent leurs expériences.

L'organisation doit avoir mis en place des procédures permettant de stocker et de transmettre de manière sécurisée les informations confidentielles.

Les services techniques doivent disposer de processus assurant l'intégrité du personnel qui participe aux évaluations compte tenu des risques encourus.

Il ne suffit pas d'établir les processus et procédures nécessaires pour se décharger des obligations imposées par le Règlement ; il faut également les appliquer de manière effective, ce qui nécessite une formation adéquate et un contrôle de qualité efficace.

Exemples de documents ou de justificatifs permettant de démontrer une mise en œuvre correcte

Documents d'interprétation des services techniques

Lignes directrices de l'autorité d'homologation concernant les meilleures pratiques, sur la base d'une synthèse des interprétations des services techniques.

Comptes rendus de réunions d'échange d'expériences entre l'autorité d'homologation et les services techniques.

E. Paragraphe 5.3.2

« 5.3.2 Chaque Partie contractante appliquant le présent Règlement doit notifier et informer les autorités d'homologation des autres Parties contractantes, 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.

Ces renseignements ne doivent être communiqués qu'avant la délivrance de la première homologation conformément au présent Règlement et 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. »

Explication de la prescription

Cette prescription vise à faire converger les Parties contractantes quant à la manière d'appliquer les prescriptions des paragraphes 5.1, 7.2 et 7.3. Il importe que les alinéas suivants soient interprétés d'une manière qui permette d'atteindre cet objectif. Les échanges doivent en outre favoriser un apprentissage mutuel et la mise sur pied d'un ensemble de meilleures pratiques qui soit susceptible d'inspirer d'autres travaux visant à modifier ultérieurement le Règlement ONU nº 155.

Comme il ressort d'une lecture conjointe des paragraphes 5.3.2 et 5.3.3, les informations sur les méthodes et critères doivent contenir :

a) Les objectifs minimaux que l'autorité d'homologation exigera en regard des spécifications qui figurent aux paragraphes 7.2 et 7.3 ;

b) Les mesures et processus que l'autorité d'homologation ou son service technique appliquera pour vérifier la conformité lors d'une demande d'homologation de type.

Ces informations devront notamment inclure :

c) Les caractéristiques et les critères d'efficacité minimale que les processus décrits au paragraphe 7.2.2.2 devront satisfaire, y compris des informations sur les critères utilisés pour déterminer si les risques évoqués à l'alinéa d) du paragraphe 7.2.2.2 sont « correctement gérés » ;

d) Les critères que l'autorité d'homologation appliquera pour évaluer si les processus mis en œuvre permettent d'atténuer dans un délai raisonnable les cybermenaces et les vulnérabilités évoquées au paragraphe 7.2.2.3, assortis d'informations sur les conditions à remplir pour que ces cybermenaces et vulnérabilités soient considérées comme atténuées ainsi que sur ce que l'on entend par « délai raisonnable » ;

e) Les critères que l'autorité d'homologation appliquera pour évaluer si les processus satisfont aux prescriptions du paragraphe 7.2.2.4 ;

f) Les critères que l'autorité d'homologation appliquera pour évaluer si le constructeur a démontré que le système de gestion de la cybersécurité (CSMS) gère les dépendances mentionnées au paragraphe 7.2.2.5 ;

g) Les critères que l'autorité d'homologation appliquera pour évaluer si le certificat de conformité du CSMS correspond au type de véhicule à homologuer ;

h) Les critères que l'autorité d'homologation appliquera dans le cas des homologations de type antérieures au 1er juillet 2024, pour évaluer si la cybersécurité a été suffisamment prise en compte pendant la phase de développement du type de véhicule en question afin que le degré de performance en la matière soit atteint ;

i) Les critères que l'autorité d'homologation appliquera pour évaluer si le constructeur a pris des mesures suffisantes en vue de répertorier et gérer, pour le type de véhicule soumis à l'homologation, les risques liés aux fournisseurs, en s'appuyant notamment sur les normes requises pour une telle gestion des risques ;

j) Les critères que l'autorité d'homologation appliquera pour évaluer si le constructeur a identifié les éléments critiques du type de véhicule, y compris la définition des « éléments critiques » que l'autorité aura adoptée à cet effet ;

k) Les critères que l'autorité d'homologation appliquera pour évaluer si le constructeur a procédé à une appréciation en profondeur des risques pour le type de véhicule concerné, comme il est prescrit au paragraphe 7.3.3 du Règlement ;

l) Les critères que l'autorité d'homologation appliquera pour évaluer si le type de véhicule concerné est protégé contre les risques répertoriés dans le cadre de l'appréciation des risques effectuée par le constructeur ;

m) Les critères que l'autorité d'homologation appliquera pour évaluer si les mesures d'atténuation prises par le constructeur sont appropriées, ainsi que l'explication de ce que l'on entend par « appropriées » ;

n) Les critères que l'autorité d'homologation appliquera pour évaluer si les mesures d'atténuation évoquées dans les parties B ou C de l'annexe 5 sont non pertinentes, insuffisantes pour le risque identifié ou irréalisables ;

o) Les critères que l'autorité d'homologation appliquera pour évaluer si une « autre mesure d'atténuation » prise par le constructeur en vertu du paragraphe 7.3.4 est « appropriée » ;

p) Les critères que l'autorité d'homologation appliquera pour évaluer si les essais effectués par le constructeur afin de s'assurer de l'efficacité des mesures de sécurité mises en œuvre ont été « appropriés » et « suffisants » ;

q) Les critères que l'autorité d'homologation appliquera pour évaluer si les mesures prises par le constructeur pour sécuriser les environnements du type du véhicule prévus pour le stockage et l'exécution des logiciels, services, applications ou données du marché secondaire sont « appropriées » et « proportionnées », ainsi que l'explication de l'adjectif « proportionné » dans ce contexte ;

r) Les documents que l'autorité d'homologation exigera pour vérifier si le constructeur du véhicule a pris les mesures nécessaires prescrites au paragraphe 5.1.1 ;

s) Les essais qui seront effectués par l'autorité d'homologation ou son service technique ainsi que la stratégie qui sera appliquée pour vérifier que le constructeur a mis en œuvre les mesures de cybersécurité dont il a fait état ;

t) Les procédures internes que l'autorité d'homologation appliquera au cours du processus d'évaluation mené en vertu de la section 5 du Règlement.

Il importe de souligner que les autorités d'homologation des Parties sont implicitement obligées d'appliquer les méthodes et prescriptions qui font l'objet de partage et d'évaluation.

F. Paragraphe 5.3.3

« 5.3.3 Les renseignements visés au paragraphe 5.3.2 doivent être téléchargés en anglais dans la base de données électronique sécurisée DETA, 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. »

Explication de la prescription

Les renseignements téléchargés doivent être objectivement suffisants pour permettre de comprendre les objectifs minimaux qu'une autorité d'homologation a fixés pour pouvoir conclure que les prescriptions du Règlement sont respectées. Ce point revêt une importance cruciale compte tenu du haut niveau et de l'utilisation fréquente de dispositions d'ordre général dans la formulation des prescriptions.

Bien que l'obligation de partager les renseignements, dont il est question au paragraphe 5.3.3, soit une obligation de résultat et doive toujours être remplie par l'autorité d'homologation, celle-ci doit s'acquitter de cette obligation en tenant compte de la nécessité d'éviter de mettre en danger la cybersécurité d'un type de véhicule homologué conformément au Règlement.

Les renseignements devraient de préférence être partagés bien à l'avance (c'est-à-dire bien avant que la première évaluation soit effectuée à l'aide de ces méthodes et critères) avec d'autres autorités d'homologation, afin de leur permettre de les examiner et, le cas échéant, d'obtenir des éclaircissement supplémentaires pour atteindre pleinement les objectifs fixés. Dans aucun cas une autorité d'homologation ne peut toutefois accorder une homologation de type sur la base de ces méthodes et critères avant que se soient écoulés au moins 14 jours depuis le moment où les renseignements ont été partagés via la base de données DETA.

Exemples de documents ou de justificatifs à fournir

On trouvera à l'annexe 1 un modèle pour l'échange de données via la base DETA conformément au paragraphe 5.3.

G. Paragraphe 5.3.4

« 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. »

Explication de la prescription

Les autorités d'homologation d'autres Parties contractantes ont la possibilité, mais pas l'obligation, de faire des observations sur les informations partagées.

Le délai de 14 jours s'applique aussi lorsque les informations visées au paragraphe 5.3.2 ont été partagées plus de 14 jours avant la décision d'homologation. Dans l'idéal, les observations formulées par d'autres autorités devraient être examinées et, si elles sont légitimes et utiles, prises en compte avant que les méthodes et critères partagés via la base de données DETA soient appliqués pour la première fois. Les autorités d'homologation intéressées devraient donc réagir le plus vite possible en transmettant leurs points de vue à l'autorité d'homologation.

H. Paragraphe 5.3.5

« 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 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. 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. »

Explication de la prescription

Les observations éventuelles d'autres Parties contractantes n'ont aucun effet suspensif sur la délivrance d'une homologation par l'autorité d'homologation de type. Cependant, si elle décide de ne pas tenir compte de ces observations, les autorités d'homologation qui ont fait les observations et l'autorité d'homologation qui a émis une décision sont tenues d'entamer une discussion devant le GRVA sur les méthodes et critères soumis et les observations reçues. Bien que l'obligation de rechercher davantage d'éclaircissements incombe aux deux autorités, il n'est pas nécessaire pour entamer la procédure en application de l'annexe 6 que l'autorité qui a soumis des informations et celle qui a fait des observations prennent toutes deux des mesures formelles à cet effet. En vertu du paragraphe 3 de l'annexe 6, le Président du GRVA doit « identifier les problèmes résultant d'interprétations divergentes » du Règlement sur la cybersécurité.

L'interprétation du GRVA doit être guidée par l'intention de la procédure de consultation spécifiée au paragraphe 5.3.2, et donc assurer une application convergente du Règlement. Elle doit donc contenir certains éléments permettant d'établir clairement si les objectifs minimaux et les processus appliqués par l'autorité d'homologation sont suffisants et adéquats pour vérifier que les prescriptions du Règlement ont été respectées. Une fois que le GRVA s'est mis d'accord sur l'interprétation du Règlement, cette interprétation doit être appliquées par toutes les autorités d'homologation dans toutes les procédures d'évaluation ultérieures (pour les homologations de type, les modifications et les extensions) au titre du Règlement. Cela peut devoir passer par des mises à jour des méthodes et critères utilisés par les autorités d'homologation de toutes les Parties contractantes ou de certaines d'entre elles.

I. Paragraphe 5.3.6

« 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. »

Explication de la prescription

Cette prescription est distincte et s'ajoute à celle du paragraphe 5.2 concernant la notification sur un formulaire type. L'homologation de type doit être notifiée en même temps que des documents justificatifs qui ne sont pas spécifiés au paragraphe 5.3.6. L'objectif de ce partage n'est pas explicitement précisé dans le Règlement, mais on peut déduire du paragraphe 5.3.7 qu'il s'agit de permettre aux autorités d'homologation « d'étudier » les homologations et de faire connaître, le cas échéant, des « avis divergents » conformément à l'annexe 6, notamment. Les documents justificatifs doivent donc contenir tous les éléments (y compris les rapports d'essai) suffisants pour permettre aux autorités d'homologation de comprendre si, et comment, les méthodes et critères auxquels il est fait référence aux paragraphes précédents ont été appliqués dans le contexte d'une décision d'homologation individuelle.

Les informations doivent être téléchargées dans la base de données DETA. Un modèle pour ce téléchargement est présenté à la section 5.

L'obligation de notification qui figure dans la première phrase du paragraphe 5.3.6 ne dépend pas de la possibilité de concilier l'obligation de télécharger les informations dans la base de données DETA avec les obligations du droit national relatives à la sécurité et éventuellement à la confidentialité des informations notifiées. Dans le cas où le téléchargement des informations dans la base DETA risque d'entrer en conflit avec de telles obligations, l'autorité d'homologation doit trouver un moyen de notifier l'information de manière sécurisée.

J. Paragraphe 5.3.7

« 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. »

Explication de la prescription

En cas de « divergence de vues » entre autorités d'homologation concernant les informations relatives à l'homologation de type, il est fait référence à l'article 10 de l'Accord et à l'annexe 6. La procédure de l'article 10 est réservée aux cas où le différend porte sur l'interprétation de l'Accord. En revanche, tout différend survenant dans le contexte de l'homologation de type et concernant l'application ou l'interprétation du Règlement (et donc l'application des méthodes et critères évoqués au paragraphe 5.3.3) doit être résolu conformément au paragraphe 2 de l'annexe 6.

K. Paragraphes 6 à 7.1.1

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

Le présent document ne comporte aucune indication concernant cette prescription.

« 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. »

Explication de la prescription

Les prescriptions du Règlement ne doivent pas limiter les prescriptions d'autres Règlements ONU ni d'autres législations nationales ou régionales, comme il est indiqué aux points 1.3 et 1.4 du champ d'application du Règlement.

L. Paragraphes 7.2 à 7.2.1

« 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. »

Explication de la prescription

Le but de cette prescription est que l'autorité d'homologation ou son service technique vérifie que :

a) Le véhicule dispose d'un système de gestion de la cybersécurité (CSMS) ;

b) Le CSMS présenté est conforme aux prescriptions du Règlement qui sont énumérées ci-après.

Pour cette prescription, l'accent est mis sur les processus élaborés par le constructeur et sur l'évaluation de leur mise en place , dans le but de vérifier la capacité du constructeur à respecter les prescriptions relatives au CSMS.

Les précisions suivantes devraient être prises en compte

c) Le CSMS peut faire partie du système de gestion de la qualité de l'organisation ou en être indépendant ;

d) Si le CSMS fait partie du système de gestion de la qualité de l'organisation, cela doit apparaître clairement.

Exemples de documents ou de justificatifs à fournir

Les normes suivantes peuvent être applicables :

e) La norme ISO PAS 5112 peut être utilisée comme base de mise en évidence et d'évaluation du CSMS. On se réfère alors aux prescriptions et recommandations énoncées dans la norme ISO/SAE 21434:2021 (E) aux articles 5 « Gestion organisationnelle de la cybersécurité », 6 « Gestion de la cybersécurité selon les projets » et 8 « Activités continues en matière de cybersécurité » pour évaluer le CSMS en général ;

f) Les normes ISO 18045 et ISO 15408 et celles des séries ISO 27000 et ISO 31000 peuvent s'appliquer à certaines parties pertinentes du CSMS.

M. Paragraphes 7.2.2 à 7.2.2.1

« 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. »

Explication de la prescription

Le but de cette prescription est que le système de gestion de la cybersécurité soit capable de démontrer comment un constructeur gérera la sécurité pendant la durée de vie des véhicules correspondant à un type donné. Il s'agit notamment de mettre en évidence que des procédures et des processus sont mis en œuvre pour couvrir les trois phases. Chacune des différentes phases du cycle de vie peut nécessiter que des activités spécifiques soient menées à bien.

Le paragraphe 7.2.2.1 décrit les différentes phases du véhicule type à prendre en considération dans le CSMS, tandis que le paragraphe 7.2.2.2 s'applique aux trois phases, sauf indication contraire. Il en va de même du paragraphe 7.2.2.4.

Le CSMS peut inclure des procédures ou des processus actifs ou réactifs portant sur la fin de l'assistance pour un type de véhicule et sur la manière dont celle-ci est mise en œuvre ou déclenchée. Il peut s'agir de la possibilité de déconnecter des fonctions ou systèmes non obligatoires et des conditions dans lesquelles cela pourrait se produire.

La durée de vie opérationnelle (phase d'utilisation) d'un véhicule commence durant la phase de production du type de véhicule. Elle prend fin soit pendant la phase de production, soit pendant la phase de postproduction du type de véhicule.

Exemples de documents ou de justificatifs à fournir

Les normes suivantes peuvent être applicables :

a) La norme ISO PAS 5112 peut être utilisée comme base de mise en évidence et d'évaluation des phases du CSMS exigées. On se réfère alors aux articles 9 « Concept », 10 « Développement du produit » et 11 « Validation de la cybersécurité » de la norme ISO/SAE 21434:2021 (E) pour évaluer la phase de développement du CSMS , à l'article 12 « Production » de la même norme pour évaluer la phase de production du CSMS , ainsi qu'aux articles 8 « Activités continues en matière de cybersécurité », 13 « Fonctionnement et maintenance » et 14 « Fin de l'appui en matière de cybersécurité et mise hors service » de la même norme pour évaluer la phase de postproduction du CSMS ;

b) Les autres normes susceptibles de s'appliquer au paragraphe 7.2.2 sont notamment les normes ISO 18045 et ISO 15408, ainsi que celles de la série ISO 27000 et de la série ISO 31000.

N. Paragraphe 7.2.2.2, alinéa a)

« 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 ; »

Explication de la prescription

Le but de cette prescription est de s'assurer que l'organisation dispose de processus de mise en œuvre du CSMS. Son champ d'application se limite aux processus qui sont pertinents pour la cybersécurité des types de véhicules, à l'exclusion d'autres aspects de l'organisation. Ainsi, par exemple, cette prescription n'est pas destinée à couvrir la totalité du système de gestion de la sécurité de l'information d'une organisation.

Les éléments suivants pourraient être utilisés pour illustrer la gamme des activités déployées par le constructeur pour gérer la cybersécurité des phases de développement, de production et de postproduction d'un type de véhicule :

a) Structure organisationnelle utilisée pour gérer la cybersécurité ;

b) Rôles et responsabilités en matière de gestion de la cybersécurité, y compris la justification.

Exemples de documents ou de justificatifs à fournir

c) La norme ISO/SAE 21434:2021 peut être utilisée comme base de mise en évidence et d'évaluation, en particulier les exigences [RQ-05-01], [RQ-05-02], [RQ-05-06] et [RQ-05-07] ;

d) La norme BSI PAS 1885 ou ISO PAS 5112 pourrait servir à démontrer le respect de cette prescription. Des systèmes nationaux de certification, comme le système UK Cyber Essentials, pourraient servir à mettre en évidence les processus organisationnels d'un constructeur.

La prescription doit être considérée comme non respectée si l'une des affirmations suivantes est vraie

1. Les processus sont absents ou incomplets.

2. Les processus ne sont pas appliqués de manière universelle ou cohérente.

3. Les processus sont parfois ou systématiquement contournés pour atteindre des objectifs commerciaux.

4. L'approche du constructeur du véhicule en matière de gestion de la sécurité et des risques n'est pas en rapport avec ses processus.

5. La sécurité du système dépend entièrement de l'application prudente et cohérente par les utilisateurs de processus de sécurité manuels.

6. Les processus n'ont pas été révisés en réponse à des changements majeurs (s'agissant par exemple de la technologie ou du cadre réglementaire), ou dans un délai approprié.

7. Les processus ne sont pas facilement accessibles au personnel, trop détaillés pour qu'on puisse s'en souvenir ou trop difficiles à comprendre.

La prescription peut être considérée comme respectée si toutes les affirmations suivantes sont vraies

1. Le constructeur du véhicule documente pleinement son cadre de gouvernance de la sécurité et de gestion des risques, ses pratiques en matière de sécurité technique et sa conformité aux règlements spécifiques. La cybersécurité fait partie intégrante de ces processus et des indicateurs de performance clefs sont communiqués à sa direction exécutive.

2. Les processus du constructeur du véhicule sont conçus pour être pratiques, utilisables et adaptés à ses politiques et technologies.

3. Les processus qui dépendent du comportement de l'utilisateur sont pratiques, adaptés et réalisables.

4. Le constructeur du véhicule revoit et met à jour ses processus à intervalles réguliers et appropriés pour s'assurer qu'ils restent pertinents, en plus des révisions suivant un incident de cybersécurité majeur.

5. Toute modification d'une fonction essentielle ou de la menace qui y est associée déclenche une révision des processus.

6. Les systèmes du constructeur du véhicule sont conçus de manière à être et rester sûrs même lorsque les politiques et procédures de sécurité de l'utilisateur ne sont pas toujours suivies. Il convient de fournir la justification d'une telle affirmation.

O. Paragraphe 7.2.2.2, alinéa b)

« 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. »

Explication de la prescription

Le but de cette prescription est que le constructeur démontre les processus et procédures qu'il utilise pour répertorier les risques auxquels les types de véhicules sont exposés.

Les processus mis en œuvre doivent tenir compte de toutes les sources probables de risques, notamment celles qui sont identifiées à l'annexe 5 du Règlement sur le cybersécurité, par exemple les risques découlant de services connectés ou de dépendances extérieurs au véhicule.

Parmi les sources de risques, on peut mentionner :

a) Les plateformes d'échanges sur les vulnérabilités et les menaces ;

b) Les enseignements tirés au sujet des risques et des vulnérabilités.

Exemples de documents ou de justificatifs à fournir

Les normes suivantes peuvent être applicables :

c) La norme ISO/SAE 21434:2021, notamment les exigences [RQ-15-01], [RQ-15-02], [RQ-15-03] et [RQ-15-08] ;

d) La norme ISO PAS 5112.

Les processus peuvent tenir compte :

e) De l'identification de la pertinence d'un système eu égard à la cybersécurité ;

f) De le description de l'ensemble du système en ce qui concerne :

i) La définition du système ou de la fonction ;

ii) Les frontières et interactions avec d'autres systèmes ;

iii) L'architecture ;

iv) L'environnement dans lequel fonctionne le système (contexte, contraintes et hypothèses) ;

g) De l'identification des ressources ;

h) De l'identification des menaces ;

i) De l'identification des vulnérabilités.

La prescription doit être considérée comme non respectée si l'une des affirmations suivantes est vraie

1. L'identification des risques ne repose pas sur une série d'hypothèses clairement définies.

2. L'identification des risques pour les types de véhicules est une activité occasionnelle (ou n'est pas effectuée du tout).

3. Les types de véhicules sont évalués de manière isolée, sans considération des dépendances et interactions avec d'autres systèmes (par exemple les interactions entre les environnements informatique et de technologie opérationnelle).

La prescription peut être considérée comme respectée si toutes les affirmations suivantes sont vraies

1. Le processus organisationnel du constructeur du véhicule permet de s'assurer que les risques encourus par les types de véhicules sont identifiés, analysés, priorisés et gérés.

2. L'approche du constructeur du véhicule en matière d'évaluation des risques est centrée sur les possibilités d'impact défavorable sur ses types de véhicules, ce qui l'amène à étudier en détail comment un tel impact est susceptible de se produire sous l'effet d'attaques, ainsi que les propriétés de sécurité de ses réseaux et systèmes.

3. Le constructeur du véhicule répertorie les risques en se fondant sur une série d'hypothèses claires et une compréhension actualisée des menaces pour la sécurité de ses types de véhicules et de son secteur.

4. Le constructeur du véhicule répertorie les risques en se fondant sur une bonne compréhension des vulnérabilités de ses types de véhicules.

5. Le constructeur du véhicule procède à une analyse détaillée des menaces et comprend comment l'appliquer à son organisation dans le contexte de ses types de véhicules et de son secteur.

P. Paragraphe 7.2.2.2, alinéa c)

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

Explication de la prescription

Le but de cette prescription est que le constructeur fasse la démonstration des processus et règles qu'il applique pour évaluer, catégoriser et traiter les risques répertoriés.

Exemples de documents ou de justificatifs à fournir

Les normes suivantes peuvent être applicables :

a) La norme ISO/SAE 21434:2021, notamment les exigences [RQ-15-15], [RQ-15-16], [RQ-15-04], [RQ-15-05], [RQ-15-10], [RQ-15-17], [RQ-09-05] et [RQ-09-06] ;

b) La norme ISO PAS 5112 ;

c) La norme BSI PAS 11281:2018 pourrait être appliquée pour l'examen de la sûreté et de la sécurité.

Les processus peuvent consister à :

d) Évaluer l'impact associé aux risques répertoriés conformément au paragraphe 7.2.2.2 b) ;

e) Recenser les voies d'attaque potentielles liées aux risques répertoriés conformément au paragraphe 7.2.2.2 b) ;

f) Déterminer la faisabilité et la probabilité de l'attaque pour chacune des voies d'attaque identifiées ci-dessus ;

g) Calculer et catégoriser les risques ;

h) Choisir les traitements à appliquer aux risques répertoriés et caractérisés.

La prescription doit être considérée comme non respectée si l'une des affirmations suivantes est vraie

1. Les résultats de l'évaluation des risques sont trop complexes ou trop peu maniables pour être utilisés par les décideurs et ne sont pas communiqués efficacement, d'une manière claire et en temps opportun.

2. Les prescriptions en matière de sécurité et les techniques d'atténuation sont arbitraires ou appliquées à partir d'un catalogue de mesures sans tenir compte de la manière dont elles contribuent à la sécurité des types de véhicules.

3. Seuls certains domaines ou types de ressources sont documentés et compris. Les dépendances entre les ressources ne sont pas comprises (comme les dépendances entre l'informatique et la technologie opérationnelle).

4. Les inventaires des ressources concernant les types de véhicules sont incomplets, inexistants ou insuffisamment détaillés.

5. Les inventaires des ressources sont négligés et dépassés.

6. Les systèmes sont évalués isolément, sans prise en compte des dépendances et interactions avec d'autres systèmes (par exemple, les interactions entre les environnements informatique et de technologie opérationnelle).

7. Les évaluations des risques ne reposent pas sur une série d'hypothèses clairement définie.

8. Les évaluations des risques relèvent de l'activité occasionnelle (ou ne sont pas effectuées du tout).

La prescription peut être considérée comme respectée si toutes les affirmations suivantes sont vraies

1. Le résultat du processus de gestion des risques appliqué par le constructeur du véhicule est une série claire de prescriptions en matière de sécurité qui traiteront les risques conformément à son approche organisationnelle de la sécurité.

2. Toutes les ressources relevant du fonctionnement sécurisé de ses types de véhicules sont identifiées et inventoriées (à un niveau de détail approprié).

3. L'inventaire est maintenu à jour.

4. Les dépendances par rapport à l'infrastructure d'appui sont reconnues et enregistrées.

5. Le constructeur du véhicule a priorisé les ressources en fonction de leur importance pour le fonctionnement de ses types de véhicules.

6. Le constructeur du véhicule a répertorié les risques en se fondant sur une série d'hypothèses claires et une compréhension actualisée des menaces pour la sécurité de ses types de véhicules et de son secteur.

7. Le constructeur du véhicule a répertorié les risques en se fondant sur une bonne compréhension des vulnérabilités de ses types de véhicules.

8. Le constructeur est en mesure de démontrer l'efficacité et la reproductibilité de ses processus de catégorisation et de traitement des risques.

Q. Paragraphe 7.2.2.2, alinéa d)

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

Explication de la prescription

Le but de cette prescription est que le constructeur démontre les processus et règles qu'il applique pour décider comment gérer les risques. Il peut s'agir notamment des critères de décision quant au traitement des risques, par exemple le processus de sélection des contrôles à appliquer et du moment où un risque doit être accepté.

Les résultats des processus d'identification et d'évaluation des risques doivent permettre de choisir entre les traitements appropriés envisageables pour ces risques. Le résultat final doit être que le risque résiduel (qui subsiste après le traitement) soit dans les limites de tolérance indiquées par le constructeur (c'est-à-dire dans des limites acceptables).

Les mesures d'atténuation visées à l'annexe 5 du Règlement sur la cybersécurité doivent être prises en compte dans les processus.

Exemples de documents ou de justificatifs à fournir

Les normes suivantes peuvent être applicables :

a) La norme ISO/SAE 21434:2021 peut être utilisée comme base de mise en évidence et d'évaluation, notamment les exigences [RQ-09-07], [RQ-09-11] et [RQ-11-01] ;

b) La norme ISO PAS 5112 ;

c) La norme ISO 31000 pourrait être appliquée, le cas échéant, pour les risques liés aux produits.

Les processus peuvent consister à :

d) Appliquer des méthodes de traitement des risques appropriées et proportionnelles ;

e) Traiter les éléments critiques (au niveau de la sécurité et de l'environnement) pour faire en sorte que les risques encourus soient atténués de manière appropriée et proportionnée sur la base des objectifs des systèmes des véhicules dépendants concernant la sécurité et l'environnement ;

f) Veiller à ce que le risque résiduel reste dans des limites acceptables pour le type de véhicule ou ses éléments ;

g) Détailler les cas dans lesquels l'organisation accepterait une justification de non-conformité à la tolérance du risque admise.

La prescription doit être considérée comme non respectée
si l'une des affirmations suivantes est vraie

1. Les éléments de sécurité des projets ou des programmes dépendent uniquement de la réalisation d'une évaluation de la gestion des risques, sans aucun égard pour ses résultats.

2. Aucun processus systémique n'est en place pour s'assurer que les risques répertoriés sont gérés de manière efficace.

3. Les risques sont conservés dans un registre pendant de longues périodes, dans l'attente de décisions à des niveaux plus élevés ou d'allocations de ressources pour y remédier.

La prescription peut être considérée comme respectée
si toutes les affirmations suivantes sont vraies

1. Les conclusions importantes dégagées au cours du processus de gestion des risques du constructeur du véhicule sont communiquées aux décideurs clefs en matière de sécurité et aux personnes responsables.

2. L'efficacité du processus de gestion des risques du constructeur du véhicule est examinée périodiquement et des améliorations lui sont apportées en cas de besoin.

R. Paragraphe 7.2.2.2, alinéa e)

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

Explication de la prescription

Le but de cette prescription est de s'assurer que le constructeur dispose des capacités et des processus appropriés pour soumettre le type de véhicule à des essais tout au long de ses phases de développement et de production.

Les processus d'essai dans la phase de production peuvent être différents de ceux qui sont appliqués pendant la phase de développement.

Exemples de documents ou de justificatifs à fournir

Les normes suivantes peuvent être applicables :

a) La norme ISO/SAE 21434:2021 peut être utilisée comme base de mise en évidence et d'évaluation, notamment les exigences [RQ-10-09], [RQ-10-10], [RQ-11-01] et [RQ-12-02] ;

b) La norme ISO PAS 5112 ;

c) La norme BSI PAS 11281:2018 pourrait être utilisée pour prendre en considération les interactions entre sûreté et sécurité, ainsi que les processus visant à démontrer que les résultats en matière de sécurité sont atteints.

Les processus peuvent porter sur :

Phase de développement :

d) Les règles spécifiques de l'organisation applicables aux contrôles pendant la phase de développement ;

e) Les processus de mise au point et d'exécution de stratégies de contrôle ;

f) Les processus de planification des contrôles en matière de cybersécurité ;

g) Les processus de contrôle de la conception du système de cybersécurité ;

h) Les processus de contrôle du logiciel de cybersécurité ;

i) Les processus de contrôle du matériel de cybersécurité ;

j) Les processus de contrôle de l'intégration de la cybersécurité ;

k) Les processus de documentation des résultats des contrôles ;

l) Les processus de gestion des vulnérabilités identifiées lors des contrôles ;

m) Les justifications et prescriptions applicables aux contrôles en matière de cybersécurité, comme les essais fonctionnels (fondés sur des directives, positifs et négatifs), l'essai d'interface, l'essai de pénétration, l'analyse des vulnérabilités ou l'essai à données aléatoires (fuzzing), notamment

Phase de production :

n) Les processus destinés à vérifier que le système produit répond aux prescriptions en matière de cybersécurité, de contrôles et de capacités mentionnés dans le plan de production ;

o) Les processus de contrôle destinés à assurer que le produit satisfait à des spécifications en matière de cybersécurité qui sont conformes avec le système en phase de développement ;

p) Les processus destinés à vérifier que les contrôles de la cybersécurité et la configuration selon les spécifications relatives à la cybersécurité sont activés dans le produit ;

q) Les processus de documentation des résultats des essais et de gestion des résultats obtenus.

La prescription doit être considérée comme non respectée si l'une des affirmations suivantes est vraie

1. Un produit ou service particulier est considéré comme une « solution miracle » et les affirmations du vendeur sont prises pour argent comptant.

2. Des méthodes d'assurance sont appliquées sans appréciation de leurs forces et de leurs faiblesses, par exemple les essais de pénétration dans des environnements opérationnels.

3. L'assurance est assumée car aucun problème n'a été recensé jusque-là.

La prescription peut être considérée comme respectée si toutes les affirmations suivantes sont vraies

1. Le constructeur du véhicule confirme que les mesures de sécurité mises en place pour protéger les systèmes sont efficaces et le restent jusqu'à la fin de vie de tous les véhicules des types considérés auxquels elles sont destinées.

2. Le constructeur du véhicule comprend les méthodes d'assurance qui sont à sa disposition et choisit celles qui sont les plus appropriées pour renforcer la confiance dans la sécurité des types de véhicules.

3. La confiance du constructeur du véhicule dans la sécurité telle qu'elle repose sur sa technologie, son personnel et ses processus peut être justifiée et vérifiée par une tierce partie.

4. Les lacunes en matière de sécurité qui ne sont pas couvertes par les activités liées à l'assurance sont évaluées, priorisées et comblées le cas échéant de manière efficace et en temps voulu.

5. Les méthodes utilisées pour l'assurance sont revues pour vérifier qu'elles fonctionnent comme prévu et qu'elles restent les plus appropriées.

S. Paragraphe 7.2.2.2, alinéa f)

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

Explication de la prescription

Le but de cette prescription est de s'assurer que l'appréciation des risques est constamment actualisée. Cela se traduit par des processus permettant de déterminer si les risques encourus par un type de véhicule ont changé et de savoir comment il en sera tenu compte dans le cadre de l'appréciation des risques.

Les sources d'identification des risques peuvent être mentionnées. Ce sont notamment :

a) Les plateformes d'échange sur les vulnérabilités et les menaces ;

b) Les enseignements tirés en matière de risques et de vulnérabilités ;

c) Les conférences.

Il est à noter que les prescriptions des alinéas f) à h) du paragraphe 7.2.2.2 peuvent se recouper en ce qui concerne les processus utilisés et que les mêmes méthodes peuvent donc être appliquées pour démontrer que ces prescriptions sont respectées.

Exemples de documents ou de justificatifs à fournir

d) La norme ISO/SAE 21434:2021 peut être utilisée comme base de mise en évidence et d'évaluation, notamment les exigences [RQ-08-07] et [RQ-06-09] ;

e) La norme ISO PAS 5112.

La prescription doit être considérée comme non respectée si l'affirmation suivante est vraie

1. Aucun processus n'est en place qui nécessite l'actualisation de l'appréciation des risques.

La prescription peut être considérée comme respectée si toutes les affirmations suivantes sont vraies

1. Le constructeur du véhicule procède à une appréciation des risques quand des événements importants sont susceptibles d'affecter les types de véhicules, par exemple le remplacement d'un système ou un changement intervenu dans les cybermenaces.

2. Les appréciations des risques par le constructeur du véhicule sont dynamiques et actualisées à la lumière de changements pertinents, qui peuvent être des modifications techniques apportées aux types de véhicules, des changements d'utilisation ou des informations concernant d'éventuelles menaces nouvelles.

T. Paragraphe 7.2.2.2, alinéa g)

« 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 ; »

Explication de la prescription

Le but de cette prescription est de s'assurer que le constructeur dispose de processus permettant de détecter des cyberattaques, menaces ou vulnérabilités concernant des véhicules dont il a fait homologuer le type, c'est-à-dire qui sont en phase de postproduction ou de production, et qu'il dispose également de processus permettant de les déjouer de manière appropriée et en temps voulu.

Il est à noter que les prescriptions des alinéas f) à h) du paragraphe 7.2.2.2 peuvent se recouper en ce qui concerne les processus utilisés et que les mêmes méthodes peuvent donc être appliquées pour démontrer que ces prescriptions sont respectées.

Exemples de documents ou de justificatifs à fournir

Les normes suivantes peuvent être applicables :

a) La norme ISO/SAE 21434:2021 peut être utilisée comme base de mise en évidence et d'évaluation, notamment les prescriptions [RQ-08-01], [RQ-08-02], [RQ-08-03], [RQ-08-04], [RQ-08-05], [RQ-08-07], [RQ-08-08], [RQ-07-06], [RC-07-08], [RQ-13-01] et [RQ-13-02] ;

b) La norme ISO PAS 5112.

Les éléments suivants pourraient servir à mettre en évidence les processus utilisés

c) Des processus de surveillance de la cybersécurité pour les véhicules en phase de postproduction. Il peut notamment s'agir de processus recueillant des informations susceptibles ou non d'être pertinentes pour le véhicule ou le système du constructeur ;

d) Des processus d'évaluation des informations relatives à la cybersécurité. Il s'agit de processus permettant de déterminer la pertinence des informations recueillies pour le véhicule ou le système du constructeur ;

e) Des processus de détermination/évaluation des risques pour les informations pertinentes ;

f) Des procédures d'intervention en cas d'incident, tant pour les véhicules des types couverts par le système de gestion de la cybersécurité qui sont déjà homologués que pour ceux qui ne le sont pas encore, ce qui pourrait passer par :

i) Des interactions avec les autorités ;

ii) Des éléments déclencheurs, identifiés ou déclarés, qui entraîneraient une escalade ou une action ;

iii) La détermination du type d'intervention à mettre en œuvre, et dans quel cas ;

iv) La gestion de toute dépendance ou interaction avec les fournisseurs ;

g) La démonstration que les procédures d'intervention fonctionneraient, par exemple à l'aide d'exercices et en vérifiant que les hypothèses de planification restent valables sous essai.

La prescription doit être considérée comme non respectée si l'une des affirmations suivantes est vraie

1. Le constructeur du véhicule ne dispose pas de sources de renseignement sur les menaces.

2. Le constructeur du véhicule ne met pas en œuvre les mises à jour en temps voulu après les avoir reçues.

3. Le constructeur du véhicule n'évalue pas l'utilité de ses informations concernant les menaces, ni ne partage les rétroactions avec les fournisseurs, les prestataires de services du marché secondaire ou d'autres utilisateurs.

4. Il n'y a pas de personnel pour assumer une fonction de surveillance.

5. Le personnel de surveillance n'a pas les compétences spécialisées requises.

6. Le personnel de surveillance n'est pas capable de faire rapport selon les critères de gouvernance d'entreprise.

7. Les alertes de sécurité relatives aux types de véhicules ne sont pas considérées comme prioritaires.

La prescription peut être considérée comme respectée si toutes les affirmations suivantes sont vraies

1. Des données relatives à la sécurité et au fonctionnement des types de véhicules sont recueillies.

2. Les alertes émanant de tiers sont étudiées et des mesures sont prises.

3. Quelques ensembles de données permettent d'effectuer aisément des recherches à l'aide d'outils qui facilitent les investigations.

4. Il est procédé régulièrement à la résolution d'alertes concernant une ressource ou un système.

5. Les alertes concernant les types de véhicules sont privilégiées.

6. Le constructeur du véhicule applique les mises à jour en temps voulu.

7. Le constructeur du véhicule dispose de processus permettant de surveiller, détecter et déjouer les cyberattaques, les cybermenaces et les vulnérabilités qui concernent directement ses activités commerciales, ou encore les menaces spécifiques dans son secteur.

8. Le constructeur du véhicule connaît l'efficacité de ses processus (par exemple en suivant la manière dont ils aident à répertorier les problèmes de sécurité).

9. Le personnel de surveillance a des compétences suffisantes et une compréhension de base des données avec lesquelles il doit travailler.

10. Le personnel de surveillance peut rendre compte à d'autres parties de l'organisation (par exemple des directeurs de la sécurité ou des responsables de la résilience).

11. Le constructeur du véhicule fait avec succès la démonstration des processus qui permettent d'évaluer si les mesures de cybersécurité mises en œuvre sont suffisamment fortes pour qu'on puisse conclure qu'elles sont encore efficaces.

U. Paragraphe 7.2.2.2, alinéa h)

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

Explication de la prescription

Cette prescription vise à s'assurer qu'un processus a bien été mis en place pour fournir les données nécessaires à l'analyse et fixer les responsabilités en matière de traitement et d'analyse des données.

Exemples de documents ou de justificatifs à fournir

Les normes suivantes peuvent être applicables :

a) La norme ISO/SAE 21434:2021 peut être utilisée comme base de mise en évidence et d'évaluation, notamment les exigences [RQ-08-02], [RQ-08-03] et [RQ-08-04] ;

b) La norme ISO PAS 5112.

Les éléments suivants pourraient servir à mettre en évidence les processus utilisés :

c) Procédure de mise en œuvre des activités de l'équipe d'intervention en cas d'incident (incidents) ;

d) Surveillance sur le terrain (obtention d'informations relatives aux incidents et vulnérabilités) ;

e) Procédure suivie lorsqu'un incident se produit (y compris un aperçu des informations transmises à l'analyste à chaque étape) ;

f) Procédure suivie lorsqu'une vulnérabilité est découverte (y compris un aperçu des informations transmises à l'analyste à chaque étape).

V. Paragraphe 7.2.2.3

« 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. »

Explication de la prescription

Cette prescription vise à s'assurer qu'une fois que les risques identifiés ont été classés, un processus a été établi pour déterminer le délai de réaction sur la base des résultats du classement.

Il est nécessaire de fixer le délai de réaction par un processus de triage, par exemple, et d'expliquer le processus de surveillance pour voir s'il est exécuté dans le délai imparti.

Les délais communiqués par les constructeurs doivent pouvoir être justifiés et expliqués. Il peut y avoir une série de délais couvrant différentes situations possibles. Elle doit comporter des délais de décision et de mise en œuvre des éventuelles réactions ou réponses.

Exemples de documents ou de justificatifs à fournir

Les normes suivantes peuvent être applicables :

a) La norme ISO/SAE 21434:2021 peut être utilisée comme base de mise en évidence des processus requis, notamment les exigences [RQ-08-07] et [RQ-08-08] ;

b) La norme ISO PAS 5112.

Les éléments suivants pourraient servir à mettre en évidence les processus utilisés :

c) Procédure de mise en œuvre d'activités en réaction à un incident de cybersécurité, comprenant notamment :

i) Surveillance sur le terrain (pour obtenir des informations sur les incidents et les vulnérabilités) ;

ii) Procédure de gestion des incidents, y compris la détermination du délai de réaction ;

iii) Procédures permettant de découvrir les vulnérabilités.

d) Démonstration de la manière dont les procédures sont mises en œuvre.

W. Paragraphe 7.2.2.4

« 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. »

Explication de la prescription

Cette prescription vise à s'assurer que les processus de surveillance des cyberattaques, cybermenaces et vulnérabilités des types de véhicules sont actifs en permanence et s'appliquent à tous les véhicules immatriculés du constructeur qui sont concernés par son système de gestion de la cybersécurité, en utilisant pour cela :

a) Des informations de surveillance acquises conformément au paragraphe 7.3.7, en plus d'autres sources d'informations de surveillance acquises conformément à l'alinéa g) du paragraphe 7.2.2.2 (comme les médias sociaux).

Il est à noter que le paragraphe 1.3 et le respect de la législation sur la protection des données sont particulièrement pertinents pour cette prescription.

Exemples de documents ou de justificatifs à fournir

Les normes suivantes peuvent être applicables :

a) La norme ISO/SAE 21434:2021 peut être utilisée comme base de mise en évidence et d'évaluation, notamment les articles 8.3 « Surveillance de la cybersécurité », 8.4 « Évaluation des incidents de cybersécurité » et 8.5 « Analyse des vulnérabilités » ;

b) La norme ISO PAS 5112.

Les éléments suivants pourraient servir à mettre en évidence les processus utilisés :

c) Procédure de mise en œuvre d'activités en réaction à un incident de cybersécurité, comprenant notamment :

i) Surveillance sur le terrain (pour obtenir des informations sur les incidents et les vulnérabilités) ;

ii) Procédure de gestion des incidents ;

iii) Procédures permettant de découvrir les vulnérabilités ;

d) Démonstration de la manière dont les procédures sont mises en œuvre.

X. Paragraphe 7.2.2.5

« 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. »

Explication de la prescription

Cette prescription vise à s'assurer qu'il est possible de connaître les risques liés aux fournisseurs et de les gérer dans le cadre des processus décrits dans le CSMS. Les mesures prises doivent être proportionnées aux risques associés aux éléments fournis.

La mise en œuvre finale des processus peut faire partie d'un accord bilatéral entre le constructeur et son fournisseur.

Le CSMS peut comporter des processus permettant :

a) De répertorier les risques associés à des pièces, composants, systèmes ou services obtenus auprès de fournisseurs ;

b) De gérer les risques pour le véhicule liés à des fournisseurs de fonctions ou de services de connectivité dont le véhicule peut avoir besoin. Il peut s'agir par exemple de fournisseurs de services cloud, d'opérateurs de télécommunications, de fournisseurs d'accès à Internet ou de fournisseurs autorisés de services du marché secondaire ;

c) De s'assurer que les fournisseurs et les prestataires de services sont capables de démontrer comment ils ont géré les risques qui les concernent. Il peut s'agir de prescriptions relatives à la validation ou aux essais destinées à prouver que les risques sont gérés de manière appropriée ;

d) De déléguer certaines prescriptions à des départements ou services pertinents relevant du constructeur, afin qu'ils puissent gérer les risques répertoriés.

Il est à noter qu'il est possible de déléguer ces prescriptions aux fournisseurs de premier rang et de leur demander de les passer à des fournisseurs de deuxième rang. Il pourrait cependant être difficile à un constructeur de déléguer plus loin dans la chaîne d'approvisionnement (surtout s'il s'agit de prescriptions juridiquement contraignantes).

Exemples de documents ou de justificatifs à fournir

Les normes suivantes peuvent être applicables :

e) La norme ISO/SAE 21434:2021 peut être utilisée comme base de mise en évidence et d'évaluation, notamment les exigences [RQ-06-10], [RQ-07-04] et [RC-07-05] ;

f) La norme ISO PAS 5112.

Les éléments suivants pourraient servir à mettre en évidence les processus utilisés

g) Des accords contractuels en vigueur, ou la preuve de l'existence de tels accords ;

h) Des arguments fondés montrant comment les processus assureront que les fournisseurs et prestataires de services seront pris en compte dans le processus d'évaluation des risques ;

i) Des procédures et méthodes de partage des informations sur les risques entre les fournisseurs et les constructeurs ;

j) Des solutions ou contrats existants tels qu'un système de gestion de la sûreté des informations peuvent être utilisés. La preuve peut en être apportée par des certificats fondés sur la norme ISO/IEC 27001 ou sur le mécanisme TISAX (Trusted Information Security Assessment eXchange).

La prescription doit être considérée comme non respectée si l'une des affirmations suivantes est vraie

1. Les contrats avec les fournisseurs et prestataires de services ne comportent aucune prescription relative à la cybersécurité.

La prescription peut être considérée comme respectée si toutes les affirmations suivantes sont vraies

1. Le constructeur du véhicule a une connaissance approfondie de sa chaîne d'approvisionnement, y compris de ses sous-traitants, et des risques encourus. Il tient compte de facteurs tels que les partenariats avec les fournisseurs, leurs concurrents, leur nationalité et les autres organisations avec lesquelles ils sous-traitent. Cela renforce ses processus d'évaluation des risques et d'approvisionnement.

2. Le constructeur du véhicule aborde la gestion des risques pour la chaîne d'approvisionnement en tenant compte de ceux que des cybercriminels compétents et disposant de ressources suffisantes s'en prenant à la chaîne d'approvisionnement font courir à ses types de véhicules.

3. Le constructeur du véhicule est confiant dans le fait que les informations échangées avec les fournisseurs qui sont essentielles au fonctionnement de ses types de véhicules sont efficacement protégées contre des attaques sophistiquées.

4. Le constructeur du véhicule est capable d'exprimer clairement les exigences de sécurité qu'il impose à ses fournisseurs, de manière à ce qu'elles soient mutuellement comprises et spécifiées dans les contrats. Il s'agit d'un modèle clair et documenté de responsabilité partagée.

5. Toutes les connexions réseau et les échanges de données avec des tiers sont gérés de manière efficace et proportionnée.

6. En cas de besoin, le processus de gestion des incidents du constructeur du véhicule et celui du fournisseur se soutiennent mutuellement en vue de régler les incidents.

Y. Paragraphes 7.3 à 7.3.1

« 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 délivrées pour la première fois avant le 1er juillet 2024 et pour toutes les extensions de ces homologations, 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. »

Explication de la prescription

Cette prescription vise à vérifier qu'il existe un certificat de conformité du CSMS permettant 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 postproduction 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 des méthodes et des critères publiés par la CEE, conformément au paragraphe 5 du Règlement ONU no 155.

Précisions 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 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.

Z. Paragraphe 7.3.2

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

Explication de la prescription

Cette prescription fait explicitement référence à la nécessité de recueillir suffisamment d'informations concernant la chaîne d'approvisionnement et est liée au paragraphe 7.2.2.5. Elle vise à s'assurer que les informations présentées (en même temps que celles du constructeur) sont suffisantes pour que l'évaluation soit menée conformément aux prescriptions des paragraphes 7.3.3 à 7.3.6.

Précisions à prendre en compte

a) S'agissant des « risques liés aux fournisseurs », il faut démontrer qu'il est possible de connaître et de gérer les risques introduits par les fournisseurs. Il est admis qu'il est difficile de faire respecter les prescriptions le long de la chaîne d'approvisionnement au-delà des fournisseurs de deuxième rang et de faire en sorte qu'elles soient juridiquement contraignantes.

Exemples de documents ou de justificatifs à fournir

Les normes suivantes peuvent être applicables :

b) La norme ISO/SAE 21434:2021 ;

c) La norme ISO PAS 5112.

L'élément suivant pourrait servir à mettre en évidence les processus utilisés :

d) Preuve de l'existence, dans les contrats avec les fournisseurs, de sections portant sur les prescriptions du Règlement.

AA. Paragraphe 7.3.3

« 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. »

Explication de la prescription

Cette prescription vise à ce que le constructeur répertorie les éléments critiques d'un type de véhicule en ce qui concerne la cybersécurité et fournisse une explication de la manière dont sont gérés les risques qui leur sont liés.

Le constructeur doit être capable d'expliquer pourquoi il a estimé que certains éléments d'un type de véhicule sont critiques (ou pas).

Précisions à prendre en compte

a) Les éléments critiques peuvent être des éléments qui contribuent à la sécurité du véhicule, à la protection de l'environnement ou la protection contre le vol. Il peut aussi s'agir d'éléments qui assurent la connectivité, ou encore des parties de l'architecture du véhicule qui jouent un rôle critique en matière de partage d'informations ou de cybersécurité (les points d'entrée pourraient aussi être considérés comme critiques) ;

b) Cette prescription vise à s'assurer que les risques sont gérés de manière appropriée, en tenant compte de toutes les menaces, y compris celles qui figurent dans la partie A de l'annexe 5, et en jugeant de la nécessité de contre-mesures basées sur les résultats de l'analyse et de l'appréciation des risques ;

c) Elle vise à permettre au constructeur du véhicule de démontrer l'application au type de véhicule du processus correspondant aux prescriptions des paragraphes 7.2.2.2 et 7.2.2.4 du CSMS ;

d) L'autorité d'homologation ou le service technique doivent se référer à l'annexe 5 du Règlement sur la cybersécurité pour étayer leur évaluation de l'appréciation des risques qui est faite par le constructeur ;

e) L'analyse des risques doit tenir compte des prescriptions du paragraphe 7.3.4 et de celles qui concernent les mesures d'atténuation proportionnées ;

f) La prise en compte des menaces et des mesures d'atténuation de l'annexe 5 dans le cadre d'une appréciation des risques peut conduire à des appréciations telles que « non pertinent » ou « risques négligeables ».

Exemples de documents ou de justificatifs à fournir

Les normes suivantes peuvent être applicables :

g) La norme ISO/SAE 21434:2021 décrit la manière de définir le concept, ce qui inclut également la prise en compte d'éléments critiques sur la base de décisions en matière de traitement des risques. Les résultats sont documentés dans les produits de travail « [WP-09-03] Objectifs en matière de cybersécurité » et « [WP-09-06] Concept de cybersécurité ». On y trouve aussi une description exhaustive de l'appréciation des risques dans l'article 15 « Méthodes d'analyse des menaces et d'évaluation des risques », dont les résultats sont documentés dans le produit de travail « [WP-09-02] Analyse des menaces et évaluation des risques » ;

h) La norme ISO PAS 5112 peut être utilisée ;

i) La norme ETSI TS 103 645 peut être utilisée pour démontrer la sécurité des éléments de l'Internet des objets d'un véhicule ;

j) La norme BSI PAS 1885 peut être utilisée.

Les éléments suivants pourraient servir à démontrer le respect de cette prescription :

k) Le type de véhicule visé ;

l) Une explication de la raison pour laquelle certains éléments sont critiques dans le type de véhicule ;

m) Les mesures de sécurité mises en œuvre, ainsi que des informations sur leur mode de fonctionnement ;

n) Les informations relatives à chacune des mesures de sécurité devraient permettre au service technique et à l'autorité d'homologation d'être sûrs de faire ce que le constructeur avait prévu et de s'assurer que les véhicules en cours de production utiliseront les mêmes mesures que celles qui ont été soumises à l'autorité d'homologation et au service technique pour le type de véhicule. La confidentialité de certains détails et la manière de la traiter devrait faire l'objet d'un accord et être consignée.

AB. Paragraphe 7.3.4

« 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 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 constructeur est tenu de fournir des arguments raisonnés à l'appui de ces mesures, prouver qu'il les a mises en œuvre dans la conception du type de véhicule et qu'elles sont suffisantes. Cela peut se faire à l'aide d'hypothèses pertinentes, concernant par exemple les systèmes extérieurs qui interagissent avec le véhicule.

Les mesures techniques d'atténuation évoquées dans les parties B et C de l'annexe 5 doivent être prises en considération chaque fois qu'elles sont applicables aux risques qu'il s'agit d'atténuer. Le constructeur peut expliquer pourquoi il considère que les mesures proposées à l'annexe 5 sont « non pertinentes ou insuffisantes », mais aussi pourquoi, selon lui, une autre mesure non énumérée à l'annexe 5 est appropriée dans le cas du risque en question. Cette explication peut être étayée par une évaluation du risque démontrant que la mesure de rechange proposée est appropriée. Cela permet 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 paragraphe 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 identifié signifie atténuation de ce risque.

d) En ce qui concerne la ligne 1 du tableau B.1 figurant dans la partie B de l'annexe 5 : cette ligne ne signifie pas que les messages reçus du Système mondial de navigation par satellite (GNSS) doivent être authentifiés de manière cryptographique par les récepteurs. Le constructeur peut opter pour l'authentification cryptographique ou pour l'utilisation d'autres moyens d'atténuer les risques liés aux messages GNSS incorrects. Il devrait être en mesure de justifier la stratégie mise en œuvre. [PROPOSITION DE REMPLACEMENT 1]

d) Des mesures d'atténuation différentes de celles qui sont énumérées à l'annexe 5 pour les risques associés sont autorisées si une justification est fournie pour expliquer comment cela permet d'atténuer suffisamment le risque visé. Il peut s'agir par exemple d'utiliser diverses sources de détermination de la position en raison de capacités insuffisantes de protection de l'authenticité et de l'intégrité des messages GNSS. [PROPOSITION DE REMPLACEMENT 2]

d) L'expression « non pertinente ou insuffisante » s'applique également aux mesures d'atténuation qui ne sont pas envisageables d'un point de vue technique, ce qui est le cas par exemple lorsqu'un système de messagerie ne permet pas de protéger l'authenticité et l'intégrité des messages. [PROPOSITION DE REMPLACEMENT 3]

Exemples de documents ou de justificatifs à fournir

Les normes suivantes peuvent être applicables :

e) La norme ISO/SAE 21434:2021 décrit l'identification d'un risque ainsi que les objectifs et les concepts en matière de cybersécurité qui en découlent. Les résultats sont documentés dans les produits de travail « [WP-09-03] Objectifs en matière de cybersécurité » et « [WP-09-06] Concept de cybersécurité » ;

f) La norme ISO PAS 5112 ;

g) La norme BSI PAS 11281:2018 et d'autres normes relatives à la présentation d'assertions, d'arguments et d'éléments factuels peuvent être utilisées pour justifier les décisions prises par le constructeur au stade de la conception.

Les éléments suivants pourraient servir à mettre en évidence les mesures d'atténuation prises :

h) La preuve que des mesures d'atténuation ont été prises en fonction de leur nécessité, y compris l'explication de :

i) La raison pour laquelle des mesures d'atténuation autres que celles des parties B et C de l'annexe 5 sont appliquées ;

ii) La raison pour laquelle les mesures d'atténuation énumérées à l'annexe 5 ne sont pas appliquées ;

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

AC. Paragraphe 7.3.5

« 7.3.5 Le constructeur du véhicule doit mettre en œuvre des mesures appropriées et proportionnées pour sécuriser les environnements du type de véhicule prévus (le cas échéant) pour le stockage et l'exécution des logiciels, services, applications ou données du marché secondaire. »

Précisions à prendre en compte

a) Des mesures « appropriées et proportionnées » exigent que le constructeur soit en mesure de justifier la manière dont sont gérés les risques associés à tout environnement prévu, tel que défini dans son appréciation des risques ;

b) Les environnements prévus peuvent se trouver sur le véhicule. Si le véhicule interagit avec des serveurs ou des services situés hors du véhicule (par exemple dans le cloud), ce sont les risques pour le véhicule qui proviennent d'eux, en rapport avec leur cybersécurité, qui doivent être pris en considération.

Exemples de documents ou de justificatifs à fournir

Les normes suivantes peuvent être applicables :

c) La norme ISO/SAE 21434:2021 décrit les étapes à suivre pour tirer des conclusions concernant l'architecture. Le produit de travail « [WP-15-03] Scénarios de menace » recense les menaces potentielles pour le stockage et l'exécution des logiciels, services, applications ou données du marché secondaire. Les mesures appropriées et proportionnées sont décrites dans le produit de travail « [WP-09-06] Concept de cybersécurité ».

d) La norme ISO PAS 5112.

Les éléments suivants pourraient servir à démontrer le respect de cette prescription :

e) Une description de l'environnement prévu ;

f) Les mesures de sécurité mises en œuvre, ainsi que des informations sur leur mode de fonctionnement ;

g) Les informations relatives à chacune des mesures de sécurité devraient permettre au service technique ou à l'autorité d'homologation d'être sûrs de faire ce que le constructeur avait prévu et de s'assurer que les véhicules en cours de production utiliseront les mêmes mesures que celles qui ont été soumises à l'autorité d'homologation ou au service technique pour le type de véhicule. La confidentialité de certains détails et la manière de la traiter devrait faire l'objet d'un accord et être consignée ;

h) L'annexe 5 du Règlement sur la cybersécurité doit servir de référence.

AD. Paragraphe 7.3.6

« 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. »

Explication de la prescription

Les résultats des essais doivent être valables au moment de l'homologation de type. Le service technique peut procéder à des essais de sécurité pour confirmer ces résultats.

Précision à prendre en compte

a) L'objectif de toute mesure de sécurité est de réduire les risques. Les essais devraient justifier les mesures de sécurité mises en œuvre.

Exemples de documents ou de justificatifs à fournir

Les normes suivantes peuvent être applicables :

b) Le constructeur peut décrire les mesures de vérification et de validation mises en œuvre conformément à la norme ISO/SAE 21434:2021, produits de travail « [WP-10-07] Rapport d'intégration et de vérification » et « [WP-11-01] Rapport de validation ».

Les éléments suivants pourraient servir à démontrer le respect de cette prescription :

c) Qu'est-ce qui est soumis à l'essai et pourquoi (par exemple, à quoi peut-on mesurer le succès de l'essai ?) ?

d) Quelle méthode est utilisée et pourquoi (il peut s'agir de notes précisant l'ampleur et la difficulté de l'essai) ?

e) Qui a réalisé l'essai et pourquoi (le constructeur, un fournisseur ou une organisation extérieure, ainsi que toute information pertinente concernant leur qualification et leur expérience) ?

f) La confirmation que le résultat de l'essai est positif (il peut s'agir des critères de réussite ou d'échec ainsi que des résultats eux-mêmes).

AE. Paragraphe 7.3.7

« 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 cyberattaques et les cyberattaques. »

Explication de la prescription

Cette prescription vise à s'assurer que sont mises en œuvre pour le type de véhicule des mesures spécifiques permettant de détecter des changements dans le contexte des menaces ainsi que de prévenir les cyberattaques, et aussi qu'existent des capacités d'analyse des tentatives de cyberattaques, qu'elles aient réussi ou non.

Précisions à prendre en compte

a) Les mesures relatives à cette prescription peuvent être appliquées sur le type de véhicule ou dans son environnement opérationnel, par exemple le système principal ou le réseau mobile « pour le type de véhicule » ;

b) Les mesures doivent viser avant tout à empêcher les cyberattaques de réussir, conformément aux paragraphes 7.3.4 et 7.3.5, afin d'assurer la protection contre les risques répertoriés dans l'évaluation des risques ;

c) Les mesures destinées à empêcher les cyberattaques de réussir contre tous les véhicules d'un type donné peuvent aussi être appliquées de manière asynchrone, c'est-à-dire après une cyberattaque effective et l'analyse de celle-ci ;

d) Les capacités de traitement des données peuvent inclure la capacité de fournir et d'analyser des données enregistrées, des codes d'erreur de diagnostic, des informations opérationnelles sur le véhicule et des informations du système principal pour enquêter sur les cyberattaques ;

e) Les capacités de traitement des données peuvent inclure une mémoire tampon circulaire (journal dynamique) à l'appui des procédures d'enquête.

Il est à noter que le paragraphe 1.3 et le respect de la législation sur la protection des données revêtent une importance particulière pour cette prescription.

Exemples de documents ou de justificatifs à fournir

Les normes suivantes peuvent être applicables :

f) La norme ISO/SAE 21434:2021. Le recensement des sources pour la surveillance de la cybersécurité est prévu dans l'exigence [RQ-08-01] et documenté dans le produit de travail « [WP-08-01] Sources d'information sur la cybersécurité ». Les résultats de l'analyse et la façon de les documenter sont décrits dans le produit de travail « [WP-08-05] Analyse des vulnérabilités ».

Les éléments suivants pourraient servir à démontrer le respect de cette prescription :

g) Les mesures destinées à empêcher les cyberattaques appliquées au type de véhicule ;

h) La démonstration de la manière dont fonctionnent les mesures préventives et les activités de surveillance pour un type de véhicule ;

i) La démonstration de la manière dont il est procédé à l'analyse.

AF. Paragraphe 7.3.8

« 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. »

Précisions à prendre en compte

Une norme consensuelle peut être une norme reconnue internationalement, ou une norme nationale communément utilisée, par exemple la norme FIPS.

Explication de la prescription

Cette prescription vise à s'assurer que les méthodes de cryptage utilisées peuvent être justifiées.

Exemples de documents ou de justificatifs à fournir

Lorsque des mesures de cryptage sont appliquées, sur la base des résultats de l'analyse et de l'évaluation des risques, le constructeur doit être en mesure :

a) D'expliquer si l'algorithme ou la mesure de cryptage est conforme à la norme de consensus actuelle ; et

b) D'expliquer la raison du choix du cryptage et pourquoi il permet d'atténuer de manière appropriée le risque identifié.

AG. Paragraphe 7.4

« 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. »

Explication de la prescription

L'objectif principal de cette prescription est de confirmer que les aspects du CSMS liés aux activités de surveillance de la cybersécurité telles qu'elles sont définies à l'alinéa g) du paragraphe 7.2.2.2 continuent à s'appliquer correctement après la phase de développement et que les mesures d'atténuation des cyberattaques mises en œuvre restent efficaces.

Le constructeur doit rendre des comptes au moins une fois par an à l'autorité d'homologation qui a délivré l'homologation ou au service technique qui a vérifié la conformité de son CSMS au Règlement. Il doit le faire plus souvent si des événements tels que des cyberattaques se produisent, surtout pour faire savoir quelles mesures ont été prises.

Exemples de documents ou de justificatifs à fournir

Les normes suivantes peuvent être applicables :

a) La norme ISO/SAE 21434:2021 définit les produits de travail « [WP-08-04] Faiblesses découlant d'incidents de cybersécurité » et « [WP-08-06] Preuves de la gestion des vulnérabilités ». Les deux peuvent servir de base pour les rapports requis ;

b) La norme ISO PAS 5112.

AH. Paragraphe 7.4.2

« 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. »

Le présent document ne comporte aucune indication concernant cette prescription.

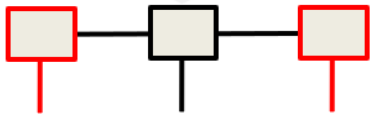
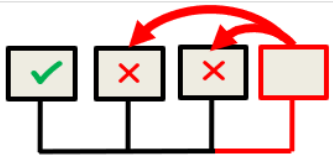
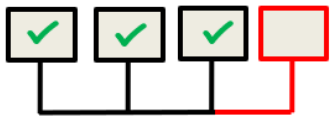
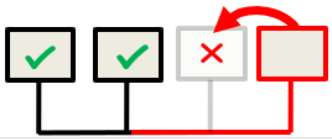
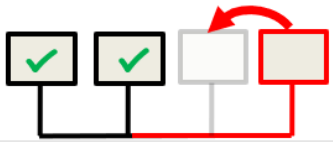
AI. Paragraphe 8

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

Exemples de documents ou de justificatifs à fournir

Le tableau suivant donne quelques exemples de modifications de l'architecture des systèmes électriques/électroniques (E/E) et de leurs répercussions potentielles sur le type de véhicule eu égard au Règlement.

Il est à noter que les exemples sont donnés à titre indicatif et qu'il ne s'agit pas d'une liste exhaustive. Lorsqu'elles sont appliquées, les modifications ci-dessous peuvent produire des résultats différents.

		Modifications possibles de l'architecture E/E	Impact sur le type	Exemples
Nouveau type	**Développement d'une nouvelle architecture E/E**		Le développement d'une nouvelle architecture E/E exige un **nouveau type**	Le développement d'une nouvelle architecture E/E exige **un nouveau type**
Nouveau type	**Modification des résultats de l'évaluation des risques sous l'effet de l'introduction de nouvelles technologies**		Exige un **nouveau type** car la sécurité du sous-système existant est affectée	• L'adjonction de nouvelles interfaces externes (communication en champ proche CCP) pour de nouveaux services tels que la personnalisation • La modification de la topologie du réseau par l'adjonction d'une nouvelle passerelle
Extension du type existant	**Modification mineure des résultats de l'évaluation des risques sous l'effet de l'adjonction ou du remplacement de sous-systèmes**	 	Le remplacement d'un sous-système existant ou l'adjonction d'un nouveau sous-système, ce qui introduit quelques modifications mineures au niveau de la cybersécurité de l'architecture E/E qui en résulte et **exige donc une extension de l'homologation de type**	• Le remplacement d'une unité de communication UMTS par une unité de communication 5G -> communication supplémentaire possible • Le remplacement d'une UCE par une nouvelle équipée d'un module de sécurité matériel (HSM)
Pas d'impact	**Aucune modification des résultats de l'évaluation des risques**		Le remplacement d'un sous-système existant, ce qui ne modifie pas la cybersécurité de l'architecture E/E qui en résulte et **n'exige donc pas d'extension de l'homologation de type.** **Cette situation est la plus courante.**	Le remplacement d'une UCE : • Nouveau processeur dernier cri, davantage de mémoire, pas de nouvelle fonctionnalité, fournisseur différent mais même performance technique

AJ. Paragraphes 9 à 12

« 9. Conformité de la production

10. Sanctions pour non-conformité de la production

11. Arrêt définitif de la production

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

Le présent document ne comporte aucune indication concernant ces prescriptions.

4. Orientations concernant la fiche de renseignements de l'annexe 1

A. Paragraphes 9 et 9.1

« 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. »

Exemples de documents ou de justificatifs à fournir

Une description écrite de l'architecture E/E.

B. Paragraphe 9.2

« 9.2 Représentation schématique du type de véhicule »

Exemples de documents ou de justificatifs à fournir

Une description schématique de l'architecture E/E ; par exemple, un schéma du circuit électrique.

C. Paragraphes 9.3 à 9.8

« 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 : »

Le présent document ne comporte aucune indication concernant ces dispositions.

5. Modèle pour l'échange de données par l'intermédiaire de la base DETA, conformément au paragraphe 5.3

Note importante

Les informations obtenues via la base de données DETA pour les besoins du système de partage de l'information défini dans le Règlement ONU doivent être protégées de manière sécurisée. Elles ne doivent pas être utilisées à d'autres fins que l'homologation de type d'un véhicule et la certification du système de gestion de la cybersécurité pour le type de véhicule.

5.1 Description de l'audit du CSMS

Aux fins de la description de l'audit du CSMS, l'autorité d'homologation doit fournir les informations suivantes à la base DETA.

5.1.1 Processus d'audit

Les coordonnées de l'autorité d'homologation et de son unité responsable du processus d'audit doivent être communiquées.

Le processus d'audit doit être décrit dans un diagramme de décision comportant éventuellement des étapes itératives et des étapes de correction.

(Diagramme de décision)

La chronologie du déroulement de l'audit doit être consignée sous la forme d'un tableau.

Phase de l'audit	*Date de début/durée*	*Ressources nécessaires (en jour-homme)*
Audit préalable, en cas de besoin *Par exemple, participation des auditeurs aux processus de production, planification de l'audit, ajustement du déroulement des opérations*		
Remise des documents		
Préparation aux activités d'audit *Notamment : examiner les documents, les classer, vérifier s'ils sont complets, vérifier leur contenu*		
Audit sur place		
Évaluation des efforts de rectification *Par exemple, les rectifications auxquelles il est procédé pendant l'audit peuvent porter sur des constatations qui viennent d'être faites*		
Élaboration et distribution du rapport d'audit		
Constatations faites au cours de l'audit		

Phase de l'audit	*Date de début/durée*	*Ressources nécessaires (en jour-homme)*
Examen des constatations et rectifications par le demandeur (le cas échéant)		
Fin de l'audit		

Des informations supplémentaires concernant les phases de l'audit peuvent être consignées dans le tableau ci-dessous si cela semble utile.

Phase de l'audit	*Remarques*

Les informations doivent également porter sur le déroulement des mesures d'audit conformes aux paragraphes 6.8 et 6.10 du Règlement ONU nº 155 ainsi que de revérification conformément au paragraphe 6.10 du même Règlement.

5.1.1.1 Audit sur place

Si des évaluations sur place du CSMS du demandeur font partie du processus d'audit, le déroulement et les principes de base (justification) de ces évaluations doivent être décrits.

5.1.1.2 Traitement des résultats et efforts de rectification

Cette section décrit le déroulement des efforts de rectification entrepris par le demandeur en réaction aux conclusions de l'audit.

(Ce déroulement devrait être inclus dans le diagramme de décision du paragraphe 5.1.1.)

5.1.1.3 Exemples de formulaires de demande

Un exemplaire du formulaire de demande de certification du CSMS doit être fourni.

5.1.1.4 Référence à des normes et spécifications

Référence doit être faite aux normes, spécifications ou autres documents extérieurs sur la base desquels s'appuie le processus d'audit.

5.1.2 Exigences de qualification et mise en place de l'équipe d'audit

Les exigences de qualification minimales de l'autorité d'homologation applicables aux services techniques et aux auditeurs qui procèdent à l'évaluation du CSMS doivent être précisées. Les fonctions au sein d'une équipe d'audit potentielle doivent être énumérées et assorties de qualifications.

5.1.2.1 Équipe d'audit potentielle

Fonctions *Exemples*	*Effectifs requis* *Exemples*	*Tâches/remarques* *Exemples*
Auditeur principal	*1*	*Diriger le processus d'audit ; comptable et responsable*
Expert en matière de processus de cybersécurité	*2*	*Responsable de l'audit des processus ; dans l'idéal, le personnel devrait être le même que celui de l'équipe d'évaluation de l'homologation de type*
Spécialiste de produit	*1*	*…*
…	*…*	
Gestion de la documentation		

5.1.2.2 Exigences de qualification

Qualification	*Fonction concernée*	*Exigences minimales*	*Preuve*
Formation	*Exemple : auditeur principal, expert en matière de processus £de cybersécurité*	*Exemple : diplôme universitaire en informatique, mathématiques, physique ou ingénierie ou équivalent*	*Exemple : diplôme ou certificat*
Expérience professionnelle		*Exemple : cinq ans d'expérience professionnelle, dont deux ans dans le domaine de la sécurité informatique*	*Exemple : références professionnelles*
Expérience pratique			
Formation complémentaire			
Certifications			

5.1.3 Exigences concernant l'audit

Les exigences concernant l'audit doivent être énumérées dans cette section. Elles doivent être jugées suffisantes, par l'autorité d'homologation, pour prouver que toutes les prescriptions énoncées aux paragraphes 7.2.2.1 à 7.2.2.5 sont respectées par le constructeur (y compris les homologations de type antérieures au 1er juillet 2024).

Elles devraient comporter un exposé justificatif permettant de décider si la cybersécurité a été abordée de manière adéquate au cours de la phase de développement du type de véhicule.

5.1.3.1 Exigences formelles

Dans le cas où des exigences formelles sont fixées par l'autorité d'homologation, elles doivent être indiquées ici. Il peut s'agir d'exiger des certifications, des permis et des licences, par exemple.

Exigence formelle	*Version/édition, date*
Par exemple : certification ISO 27001	

5.1.3.2 Informations requises

Dans cette section, il convient de fournir une liste structurée des documents que l'organe d'audit doit recevoir de l'entité auditée. Toute exigence formelle en matière de documentation doit y figurer.

Note : Il pourrait notamment s'agir d'une liste de points qui doivent être abordés. Une référence aux documents exigés par des normes telles que les normes ISO/SAE 21434 et ISO PAS 5112 est également possible.

5.1.3.3 Évaluation des documents

Dans cette section, il faut fournir des détails concernant la justification de l'évaluation des documents reçus. Il doit s'agir de quelques critères d'évaluation généraux qui s'appliquent à tous les documents, indiquant notamment qu'ils sont contrôlés, utilisés, accessibles, en cours de révision, etc.

N°	*Titre*	*Description*	*Remarques*	*Justification de l'évaluation*
1				*Note* : Les justifications doivent être à différents niveaux. Le niveau d'intégration des procédures (pour s'assurer qu'elle sont pertinentes les unes par rapport aux autres) doit être en relation avec les prescriptions
2				

5.1.3.4 Questionnaire d'audit

<Domaine d'intervention 1 (par exemple, analyse des menaces)>

Prescription	*Question d'audit*	*Objet/but de la question*	*Critères de performances minimaux*	*Meilleure pratique*	*Informations supplémentaires/contexte*[1]

<Domaine d'intervention 2 (*par exemple, gestion des risques*)>

Prescription	*Question d'audit*	*Objet/but de la question*	*Critères de performances minimaux*	*Meilleure pratique*	*Informations supplémentaires/contexte*[1]

5.2 Description de l'homologation

5.2.1 Processus d'homologation

Les coordonnées de l'autorité d'homologation et de son unité responsable du processus d'homologation doivent être communiquées.

Le processus d'homologation doit être documenté dans un diagramme de décision.

(Diagramme de décision)

5.2.2 Exigences de qualification et mise en place de l'équipe des évaluateurs

Les exigences de qualification minimales de l'autorité d'homologation applicables aux services techniques qui procèdent à l'évaluation en vue de l'homologation de type doivent être précisées. Les fonctions au sein d'une équipe d'évaluation potentielle doivent être énumérées et attribuées en fonction des qualifications.

5.2.2.1 Équipe d'évaluation potentielle

Fonction Exemples	*Effectifs requis*	*Tâches/remarques*
Vérificateur principal	*1*	*Diriger les processus d'évaluation ; comptable et responsable*
Expert en matière de processus de cybersécurité	*1*	*Responsable du transfert des connaissances du fonctionnement du CSMS à l'évaluation du type de véhicules ; dans l'idéal, le personnel serait le même que celui de l'équipe d'audit du CSMS*

[1] Le cas échéant, les circonstances dans lesquelles les questions peuvent être posées ou omises, ou les variations possibles en fonction du contexte, etc.

Fonction *Exemples*	*Effectifs requis*	*Tâches/remarques*
Spécialiste de produit de cybersécurité	*2*	
Responsable de l'essai de pénétration	*1-2*	
…		
Gestion des documents		

5.2.2.2 Exigences de qualification

Qualification	*Fonction concernée*	*Exigences minimales*	*Preuve*
Formation	*Exemple : vérificateur principal, expert en produits*	*Exemple : diplôme universitaire en informatique, mathématiques, physique ou ingénierie ou équivalent*	*Exemple : diplôme ou certificat*
Expérience professionnelle		*Exemple : cinq ans d'expérience professionnelle, dont deux ans dans le domaine de la sécurité informatique*	*Exemple : références professionnelles*
Expérience pratique		*Exemple : expérience dans les domaines de l'architecture E/E automobile ainsi que de l'évaluation de la cybersécurité et des essais de pénétration*	*Exemple : références du travail ou du projet*
Formation complémentaire			
Certifications			

5.2.3 Exigences concernant l'évaluation

Cette section concerne les moyens permettant de déterminer si le constructeur du véhicule a bien pris les mesures mentionnées au paragraphe 5.1.1.

5.2.3.1 Mesures d'évaluation générales

Il doit s'agir de mesures que l'autorité d'homologation juge suffisantes pour permettre de vérifier que :

a) Le certificat du CSMS correspond au type de véhicule en voie d'homologation.

Gestion des risques

b) Le constructeur du véhicule a pris des mesures suffisantes pour répertorier et gérer, pour le type de véhicule en voie d'homologation, les risques liés aux fournisseurs, compte tenu notamment les normes requises pour une telle gestion des risques.

Définition des risques

c) Le constructeur du véhicule a identifié les éléments critiques du type de véhicule ;

d) Les « éléments critiques » ont été définis ;

e) Le constructeur du véhicule a procédé à une appréciation complète des risques pour le type de véhicule, comme il est prescrit au paragraphe 7.3.3 du Règlement.

Atténuation des risques

f) Le type de véhicule est protégé contre les risques répertoriés dans le cadre de l'appréciation des risques effectuée par le constructeur ;

g) Les mesures d'atténuation prises par le constructeur sont proportionnées et une explication est donnée de l'interprétation de l'adjectif « proportionnées » ;

h) Les raisons permettant d'affirmer, le cas échéant, que les mesures d'atténuation mentionnées dans les parties B et C de l'annexe 5 ne sont pas pertinentes, insuffisantes pour le risque identifié ou irréalisables ;

i) Les « autres mesures d'atténuation » mises en œuvre par le constructeur en vertu du paragraphe 7.3.4 sont « appropriées ».

Surveillance et intervention

j) Les principes à la base du CSMS qui permettent de surveiller les menaces et d'intervenir en cas d'incident éventuel ont été pleinement appliqués au type de véhicule et sont effectivement en place ;

k) L'efficacité et l'efficience des mesures d'atténuation appliquées ont été soumises à essai et feront l'objet d'une surveillance.

L'autorité d'homologation doit exposer de manière détaillée les normes d'évaluation utilisées dans le cadre de la vérification ci-dessus.

2.3.2 Exigences concernant les documents

La liste des documents et du contenu qui en est principalement attendu doit être établie. Les documents doivent permettre d'évaluer les prescriptions énumérées au paragraphe 2.3.1.

2.3.3 Évaluation technique

La stratégie d'évaluation technique doit être élaborée. Elle doit inclure les essais et la manière de les appliquer pour vérifier que le constructeur a mis en œuvre les mesures de sécurité que le règlement exige et qu'il a lui-même documentées. La stratégie d'essais doit tenir compte des essais effectués par des tiers, *par exemple ceux qu'ont réalisés des services techniques ou des fournisseurs de services, des sous-traitants du constructeur ou des institutions de recherche, qu'ils aient été suscités par le constructeur ou par des autorités d'homologation*.

La stratégie utilisée pour reproduire les essais du constructeur doit aussi être incluse.

Note : Même si les mesures d'évaluation mentionnées au paragraphe 2.3.1 sont censées inclure l'évaluation d'essais précédents documentés par le constructeur, la stratégie utilisée pour les reproduire doit justifier le choix des essais à reproduire et de la manière de procéder pour ce faire.

6. Liens avec la norme ISO/SAE 21434:2021 (E)

Le tableau suivant résume les liens entre les prescriptions du Règlement et les paragraphes pertinents de la norme ISO/SAE 21434:2021.

Paragraphe	*Articles de la norme ISO/SAE 21434:2021*
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 ce système est conforme au présent Règlement	
Vérifier qu'un système de gestion de la cybersécurité est en place	Articles 5, 6, 8
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 : • Phase de développement ;	

• Phase de production ; • Phase de postproduction.	
Phase de développement	Articles 7, 8, 9, 10, 11
Phase de production	Article 8, 12
Phase de postproduction	Articles 7, 8, 13, 14
7.2.2.2 a) Les processus mis en œuvre en interne par le constructeur pour gérer la cybersécurité	
Politique de cybersécurité à l'échelle de l'organisation	[RQ-05-01]
Gestion des processus pertinents en matière de cybersécurité	[RQ-05-02], [RQ-05-08]
a3) Instauration et maintien d'une culture et d'une vigilance en matière de cybersécurité	[RQ-05-06], [RQ-05-07]
7.2.2.2 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	
b1) Processus établi qui permette de répertorier les risques de cybersécurité auxquels chaque type de véhicule est exposé tout au long des phases de développement, de production et de postproduction	[RQ-15-01], [RQ-15-02], [RQ-15-03], [RQ-15-08], [RQ-15-09]. Les menaces recensées à l'annexe 5 du Règlement ONU nº 155 sortent du cadre de la norme ISO/SAE 21434:2021
7.2.2.2 c) Les processus mis en œuvre pour apprécier, catégoriser et traiter les risques répertoriés	
c1) Y a-t-il un processus établi qui permette d'apprécier et de catégoriser les risques de cybersécurité auxquels chaque type de véhicule est exposé tout au long des phases de développement, de production et de postproduction ?	[RQ-15-15], [RQ-15-04], [RQ-05-05], [RQ-15-10], [RQ-15-16]
c2) Y a-t-il un processus établi qui permette de traiter les risques de cybersécurité auxquels chaque type de véhicule est exposé tout au long des phases de développement, de production et de postproduction ?	[RQ-15-17], [RQ-09-05], [RQ-09-06]
7.2.2.2 d) Les processus en place pour vérifier que les risques répertoriés sont correctement gérés	
d1) Y a-t-il un processus établi qui permette de vérifier que les risques répertoriés sont correctement gérés ?	[RQ-09-07], [RQ-09-11], [RQ-11-01]
e) Les processus mis en œuvre pour contrôler la cybersécurité d'un type de véhicule	
e1) Y a-t-il un processus établi qui permette de spécifier les prescriptions en matière de cybersécurité ?	[RQ-09-09], [RQ-10-01]
e2) Y a-t-il un processus établi qui permette de valider les prescriptions en matière de cybersécurité au cours de la phase de développement ?	[RQ-11-01]

e3) Y a-t-il un processus établi qui permette de valider les prescriptions en matière de cybersécurité au cours de la phase de production ?	[RQ-12-01], [RQ-12-02]
7.2.2.2 f) Les processus mis en œuvre pour garantir que l'appréciation des risques est actualisée	
f1) Y a-t-il un processus établi qui permette de garantir que l'appréciation des risques est actualisée ?	[RQ-08-07], [RQ-06-09], [RQ-07-06]
7.2.2.2 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	
g1) Y a-t-il un processus établi qui permette de surveiller les informations en matière de cybersécurité ?	[RQ-08-01]
g2) Y a-t-il un processus établi qui permette de détecter les incidents de cybersécurité ?	[RQ-08-02], [RQ-08-03]
g3) Y a-t-il un processus établi qui permette d'évaluer les incidents de cybersécurité et d'analyser les vulnérabilités en la matière ?	[RQ-08-04], [RQ-08-05], [RQ-08-06]
g4) Y a-t-il un processus établi qui permette de gérer les vulnérabilités qui ont été répertoriées ?	[RQ-08-07], [RQ-08-08], [RQ-07-06], [RC-07-08]
g5) Y a-t-il un processus établi qui permette de réagir aux incidents de cybersécurité ?	[RQ-13-01], [RQ-13-02]
g6) Y a-t-il un processus établi qui permette de valider l'efficacité de la réaction ?	[RQ-11-01]
7.2.2.2 h) Les processus mis en œuvre pour recueillir les données utiles à l'analyse des tentatives de cyberattaques et des cyberattaques	
Y a-t-il un processus établi qui permette de fournir des données pertinentes à l'appui de l'analyse ?	[RQ-08-01], [RQ-08-02], [RQ-08-03]
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, sur la base des catégories mentionnées aux alinéas c) et g) du paragraphe 7.2.2.2, que les cybermenaces et les vulnérabilités auxquelles il doit réagir sont atténuées dans un délai raisonnable	
Atténuation dans un délai raisonnable	Pas de délai fixé par la norme ISO/SAE 21434:2021 [RQ-08-07], [RQ-08-08]
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.	

Surveillance après la première immatriculation	Article 8.3 « Surveillance de la cybersécurité »
Capacité d'analyser et de détecter les cybermenaces, les vulnérabilités et les cyberattaques à partir des données et des journaux du véhicule	8.4 « Évaluation des incidents de cybersécurité » 8.5 « Analyse des vulnérabilités »
Respect des droits des propriétaires ou des conducteurs des véhicules en matière de vie privée, en particulier s'agissant du consentement	Hors du champ d'action de la norme ISO/SAE 21434:2021, qui n'est donc pas applicable
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	
Dépendances pouvant exister avec les fournisseurs	[RQ-06-10], [RQ-07-04], [RC-07-05]
Dépendances pouvant exister avec les prestataires de services	[RQ-06-10], [RQ-07-04], [RC-07-05]
Dépendances pouvant exister avec les sous-entités du constructeur	[RQ-06-10], [RQ-07-04], [RC-07-05]

B. Partie B

Lignes directrices relatives à l'utilisation de la base DETA pour échanger des informations concernant la cybersécurité (en application du Règlement ONU nº 155)

I. Introduction

1. Le présent document d'orientation a pour objet de guider les autorités d'homologation des Parties contractantes à l'Accord de 1958 dans l'utilisation de la base DETA pour la mise en œuvre du Règlement ONU nº 155 énonçant des prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne la cybersécurité et de leurs systèmes de gestion de la cybersécurité (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).

2. Le présent document d'orientation ne modifie en rien les dispositions du Règlement ONU nº 155. En cas de divergence entre les directives et le texte du Règlement ONU, c'est ce dernier qui prévaut.

3. Le présent document d'orientation s'entend sans préjudice d'autres lignes directrices, règles et instructions de manuels, modes d'emploi, instructions en matière d'administration clientèle, directives ou tout autre document de la base DETA.

4. Aux fins des présentes lignes directrices, on entend par « DETA » la « Base de données pour l'échange de renseignements sur les homologations de type, établie par la Commission économique pour l'Europe ».

II. Principes généraux de l'échange d'informations sur la cybersécurité par l'intermédiaire de la base DETA

5. Paragraphes du Règlement ONU nº 155 pertinents pour l'utilisation de la base DETA :

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.

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, 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.

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.

6. La section 5 ci-dessus a pour effet que, dans le cas général d'utilisation de la base DETA, l'autorité d'homologation qui s'apprête à délivrer une homologation de type en vertu du Règlement ONU nº 155 (ci-après appelée « autorité émettrice ») :

a) Télécharge les informations requises concernant la cybersécurité dans la base DETA ;

b) En informe les autres autorités en ajoutant un message de notification dans la base DETA.

7. Les informations concernant la cybersécurité téléchargées dans la base DETA ne sont accessibles qu'aux Parties contractantes appliquant le Règlement ONU nº 155. Le message de notifications est visible par tous les utilisateurs de la base DETA.

III. Lignes directrices générales concernant l'utilisation de la base DETA pour échanger des informations sur la cybersécurité

8. L'autorité émettrice doit procéder comme suit :

a) Toutes les informations relatives à la cybersécurité mentionnées au paragraphe 5.3.2 du Règlement ONU nº 155 doivent être réunies dans un ou plusieurs fichiers PDF. Ces fichiers doivent être téléchargés en tant que parties de document du type « OTHER » ;

b) Un certain nombre d'attributs peuvent être saisis. Il faut remplir au moins les champs obligatoires, à savoir :

i) Le « numéro d'homologation », qui doit être réservé par l'autorité d'homologation ;

ii) La « date d'homologation » à laquelle l'homologation doit être délivrée. Cette date doit se situer au moins 14 jours après la date de notification aux autres autorités ;

iii) Le « statut d'homologation », qui doit correspondre à « en cours » ;

c) L'autorité émettrice saisit alors la notification proprement dite dans l'onglet « News ». Cette notification comporte au minimum le texte standard et le numéro d'homologation, de sorte que l'on puisse retrouver les informations correspondantes dans la base DETA :

« *L'autorité d'homologation de [nom du pays] avise par la présente les autorités d'homologation des autres Parties contractantes appliquant le Règlement ONU nº 155 des méthodes et critères servant de base pour évaluer le caractère approprié des mesures prises conformément au présent Règlement et en particulier aux paragraphes 5.1, 7.2 et 7.3. Veuillez vous référer à l'homologation de type nº […] pour les détails.* ».

Note : « News » n'est pas un système postal. Les autres utilisateurs ne peuvent voir les messages qu'après avoir accédé au système. C'est la raison pour laquelle les présentes lignes directrices recommandent aux autorités d'homologation de vérifier quotidiennement la section « News » de la base DETA ;

d) Lorsque, 14 jours au moins après avoir envoyé son message de notification aux autres, l'autorité émettrice décide de délivrer l'homologation de type, elle doit le plus vite possible :

i) Compléter tous les attributs nécessaires, y compris la valeur finale de la « date d'homologation » ;

ii) Télécharger les parties du document des types « CERT », « IF » et « TR ».

9. Les autres autorités d'homologation des Parties contractantes appliquant le Règlement ONU nº 155 qui prennent note du message de notification de l'autorité émettrice peuvent soumettre des observations à l'autorité émettrice dans un délai de 14 jours à partir de la notification. Elles doivent alors :

a) Envoyer à l'autorité émettrice un courriel contenant toutes les informations pertinentes ;

b) Ajouter un message dans l'onglet « News » pour informer les autres autorités que des observations ont été soumises à l'autorité émettrice. Ce message doit comporter au minimum le texte standard et le numéro d'homologation, comme suit :

« *L'autorité d'homologation de [nom du pays] informe par la présente les autorités d'homologation des autres Parties contractantes appliquant le Règlement ONU* nº *155 que des observations ont été soumises au sujet de la notification publiée par l'autorité d'homologation de [nom du pays]. Veuillez vous référer à l'homologation de type nº […] pour les détails.* ».

L'autorité émettrice ajoute, dans un délai raisonnable, les observations reçues à la base DETA, en les téléchargeant, en tant que fichier PDF du type de document « OTHER », dans la même section que les documents originaux.

Note : Il faut procéder ainsi pour ne divulguer des informations confidentielles ou protégées qu'aux Parties contractantes appliquant le Règlement ONU nº 155.

10. Les sections 8 et 9 ci-dessus s'appliquent avant qu'une homologation soit délivrée en vertu du Règlement ONU nº 155 pour la première fois et chaque fois que les méthodes ou les critères sont actualisés.