No. 4789. Multilateral

AGREEMENT CONCERNING THE ADOPTION OF HARMONIZED TECHNICAL UNITED NATIONS REGULATIONS FOR WHEELED VEHICLES, EQUIPMENT AND PARTS WHICH CAN BE FITTED AND/OR BE USED ON WHEELED VEHICLES AND THE CONDITIONS FOR RECIPROCAL RECOGNITION OF APPROVALS GRANTED ON THE BASIS OF THESE UNITED NATIONS REGULATIONS. GENEVA, 20 MARCH 1958 [*United Nations, Treaty Series, vol. 335, I-4789.*]

UNITED NATIONS REGULATION NO. 155. UN REGULATION ON UNIFORM PROVISIONS CONCERNING THE APPROVAL OF VEHICLES WITH REGARD TO CYBER SECURITY AND OF THEIR CYBERSECURITY MANAGEMENT SYSTEMS. GENEVA, 24 JUNE 2020[*]

Entry into force: 22 January 2021, in accordance with article 1(4)

Authentic texts: English, French and Russian

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record. The Text(s) reproduced below, if attached, are the authentic texts of the agreement /action attachment as submitted for registration and publication to the Secretariat. For ease of reference they were sequentially paginated. Translations, if attached, are not final and are provided for information only.*

Nº 4789. Multilatéral

ACCORD CONCERNANT L'ADOPTION DE RÈGLEMENTS TECHNIQUES HARMONISÉS DE L'ONU APPLICABLES AUX VÉHICULES À ROUES ET AUX ÉQUIPEMENTS ET PIÈCES SUSCEPTIBLES D'ÊTRE MONTÉS OU UTILISÉS SUR LES VÉHICULES À ROUES ET LES CONDITIONS DE RECONNAISSANCE RÉCIPROQUE DES HOMOLOGATIONS DÉLIVRÉES CONFORMÉMENT À CES RÈGLEMENTS. GENÈVE, 20 MARS 1958 [*Nations Unies, Recueil des Traités, vol. 335, I-4789.*]

RÈGLEMENT DE L'ONU N° 155. 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. GENÈVE, 24 JUIN 2020[*]

Entrée en vigueur : 22 janvier 2021, conformément au paragraphe 4 de l'article 1

Textes authentiques : anglais, français et russe

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Aucun numéro de volume n'a encore été attribué à ce dossier. Les textes disponibles qui sont reproduits ci-dessous sont les textes originaux de l'accord ou de l'action tels que soumis pour enregistrement. Par souci de clarté, leurs pages ont été numérotées. Les traductions qui accompagnent ces textes ne sont pas définitives et sont fournies uniquement à titre d'information.*

[ENGLISH TEXT – TEXTE ANGLAIS]

Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

Submitted by the Working Party on Automated/autonomous and Connected Vehicles *

The text reproduced below, proposing a new UN Regulation on on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system, was drafted by the Task Force on Cyber Security and Over-the-Air issues and reviewed by GRVA. It was produced in accordance with the Framework Document on the safety of Automated Vehicles ECE/TRANS/WP.29/2019/34 as revised. It was adopted by the Working Party on Automated/autonomous and Connected Vehicles at its fifth session, see ECE/TRANS/WP.29/GRVA/6, para. 23., based on ECE/TRANS/WP29/GRVA/2020/3 as amended by GRVA-06-19-Rev.1. It is submitted to the World Forum for Harmonization of Vehicle Regulations (WP.29) and its Administrative Committee for the 1958 Agreement (AC.1) for consideration and vote at their June 2020 sessions.

GRVA was not in the position to finalize the drafting of paragraph 5.3. due to the lack of time. The Contracting Parties having expressed a position on this paragraph volunteered to further discuss after the session and to prepare a document solving the issue on para. 5.3. and subparagraphs complementing this document. This document is bearing the official symbol ECE/TRANS/WP.29/2020/97.

* In accordance with the programme of work of the Inland Transport Committee for 2020 as outlined in proposed programme budget for 2020 (A/74/6 (part V sect. 20) para 20.37), the World Forum will develop, harmonize and update UN Regulations in order to enhance the performance of vehicles. The present document is submitted in conformity with that mandate.

UN Regulation on uniform provisions concerning the approval of vehicles with regard to cyber security and of their cybersecurity management systems

Contents

** Page numbers will be added at a later stage.

1. Scope

1.1. This Regulation applies to vehicles, with regard to cyber security, of the Categories M and N.

This Regulation also applies to vehicles of Category O if fitted with at least one electronic control unit.

1.2. This Regulation also applies to vehicles of the Categories L_6 and L_7 if equipped with automated driving functionalities from level 3 onwards, as defined in the reference document with definitions of Automated Driving under WP.29 and the General Principles for developing a UN Regulation on automated vehicles (ECE/TRANS/WP.29/1140).

1.3. This Regulation is without prejudice to other UN Regulations, regional or national legislations governing the access by authorized parties to the vehicle, its data, functions and resources, and conditions of such access. It is also without prejudice to the application of national and regional legislation on privacy and the protection of natural persons with regard to the processing of their personal data.

1.4. This Regulation is without prejudice to other UN Regulations, national or regional legislation governing the development and installation/system integration of replacement parts and components, physical and digital, with regards to cybersecurity.

2. Definitions

For the purpose of this Regulation the following definitions shall apply:

2.1. "*Vehicle type*" means vehicles which do not differ in at least the following essential respects:

(a) The manufacturer's designation of the vehicle type;

(b) Essential aspects of the electric/electronic architecture and external interfaces with respect to cyber security.

2.2. "*Cyber security*" means the condition in which road vehicles and their functions are protected from cyber threats to electrical or electronic components.

2.3. "*Cyber Security Management System (CSMS)*" means a systematic risk-based approach defining organisational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyber-attacks.

2.4. "*System*" means a set of components and/or sub-systems that implements a function or functions.

2.5. "*Development phase*" means the period before a vehicle type is type approved.

2.6. "*Production phase*" refers to the duration of production of a vehicle type.

2.7. "*Post-production phase*" refers to the period in which a vehicle type is no longer produced until the end-of-life of all vehicles under the vehicle type. Vehicles incorporating a specific vehicle type will be operational during this phase but will no longer be produced. The phase ends when there are no longer any operational vehicles of a specific vehicle type.

2.8. "*Mitigation*" means a measure that is reducing risk.

2.9. "*Risk*" means the potential that a given threat will exploit vulnerabilities of a vehicle and thereby cause harm to the organization or to an individual.

2.10. "*Risk Assessment*" means the overall process of finding, recognizing and describing risks (risk identification), to comprehend the nature of risk and to

determine the level of risk (risk analysis), and of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable (risk evaluation).

2.11. "*Risk Management*" means coordinated activities to direct and control an organization with regard to risk.

2.12. "*Threat*" means a potential cause of an unwanted incident, which may result in harm to a system, organization or individual.

2.13. "*Vulnerability*" means a weakness of an asset or mitigation that can be exploited by one or more threats.

3. Application for approval

3.1. The application for approval of a vehicle type with regard to cyber security shall be submitted by the vehicle manufacturer or by their duly accredited representative.

3.2. It shall be accompanied by the undermentioned documents in triplicate, and by the following particulars:

3.2.1. A description of the vehicle type with regard to the items specified in Annex 1 to this Regulation.

3.2.2. In cases where information is shown to be covered by intellectual property rights or to constitute specific know-how of the manufacturer or of their suppliers, the manufacturer or their suppliers shall make available sufficient information to enable the checks referred to in this Regulation to be made properly. Such information shall be treated on a confidential basis.

3.2.3. The Certificate of Compliance for CSMS according to paragraph 6 of this Regulation.

3.3. Documentation shall be made available in two parts:

(a) The formal documentation package for the approval, containing the material specified in Annex 1 which shall be supplied to the Approval Authority or its Technical Service at the time of submission of the type approval application. This documentation package shall be used by the Approval Authority or its Technical Service as the basic reference for the approval process. The Approval Authority or its Technical Service shall ensure that this documentation package remains available for at least 10 years counted from the time when production of the vehicle type is definitively discontinued.

(b) Additional material relevant to the requirements of this regulation may be retained by the manufacturer, but made open for inspection at the time of type approval. The manufacturer shall ensure that any material made open for inspection at the time of type approval remains available for at least a period of 10 years counted from the time when production of the vehicle type is definitively discontinued.

4. Marking

4.1. There shall be affixed, conspicuously and in a readily accessible place specified on the approval form, to every vehicle conforming to a vehicle type approved under this Regulation an international approval mark consisting of:

4.1.1. A circle surrounding the Letter "E" followed by the distinguishing number of the country which has granted approval.

4.1.2. The number of this Regulation, followed by the letter "R", a dash and the approval number to the right of the circle described in paragraph 4.1.1. above.

4.2. If the vehicle conforms to a vehicle type approved under one or more other Regulations annexed to the Agreement in the country which has granted approval under this Regulation, the symbol prescribed in paragraph 4.1.1. above need not be repeated; in this case the Regulation and approval numbers and the additional symbols of all the Regulations under which approval has been granted in the country which has granted approval under this Regulation shall be placed in vertical columns to the right of the symbol prescribed in paragraph 4.1.1. above.

4.3. The approval mark shall be clearly legible and shall be indelible.

4.4. The approval mark shall be placed on or close to the vehicle data plate affixed by the Manufacturer.

4.5. Annex 3 to this Regulation gives examples of the arrangements of the approval mark.

5. Approval

5.1. Approval Authorities shall grant, as appropriate, type approval with regard to cyber security, only to such vehicle types that satisfy the requirements of this Regulation.

5.1.1. The Approval Authority or the Technical Service shall verify by means of document checks that the vehicle manufacturer has taken the necessary measures relevant for the vehicle type to:

(a) Collect and verify the information required under this Regulation through the supply chain so as to demonstrate that supplier-related risks are identified and are managed;

(b) Document risks assessment (conducted during development phase or retrospectively), test results and mitigations applied to the vehicle type, including design information supporting the risk assessment;

(c) Implement appropriate cyber security measures in the design of the vehicle type;

(d) Detect and respond to possible cyber security attacks;

(e) Log data to support the detection of cyber-attacks and provide data forensic capability to enable analysis of attempted or successful cyber-attacks.

5.1.2. The Approval Authority or the Technical Service shall verify by testing of a vehicle of the vehicle type that the vehicle manufacturer has implemented the cyber security measures they have documented. Tests shall be performed by the Approval Authority or the Technical Service itself or in collaboration with the vehicle manufacturer by sampling. Sampling shall be focused but not limited to risks that are assessed as high during the risk assessment.

5.1.3. The Approval Authority or Technical Service shall refuse to grant the type approval with regard to cyber security where the vehicle manufacturer has not fulfilled one or more of the requirements referred to in paragraph 7.3., notably:

(a) The vehicle manufacturer did not perform the exhaustive risk assessment referred to in paragraph 7.3.3.; including where the manufacturer did not consider all the risks related to threats referred to in Annex 5, Part A;

(b) The vehicle manufacturer did not protect the vehicle type against risks identified in the vehicle manufacturer's risk assessment or proportionate mitigations were not implemented as required by paragraph 7.;

(c) The vehicle manufacturer did not put in place appropriate and proportionate measures to secure dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data;

(d) The vehicle manufacturer did not perform, prior to the approval, appropriate and sufficient testing to verify the effectiveness of the security measures implemented.

5.1.4 The assessing Approval Authority shall also refuse to grant the type approval with regard to cyber security where the Approval Authority or Technical Service has not received sufficient information from the vehicle manufacturer to assess the cyber security of the vehicle type.

5.2. Notice of approval or of extension or refusal of approval of a vehicle type pursuant to this Regulation shall be communicated to the Parties to the 1958 Agreement which apply this Regulation, by means of a form conforming to the model in Annex 2 to this Regulation.

5.3. Approval Authorities shall not grant any type approval without verifying that the manufacturer has put in place satisfactory arrangements and procedures to manage properly the cyber security aspects as covered by this Regulation.

5.3.1.-5.3.7. (Reserved)

5.4. For the purpose of paragraph 7.2. of this Regulation, the manufacturer shall ensure that the cyber security aspects covered by this Regulation are implemented.

6. Certificate of Compliance for Cyber Security Management System

6.1. Contracting Parties shall appoint an Approval Authority to carry out the assessment of the manufacturer and to issue a Certificate of Compliance for CSMS.

6.2. An application for a Certificate of Compliance for Cyber Security Management System shall be submitted by the vehicle manufacturer or by their duly accredited representative.

6.3. It shall be accompanied by the undermentioned documents in triplicate, and by the following particular:

6.3.1. Documents describing the Cyber Security Management System.

6.3.2. A signed declaration using the model as defined in Appendix 1 to Annex 1.

6.4. In the context of the assessment, the manufacturer shall declare using the model as defined in Appendix 1 to Annex 1 and demonstrate to the satisfaction of the Approval Authority or its Technical Service that they have the necessary processes to comply with all the requirements for cyber security according to this Regulation.

6.5. When this assessment has been satisfactorily completed and in receipt of a signed declaration from the manufacturer according to the model as defined in Appendix 1 to Annex 1, a certificate named Certificate of Compliance for CSMS as described in Annex 4 to this Regulation (hereinafter the Certificate of Compliance for CSMS) shall be granted to the manufacturer.

6.6. The Approval Authority or its Technical Service shall use the model set out in Annex 4 to this Regulation for the Certificate of Compliance for CSMS.

6.7. The Certificate of Compliance for CSMS shall remain valid for a maximum of three years from the date of deliverance of the certificate unless it is withdrawn.

6.8. The Approval Authority which has granted the Certificate of Compliance for CSMS may at any time verify that the requirements for it continue to be met. The Approval Authority shall withdraw the Certificate of Compliance for CSMS if the requirements laid down in this Regulation are no longer met.

6.9. The manufacturer shall inform the Approval Authority or its Technical Service of any change that will affect the relevance of the Certificate of Compliance for CSMS. After consultation with the manufacturer, the Approval Authority or its Technical Service shall decide whether new checks are necessary.

6.10. At the end of the period of validity of the Certificate of Compliance for CSMS, the Approval Authority shall, after a positive assessment, issue a new Certificate of Compliance for CSMS or extend its validity for a further period of three years. The Approval Authority shall issue a new certificate in cases where changes have been brought to the attention of the Approval Authority or its Technical Service and the changes have been positively re-assessed.

6.11. The expiry or withdrawal of the manufacturer's Certificate of Compliance for CSMS shall be considered, with regard to the vehicle types to which the CSMS concerned was relevant, as modification of approval, as referred to in paragraph 8.

7. Specifications

7.1. General specifications

7.1.1. The requirements of this Regulation shall not restrict provisions or requirements of other UN Regulations.

7.2. Requirements for the Cyber Security Management System

7.2.1. For the assessment the Approval Authority or its Technical Service shall verify that the vehicle manufacturer has a Cyber Security Management System in place and shall verify its compliance with this Regulation.

7.2.2. The Cyber Security Management System shall cover the following aspects:

7.2.2.1. The vehicle manufacturer shall demonstrate to an Approval Authority or Technical Service that their Cyber Security Management System applies to the following phases:

(a) Development phase;

(b) Production phase;

(c) Post-production phase.

7.2.2.2. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System ensure security is adequately considered, including risks and mitigations listed in Annex 5. This shall include:

(a) The processes used within the manufacturer's organization to manage cyber security;

(b) The processes used for the identification of risks to vehicle types. Within these processes, the threats in Annex 5, Part A, and other relevant threats shall be considered;

(c) The processes used for the assessment, categorization and treatment of the risks identified;

(d) The processes in place to verify that the risks identified are appropriately managed;

(e) The processes used for testing the cyber security of a vehicle type;

(f) The processes used for ensuring that the risk assessment is kept current;

(g) The processes used to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified.

(h) The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks.

7.2.2.3. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that, based on categorization referred to in paragraph 7.2.2.2 (c) and 7.2.2.2 (g), cyber threats and vulnerabilities which require a response from the vehicle manufacturer shall be mitigated within a reasonable timeframe.

7.2.2.4. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that the monitoring referred to in paragraph 7.2.2.2 (g) shall be continual. This shall:

(a) Include vehicles after first registration in the monitoring;

(b) Include the capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs. This capability shall respect paragraph 1.3. and the privacy rights of car owners or drivers, particularly with respect to consent.

7.2.2.5. The vehicle manufacturer shall be required to demonstrate how their Cyber Security Management System will manage dependencies that may exist with contracted suppliers, service providers or manufacturer's sub-organizations in regards of the requirements of paragraph 7.2.2.2.

7.3. Requirements for vehicle types

7.3.1. The manufacturer shall have a valid Certificate of Compliance for the Cyber Security Management System relevant to the vehicle type being approved.

However, for type approvals prior to 1 July 2024, if the vehicle manufacturer can demonstrate that the vehicle type could not be developed in compliance with the CSMS, then the vehicle manufacturer shall demonstrate that cyber security was adequately considered during the development phase of the vehicle type concerned.

7.3.2. The vehicle manufacturer shall identify and manage, for the vehicle type being approved, supplier-related risks.

7.3.3. The vehicle manufacturer shall identify the critical elements of the vehicle type and perform an exhaustive risk assessment for the vehicle type and shall treat/manage the identified risks appropriately. The risk assessment shall consider the individual elements of the vehicle type and their interactions. The risk assessment shall further consider interactions with any external systems. While assessing the risks, the vehicle manufacturer shall consider the risks related to all the threats referred to in Annex 5, Part A, as well as any other relevant risk.

7.3.4. The vehicle manufacturer shall protect the vehicle type against risks identified in the vehicle manufacturer's risk assessment. Proportionate mitigations shall be implemented to protect the vehicle type. The mitigations implemented shall include all mitigations referred to in Annex 5, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex 5, Part B or C, is not relevant or not sufficient for the risk identified, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented.

In particular, for type approvals prior to 1 July 2024, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented if a mitigation

measure referred to in Annex 5, Part B or C is technically not feasible. The respective assessment of the technical feasibility shall be provided by the manufacturer to the approval authority.

7.3.5. The vehicle manufacturer shall put in place appropriate and proportionate measures to secure dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data.

7.3.6. The vehicle manufacturer shall perform, prior to type approval, appropriate and sufficient testing to verify the effectiveness of the security measures implemented.

7.3.7. The vehicle manufacturer shall implement measures for the vehicle type to:

(a) Detect and prevent cyber-attacks against vehicles of the vehicle type;

(b) Support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle type;

(c) Provide data forensic capability to enable analysis of attempted or successful cyber-attacks.

7.3.8. Cryptographic modules used for the purpose of this Regulation shall be in line with consensus standards. If the cryptographic modules used are not in line with consensus standards, then the vehicle manufacturer shall justify their use.

7.4. Reporting provisions

7.4.1. The vehicle manufacturer shall report at least once a year, or more frequently if relevant, to the Approval Authority or the Technical Service the outcome of their monitoring activities, as defined in paragraph 7.2.2.2.(g)), this shall include relevant information on new cyber-attacks. The vehicle manufacturer shall also report and confirm to the Approval Authority or the Technical Service that the cyber security mitigations implemented for their vehicle types are still effective and any additional actions taken.

7.4.2 The Approval Authority or the Technical Service shall verify the provided information and, if necessary, require the vehicle manufacturer to remedy any detected ineffectiveness.

If the reporting or response is not sufficient the Approval Authority may decide to withdraw the CSMS in compliance with paragraph 6.8.

8. Modification and extension of the vehicle type

8.1. Every modification of the vehicle type which affects its technical performance with respect to cybersecurity and/or documentation required in this Regulation shall be notified to the approval authority which approved the vehicle type. The Approval Authority may then either:

8.1.1. Consider that the modifications made still comply with the requirements and documentation of existing type approval; or

8.1.2. Require a further test report from the Technical Service responsible for conducting the tests.

8.1.3. Confirmation or extension or refusal of approval, specifying the alterations, shall be communicated by means of a communication form conforming to the model in Annex 2 to this Regulation. The Approval Authority issuing the extension of approval shall assign a series number for such an extension and inform there of the other Parties to the 1958 Agreement applying this Regulation by means of a communication form conforming to the model in Annex 2 to this Regulation.

9. Conformity of production

9.1. The Conformity of Production Procedures shall comply with those set out in the 1958 Agreement, Schedule 1 (E/ECE/TRANS/505/Rev.3) with the following requirements:

9.1.1. The holder of the approval shall ensure that results of the conformity of production tests are recorded and that the annexed documents remain available for a period determined in agreement with the Approval Authority or its Technical Service. This period shall not exceed 10 years counted from the time when production is definitively discontinued;

9.1.2. The Approval Authority which has granted type approval may at any time verify the conformity control methods applied in each production facility. The normal frequency of these verifications shall be once every three years.

10. Penalties for non-conformity of production

10.1. The approval granted in respect of a vehicle type pursuant to this Regulation may be withdrawn if the requirements laid down in this Regulation are not complied with or if sample vehicles fail to comply with the requirements of this Regulation.

10.2. If an Approval Authority withdraws an approval it has previously granted, it shall forthwith so notify the Contracting Parties applying this Regulation, by means of a communication form conforming to the model in Annex 2 to this Regulation.

11. Production definitively discontinued

11.1. If the holder of the approval completely ceases to manufacture a type of vehicle approved in accordance with this Regulation, he shall so inform the authority which granted the approval. Upon receiving the relevant communication that authority shall inform thereof the other Contracting Parties to the Agreement applying this Regulation by means of a copy of the approval form bearing at the end, in large letters, the signed and dated annotation "PRODUCTION DISCONTINUED".

12. Names and addresses of Technical Services responsible for conducting approval test, and of Type Approval Authorities

12.1. The Contracting Parties to the Agreement which apply this Regulation shall communicate to the United Nations Secretariat the names and addresses of the Technical Services responsible for conducting approval tests and of the Type Approval Authorities which grant approval and to which forms certifying approval or extension or refusal or withdrawal of approval, issued in other countries, are to be sent.

Annex 1

Information document

The following information, if applicable, shall be supplied in triplicate and include a list of contents. Any drawings shall be supplied in appropriate scale and in sufficient detail on size A4 or on a folder of A4 format. Photographs, if any, shall show sufficient detail.

1. Make (trade name of manufacturer): .....

2. Type and general commercial description(s): .....

3. Means of identification of type, if marked on the vehicle: .....

4. Location of that marking: .....

5. Category(ies) of vehicle: .....

6. Name and address of manufacturer/ manufacturer's representative: .....

7. Name(s) and Address(es) of assembly plant(s): .....

8. Photograph(s) and/or drawing(s) of a representative vehicle: .....

9. Cyber Security

9.1. General construction characteristics of the vehicle type, including:

(a) The vehicle systems which are relevant to the cyber security of the vehicle type;

(b) The components of those systems that are relevant to cyber security;

(c) The interactions of those systems with other systems within the vehicle type and external interfaces.

9.2. Schematic representation of the vehicle type

9.3. The number of the Certificate of Compliance for CSMS: .....

9.4. Documents for the vehicle type to be approved describing the outcome of its risk assessment and the identified risks: .....

9.5 Documents for the vehicle type to be approved describing the mitigations that have been implemented on the systems listed, or to the vehicle type, and how they address the stated risks: .....

9.6. Documents for the vehicle type to be approved describing protection of dedicated environments for aftermarket software, services, applications or data: .....

9.7. Documents for the vehicle type to be approved describing what tests have been used to verify the cyber security of the vehicle type and its systems and the outcome of those tests: .....

9.8. Description of the consideration of the supply chain with respect to cyber security: ...

Annex 1 - Appendix 1

Model of Manufacturer's Declaration of Compliance for CSMS

Manufacturer's declaration of compliance with the requirements for the Cyber Security Management System

Manufacturer Name: .....

Manufacturer Address: .....

……..(*Manufacturer Name*) attests that the necessary processes to comply with the requirements for the Cyber Security Management System laid down in paragraph 7.2 of UN Regulation [15X] are installed and will be maintained.

Done at: …… (*place*)

Date: .....

Name of the signatory: .....

Function of the signatory: .....

.....

(*Stamp and signature of the manufacturer's representative*)

Annex 2

Communication

(Maximum format: A4 (210 x 297 mm))

issued by: Name of administration:
.....
.....
.....

Concerning:[2] Approval granted
Approval extended
Approval withdrawn with effect from dd/mm/yyyy
Approval refused
Production definitively discontinued

of a vehicle type, pursuant to UN Regulation No. [15X]

Approval No.: .....

Extension No.: .....

Reason for extension: .....

1. Make (trade name of manufacturer): .....
2. Type and general commercial description(s) .....
3. Means of identification of type, if marked on the vehicle: .....
3.1. Location of that marking: .....
4. Category(ies) of vehicle: .....
5. Name and address of manufacturer / manufacturer's representative: .....
6. Name(s) and Address(es) of the production plant(s) .....
7. Number of the certificate of compliance for cyber security management system: .....
8. Technical Service responsible for carrying out the tests: .....
9. Date of test report: .....
10. Number of test report: .....
11. Remarks: (if any). .....
12. Place: .....
13. Date: .....
14. Signature: .....
15. The index to the information package lodged with the Approval Authority, which may be obtained on request is attached:

---

[1] Distinguishing number of the country which has granted/extended/refused/withdrawn approval (see approval provisions in the Regulation).

[2] Strike out what does not apply.

Annex 3

Arrangement of approval mark

Model A
(See paragraph 4.2 of this Regulation)

a = 8 mm min.

The above approval mark affixed to a vehicle shows that the road vehicle type concerned has been approved in the Netherlands (E 4), pursuant to Regulation No. [15X], and under the approval number 001234. The first two digits of the approval number indicate that the approval was granted in accordance with the requirements of this Regulation in its original form (00).

Annex 4

Model of Certificate of Compliance for CSMS

Certificate of compliance for cyber security management system

With UN Regulation No. [*This Regulation*]

Certificate Number [*Reference number*]

[……. *Approval Authority*]

Certifies that

Manufacturer: .....

Address of the manufacturer: .....

complies with the provisions of paragraph 7.2 of Regulation No. [15X]

Checks have been performed on:.....

by (name and address of the Approval Authority or Technical Service): .....

Number of report: .....

The certificate is valid until […..*Date*]

Done at [……*Place*]

On […….*Date*]

[……..*Signature*]

Attachments: description of the Cyber Security Management System by the manufacturer.

Annex 5

List of threats and corresponding mitigations

1. This annex consists of three parts. Part A of this annex describes the baseline for threats, vulnerabilities and attack methods. Part B of this annex describes mitigations to the threats which are intended for vehicle types. Part C describes mitigations to the threats which are intended for areas outside of vehicles, e.g. on IT backends.

2. Part A, Part B, and Part C shall be considered for risk assessment and mitigations to be implemented by vehicle manufacturers.

3. The high-level vulnerability and its corresponding examples have been indexed in Part A. The same indexing has been referenced in the tables in Parts B and C to link each of the attack/vulnerability with a list of corresponding mitigation measures.

4. The threat analysis shall also consider possible attack impacts. These may help ascertain the severity of a risk and identify additional risks. Possible attack impacts may include:

   (a) Safe operation of vehicle affected;

   (b) Vehicle functions stop working;

   (c) Software modified, performance altered;

   (d) Software altered but no operational effects;

   (e) Data integrity breach;

   (f) Data confidentiality breach;

   (g) Loss of data availability;

   (h) Other, including criminality.

Part A. Vulnerability or attack method related to the threats

1. High level descriptions of threats and relating vulnerability or attack method are listed in Table A1.

Table A1
List of vulnerability or attack method related to the threats

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
4.3.1 Threats regarding back-end servers related to vehicles in the field	1	Back-end servers used as a means to attack a vehicle or extract data	1.1	Abuse of privileges by staff (**insider attack**)
			1.2	**Unauthorized internet access** to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
			1.3	**Unauthorized physical access** to the server (conducted by for example USB sticks or other media connecting to the server)
	2	Services from back-end server being disrupted, affecting the operation of a vehicle	2.1	**Attack on back-end server stops it functioning**, for example it prevents it from interacting with vehicles and providing services they rely on
	3	Vehicle related data held on back-end servers being lost or compromised ("data breach")	3.1	Abuse of privileges by staff (**insider attack**)
			3.2	**Loss of information in the cloud**. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers
			3.3	**Unauthorized internet access to the server** (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
			3.4	**Unauthorized physical access to the server** (conducted for example by USB sticks or other media connecting to the server)
			3.5	**Information breach** by unintended sharing of data (e.g. admin errors)
4.3.2 Threats to vehicles regarding their communication channels	4	Spoofing of messages or data received by the vehicle	4.1	**Spoofing of messages** by impersonation (e.g. 802.11p V2X during platooning, GNSS messages, etc.)
			4.2	**Sybil attack** (in order to spoof other vehicles as if there are many vehicles on the road)
	5	Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data	5.1	Communications channels permit **code injection**, for example tampered software binary might be injected into the communication stream
			5.2	Communications channels permit **manipulate** of vehicle held data/code
			5.3	Communications channels permit **overwrite** of vehicle held data/code
			5.4	Communications channels permit **erasure** of vehicle held data/code
			5.5	Communications channels permit introduction of data/code to the vehicle (write data code)
	6	Communication channels permit untrusted/unreliable messages to be accepted or are	6.1	Accepting information from an **unreliable or untrusted source**
			6.2	**Man in the middle** attack/ session hijacking

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
		vulnerable to session hijacking/replay attacks	6.3	**Replay attack**, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway
	7	Information can be readily disclosed. For example, through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders	7.1	**Interception of information** / interfering radiations / monitoring communications
			7.2	Gaining **unauthorized access** to files or data
	8	Denial of service attacks via communication channels to disrupt vehicle functions	8.1	**Sending** a large number of garbage **data** to vehicle information system, **so that it is unable to provide services** in the normal manner
			8.2	**Black hole attack**, in order to disrupt communication between vehicles the attacker is able to block messages between the vehicles
	9	An unprivileged user is able to gain privileged access to vehicle systems	9.1	An unprivileged user is able to **gain privileged access**, for example root access
	10	Viruses embedded in communication media are able to infect vehicle systems	10.1	**Virus** embedded in communication media infects vehicle systems
	11	Messages received by the vehicle (for example X2V or diagnostic messages), or transmitted within it, contain malicious content	11.1	Malicious **internal** (e.g. CAN) **messages**
			11.2	Malicious **V2X messages,** e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM)
			11.3	Malicious diagnostic messages
			11.4	Malicious **proprietary messages** (e.g. those normally sent from OEM or component/system/function supplier)
4.3.3. Threats to vehicles regarding their update procedures	12	Misuse or compromise of update procedures	12.1	Compromise of **over the air software update procedures**. This includes fabricating the system update program or firmware
			12.2	Compromise of **local/physical software update procedures**. This includes fabricating the system update program or firmware
			12.3	The **software** is **manipulated before the update process** (and is therefore corrupted), although the update process is intact
			12.4	**Compromise** of cryptographic keys of the software provider **to allow invalid update**
	13	It is possible to deny legitimate updates	13.1	Denial of Service attack against update server or network to **prevent rollout of critical software updates** and/or unlock of customer specific features
4.3.4 Threats to vehicles regarding unintended human actions facilitating a cyber attack	15	Legitimate actors are able to take actions that would unwittingly facilitate a cyber-attack	15.1	Innocent victim (e.g. owner, operator or maintenance engineer) being **tricked into taking an action** to unintentionally load malware or enable an attack
			15.2	**Defined security procedures** are not followed

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
4.3.5 Threats to vehicles regarding their external connectivity and connections	16	Manipulation of the connectivity of vehicle functions enables a cyber-attack, this can include telematics; systems that permit remote operations; and systems using short range wireless communications	16.1	Manipulation of **functions designed to remotely operate systems**, such as remote key, immobilizer, and charging pile
			16.2	**Manipulation of vehicle telematics** (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)
			16.3	Interference with **short range wireless systems** or sensors
	17	Hosted 3rd party software, e.g. entertainment applications, used as a means to attack vehicle systems	17.1	**Corrupted applications**, or those with poor software security, used as a method to attack vehicle systems
	18	Devices connected to external interfaces e.g. USB ports, OBD port, used as a means to attack vehicle systems	18.1	**External interfaces** such as USB or other ports used as a point of attack, for example through code injection
			18.2	Media infected with a **virus** connected to a vehicle system
			18.3	**Diagnostic access (e.g. dongles in OBD port)** used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly)
4.3.6 Threats to vehicle data/code	19	Extraction of vehicle data/code	19.1	Extraction of copyright or proprietary software from vehicle systems (product **piracy**)
			19.2	Unauthorized access to the **owner's privacy information** such as personal identity, payment account information, address book information, location information, vehicle's electronic ID, etc.
			19.3	Extraction of cryptographic keys
	20	Manipulation of vehicle data/code	20.1	Illegal/unauthorized changes to **vehicle's electronic ID**
			20.2	**Identity fraud.** For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend
			20.3	Action to **circumvent monitoring systems** (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)
			20.4	Data manipulation to **falsify vehicle's driving data** (e.g. mileage, driving speed, driving directions, etc.)
			20.5	Unauthorized changes to **system diagnostic data**
	21	Erasure of data/code	21.1	Unauthorized deletion/manipulation of **system event logs**
	22	Introduction of malware	22.2	Introduce **malicious software** or malicious software activity
	23	Introduction of new software or overwrite existing software	23.1	**Fabrication of software** of the vehicle control system or information system

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
	24	Disruption of systems or operations	24.1	**Denial of service**, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging
	25	Manipulation of vehicle parameters	25.1	Unauthorized access of **falsify the configuration parameters** of vehicle's key functions, such as brake data, airbag deployed threshold, etc.
			25.2	Unauthorized access of **falsify the charging parameters**, such as charging voltage, charging power, battery temperature, etc.
4.3.7 Potential vulnerabilities that could be exploited if not sufficiently protected or hardened	26	Cryptographic technologies can be compromised or are insufficiently applied	26.1	Combination of short **encryption keys** and long period of validity enables attacker to break encryption
			26.2	Insufficient use of cryptographic algorithms to protect sensitive systems
			26.3	Using already or soon to be deprecated **cryptographic algorithms**
	27	Parts or supplies could be compromised to permit vehicles to be attacked	27.1	**Hardware or software, engineered to enable an attack** or fails to meet design criteria to stop an attack
	28	Software or hardware development permits vulnerabilities	28.1	**Software bugs**. The presence of software bugs can be a basis for potential exploitable vulnerabilities. This is particularly true if software has not been tested to verify that known bad code/bugs is not present and reduce the risk of unknown bad code/bugs being present
			28.2	**Using remainders** from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, …) can permit access to ECUs or permit attackers to gain higher privileges
	29	Network design introduces vulnerabilities	29.1	**Superfluous internet ports left open**, providing access to network systems
			29.2	Circumvent **network separation** to gain control. Specific example is the use of unprotected gateways, or access points (such as truck-trailer gateways), to circumvent protections and gain access to other network segments to perform malicious acts, such as sending arbitrary CAN bus messages
	31	Unintended transfer of data can occur	31.1	Information breach. Personal data may be leaked when the **car changes user** (e.g. is sold or is used as hire vehicle with new hirers)
	32	Physical manipulation of systems can enable an attack	32.1	**Manipulation of electronic hardware**, e.g. unauthorized electronic hardware added to a vehicle to enable "man-in-the-middle" attack **Replacement of authorized electronic hardware** (e.g., sensors) with unauthorized electronic hardware **Manipulation of the information** collected by a sensor (for example, using a magnet to tamper with the Hall effect sensor connected to the gearbox)

Part B. Mitigations to the threats intended for vehicles

1. Mitigations for "Vehicle communication channels"

Mitigations to the threats which are related to "Vehicle communication channels" are listed in Table B1.

Table B1
Mitigation to the threats which are related to "Vehicle communication channels"

Table A1 reference	*Threats to "Vehicle communication channels"*	*Ref*	*Mitigation*
4.1	Spoofing of messages (e.g. 802.11p V2X during platooning, GNSS messages, etc.) by impersonation	M10	The vehicle shall verify the authenticity and integrity of messages it receives
4.2	Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)	M11	Security controls shall be implemented for storing cryptographic keys (e.g., use of Hardware Security Modules)
5.1	Communication channels permit code injection into vehicle held data/code, for example tampered software binary might be injected into the communication stream	M10 M6	The vehicle shall verify the authenticity and integrity of messages it receives Systems shall implement security by design to minimize risks
5.2	Communication channels permit manipulation of vehicle held data/code	M7	Access control techniques and designs shall be applied to protect system data/code
5.3	Communication channels permit overwrite of vehicle held data/code		
5.4 21.1	Communication channels permit erasure of vehicle held data/code		
5.5	Communication channels permit introduction of data/code to vehicle systems (write data code)		
6.1	Accepting information from an unreliable or untrusted source	M10	The vehicle shall verify the authenticity and integrity of messages it receives
6.2	Man in the middle attack / session hijacking	M10	The vehicle shall verify the authenticity and integrity of messages it receives
6.3	Replay attack, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway		
7.1	Interception of information / interfering radiations / monitoring communications	M12	Confidential data transmitted to or from the vehicle shall be protected
7.2	Gaining unauthorized access to files or data	M8	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Example of Security Controls can be found in OWASP
8.1	Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner	M13	Measures to detect and recover from a denial of service attack shall be employed

Table A1 reference	*Threats to "Vehicle communication channels"*	*Ref*	*Mitigation*
8.2	Black hole attack, disruption of communication between vehicles by blocking the transfer of messages to other vehicles	M13	Measures to detect and recover from a denial of service attack shall be employed
9.1	An unprivileged user is able to gain privileged access, for example root access	M9	Measures to prevent and detect unauthorized access shall be employed
10.1	Virus embedded in communication media infects vehicle systems	M14	Measures to protect systems against embedded viruses/malware should be considered
11.1	Malicious internal (e.g. CAN) messages	M15	Measures to detect malicious internal messages or activity should be considered
11.2	Malicious V2X messages, e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM)	M10	The vehicle shall verify the authenticity and integrity of messages it receives
11.3	Malicious diagnostic messages		
11.4	Malicious proprietary messages (e.g. those normally sent from OEM or component/system/function supplier)		

2. Mitigations for "Update process"

Mitigations to the threats which are related to "Update process" are listed in Table B2.

Table B2
Mitigations to the threats which are related to "Update process"

Table A1 reference	*Threats to "Update process"*	*Ref*	*Mitigation*
12.1	Compromise of over the air software update procedures. This includes fabricating the system update program or firmware	M16	Secure software update procedures shall be employed
12.2	Compromise of local/physical software update procedures. This includes fabricating the system update program or firmware		
12.3	The software is manipulated before the update process (and is therefore corrupted), although the update process is intact		
12.4	Compromise of cryptographic keys of the software provider to allow invalid update	M11	Security controls shall be implemented for storing cryptographic keys
13.1	Denial of Service attack against update server or network to prevent rollout of critical software updates and/or unlock of customer specific features	M3	Security Controls shall be applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP

3. Mitigations for "Unintended human actions facilitating a cyber attack"

Mitigations to the threats which are related to "Unintended human actions facilitating a cyber attack" are listed in Table B3.

Table B3
Mitigations to the threats which are related to "Unintended human actions facilitating a cyber attack"

Table A1 reference	*Threats relating to "Unintended human actions"*	*Ref*	*Mitigation*
15.1	Innocent victim (e.g. owner, operator or maintenance engineer) is tricked into taking an action to unintentionally load malware or enable an attack	M18	Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege
15.2	Defined security procedures are not followed	M19	Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions

4. Mitigations for "External connectivity and connections"

Mitigations to the threats which are related to "external connectivity and connections" are listed in Table B4.

Table B4
Mitigation to the threats which are related to "external connectivity and connections"

Table A1 reference	*Threats to "External connectivity and connections"*	*Ref*	*Mitigation*
16.1	Manipulation of functions designed to remotely operate vehicle systems, such as remote key, immobiliser, and charging pile	M20	Security controls shall be applied to systems that have remote access
16.2	Manipulation of vehicle telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)		
16.3	Interference with short range wireless systems or sensors		
17.1	Corrupted applications, or those with poor software security, used as a method to attack vehicle systems	M21	Software shall be security assessed, authenticated and integrity protected. Security controls shall be applied to minimise the risk from third party software that is intended or foreseeable to be hosted on the vehicle
18.1	External interfaces such as USB or other ports used as a point of attack, for example through code injection	M22	Security controls shall be applied to external interfaces
18.2	Media infected with viruses connected to the vehicle		
18.3	Diagnostic access (e.g. dongles in OBD port) used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly)	M22	Security controls shall be applied to external interfaces

5. Mitigations for "Potential targets of, or motivations for, an attack "

Mitigations to the threats which are related to "Potential targets of, or motivations for, an attack " are listed in Table B5.

Table B5
Mitigations to the threats which are related to "Potential targets of, or motivations for, an attack"

Table A1 reference	*Threats to "Potential targets of, or motivations for, an attack"*	*Ref*	*Mitigation*
19.1	Extraction of copyright or proprietary software from vehicle systems (product piracy / stolen software)	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP
19.2	Unauthorized access to the owner's privacy information such as personal identity, payment account information, address book information, location information, vehicle's electronic ID, etc.	M8	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Examples of Security Controls can be found in OWASP
19.3	Extraction of cryptographic keys	M11	Security controls shall be implemented for storing cryptographic keys e.g. Security Modules
20.1	Illegal/unauthorised changes to vehicle's electronic ID	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP
20.2	Identity fraud. For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend		
20.3	Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP. Data manipulation attacks on sensors or transmitted data could be mitigated by correlating the data from different sources of information
20.4	Data manipulation to falsify vehicle's driving data (e.g. mileage, driving speed, driving directions, etc.)		
20.5	Unauthorised changes to system diagnostic data		
21.1	Unauthorized deletion/manipulation of system event logs	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP.
22.2	Introduce malicious software or malicious software activity	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP.
23.1	Fabrication of software of the vehicle control system or information system		
24.1	Denial of service, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging	M13	Measures to detect and recover from a denial of service attack shall be employed
25.1	Unauthorized access to falsify configuration parameters of vehicle's key functions, such as brake data, airbag deployed threshold, etc.	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP
25.2	Unauthorized access to falsify charging parameters, such as charging voltage, charging power, battery temperature, etc.		

6. Mitigations for "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"

Mitigations to the threats which are related to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened" are listed in Table B6.

Table B6
Mitigations to the threats which are related to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"

Table A1 reference	*Threats to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"*	*Ref*	*Mitigation*
26.1	Combination of short encryption keys and long period of validity enables attacker to break encryption	M23	Cybersecurity best practices for software and hardware development shall be followed
26.2	Insufficient use of cryptographic algorithms to protect sensitive systems		
26.3	Using deprecated cryptographic algorithms		
27.1	Hardware or software, engineered to enable an attack or fail to meet design criteria to stop an attack	M23	Cybersecurity best practices for software and hardware development shall be followed
28.1	The presence of software bugs can be a basis for potential exploitable vulnerabilities. This is particularly true if software has not been tested to verify that known bad code/bugs is not present and reduce the risk of unknown bad code/bugs being present	M23	Cybersecurity best practices for software and hardware development shall be followed. Cybersecurity testing with adequate coverage
28.2	Using remainders from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, …) can permit an attacker to access ECUs or gain higher privileges		
29.1	Superfluous internet ports left open, providing access to network systems		
29.2	Circumvent network separation to gain control. Specific example is the use of unprotected gateways, or access points (such as truck-trailer gateways), to circumvent protections and gain access to other network segments to perform malicious acts, such as sending arbitrary CAN bus messages	M23	Cybersecurity best practices for software and hardware development shall be followed. Cybersecurity best practices for system design and system integration shall be followed

7. Mitigations for "Data loss / data breach from vehicle"

Mitigations to the threats which are related to "Data loss / data breach from vehicle" are listed in Table B7.

Table B7
Mitigations to the threats which are related to "Data loss / data breach from vehicle"

Table A1 reference	*Threats of "Data loss / data breach from vehicle"*	*Ref*	*Mitigation*
31.1	Information breach. Personal data may be breached when the car changes user (e.g. is sold or is used as hire vehicle with new hirers)	M24	Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data.

8. Mitigations for "Physical manipulation of systems to enable an attack"

Mitigation to the threats which are related to "Physical manipulation of systems to enable an attack" are listed in Table B8.

Table B8
Mitigations to the threats which are related to "Physical manipulation of systems to enable an attack"

Table A1 reference	*Threats to "Physical manipulation of systems to enable an attack"*	*Ref*	*Mitigation*
32.1	Manipulation of OEM hardware, e.g. unauthorised hardware added to a vehicle to enable "man-in-the-middle" attack	M9	Measures to prevent and detect unauthorized access shall be employed

Part C. Mitigations to the threats outside of vehicles

1. Mitigations for "Back-end servers"

Mitigations to the threats which are related to "Back-end servers" are listed in Table C1.

Table C1
Mitigations to the threats which are related to "Back-end servers"

Table A1 reference	*Threats to "Back-end servers"*	*Ref*	*Mitigation*
1.1 & 3.1	Abuse of privileges by staff (insider attack)	M1	Security Controls are applied to back-end systems to minimise the risk of insider attack
1.2 & 3.3	Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)	M2	Security Controls are applied to back-end systems to minimise unauthorised access. Example Security Controls can be found in OWASP
1.3 & 3.4	Unauthorised physical access to the server (conducted by for example USB sticks or other media connecting to the server)	M8	Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data
2.1	Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on	M3	Security Controls are applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP
3.2	Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers	M4	Security Controls are applied to minimise risks associated with cloud computing. Example Security Controls can be found in OWASP and NCSC cloud computing guidance
3.5	Information breach by unintended sharing of data (e.g. admin errors, storing data in servers in garages)	M5	Security Controls are applied to back-end systems to prevent data breaches. Example Security Controls can be found in OWASP

2. Mitigations for "Unintended human actions"
Mitigations to the threats which are related to "Unintended human actions" are listed in Table C2.

Table C2
Mitigations to the threats which are related to "Unintended human actions"

Table A1 reference	*Threats relating to "Unintended human actions"*	*Ref*	*Mitigation*
15.1	Innocent victim (e.g. owner, operator or maintenance engineer) is tricked into taking an action to unintentionally load malware or enable an attack	M18	Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege
15.2	Defined security procedures are not followed	M19	Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions

3. Mitigations for "Physical loss of data"
Mitigations to the threats which are related to "Physical loss of data" are listed in Table C3.

Table C3
Mitigations to the threats which are related to "Physical loss of data loss"

Table A1 reference	*Threats of "Physical loss of data"*	*Ref*	*Mitigation*
30.1	Damage caused by a third party. Sensitive data may be lost or compromised due to physical damages in cases of traffic accident or theft	M24	Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data. Example Security Controls can be found in ISO/SC27/WG5
30.2	Loss from DRM (digital right management) conflicts. User data may be deleted due to DRM issues		
30.3	The (integrity of) sensitive data may be lost due to IT components wear and tear, causing potential cascading issues (in case of key alteration, for example)		

[FRENCH TEXT – TEXTE FRANÇAIS]

Proposition de nouveau Règlement ONU énonçant des prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne la cybersécurité et le système de gestion de la cybersécurité

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

Le texte ci-après, qui constitue une proposition de nouveau Règlement ONU énonçant des prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne la cybersécurité et le système de gestion de la cybersécurité, a été établi par le groupe de travail informel de la cybersécurité et des questions de sûreté des transmissions sans fil et revu par le Groupe de travail des véhicules automatisés/autonomes et connectés (GRVA). Ce texte a été élaboré conformément au Document-cadre sur les véhicules automatisés/autonomes (ECE/TRANS/WP.29/2019/34), tel que révisé. Il a été adopté par le GRVA à sa cinquième session (voir ECE/TRANS/WP.29/GRVA/6, par. 23), sur la base du document ECE/TRANS/WP.29/GRVA/2020/3 tel que modifié par le document informel GRVA-06-19-Rev.1. Il est soumis au Forum mondial de l'harmonisation des Règlements concernant les véhicules (WP.29) et au Comité d'administration de l'Accord de 1958 (AC.1) pour examen et vote à leurs sessions de juin 2020.

Faute de temps, le GRVA n'a pas été en mesure de parachever la formulation du paragraphe 5.3. Les Parties contractantes qui avaient exprimé leurs vues à ce sujet ont offert de poursuivre les échanges à l'issue de la session et de trouver une solution pour le

* Conformément au programme de travail du Comité des transports intérieurs pour 2020 tel qu'il figure dans le projet de budget-programme pour 2020 (A/74/6 (titre V, chap. 20), par. 20.37), 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.

paragraphe 5.3 et ses sous-paragraphes. Leurs propositions, qui viennent compléter le présent document, sont publiées sous la cote ECE/TRANS/WP.29/2020/97.

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

Table des matières

** Les numéros de page seront ajoutés ultérieurement.

1. Champ d'application

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

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

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

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

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

2. Définitions

Aux fins du présent Règlement, on entend par :

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

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

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

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

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

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

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

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

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

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

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

2.10 « *Appréciation des risques* », le processus englobant la recherche, la reconnaissance et la description des risques (définition des risques), en vue d'en comprendre la nature et d'en déterminer le niveau (analyse des risques), et la comparaison des résultats de l'analyse des risques aux critères de risque afin de déterminer si les risques et/ou leur importance sont acceptables ou tolérables (évaluation des risques).

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

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

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

3. Demande d'homologation

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

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

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

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

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

3.3 La documentation doit être fournie en deux parties :

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

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

4. Marquage

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

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

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

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

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

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

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

5. Homologation

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

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

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

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

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

d) Détecter les menaces de cyberattaque et y réagir ;

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

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

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

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

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

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

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

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

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

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

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

5.3.1-5.3.7 (Réservés)

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

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

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

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

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

6.3.1 Une description du système de gestion de la cybersécurité ;

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

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

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

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

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

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

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

6.10 À la fin de la période de validité du certificat de conformité du CSMS, l'autorité d'homologation doit, après une évaluation positive, délivrer un nouveau certificat de conformité du CSMS ou prolonger la validité du certificat périmé pour une nouvelle période de trois ans. L'autorité d'homologation doit délivrer un nouveau certificat lorsque des modifications ont été portées à son attention ou à celle de son service technique et que ces modifications ont fait l'objet d'une réévaluation positive.

6.11 L'expiration ou le retrait du certificat de conformité du CSMS accordé au constructeur est à considérer, en ce qui concerne les types de véhicules auxquels le CSMS s'appliquait, comme une modification de l'homologation telle que visée au paragraphe 8.

7. Spécifications

7.1 Spécifications générales

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

7.2 Prescriptions relatives au système de gestion de la cybersécurité

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

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

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

a) Phase de développement ;

b) Phase de production ;

c) Phase de postproduction.

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

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

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

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

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

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

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

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

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

7.2.2.3 Le constructeur du véhicule doit démontrer que les processus mis en œuvre dans le cadre de son système de gestion de la cybersécurité garantissent que, sur la base des catégories mentionnées aux alinéas c) et g) du paragraphe 7.2.2.2, les cybermenaces et les vulnérabilités auxquelles il doit réagir sont atténuées dans un délai raisonnable.

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

a) Commencer dès la première immatriculation du véhicule ;

b) Permettre d'analyser et de détecter les cybermenaces, les vulnérabilités et les cyberattaques à partir des données et des journaux du véhicule. Cette capacité doit s'exercer conformément au paragraphe 1.3 et dans le respect des droits des propriétaires ou des conducteurs des véhicules en matière de vie privée, en particulier s'agissant du consentement.

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

7.3 Prescriptions relatives aux types de véhicules

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

Toutefois, pour les homologations de type antérieures au 1er juillet 2024, si le constructeur peut donner la preuve que le type de véhicule n'a pas pu être développé conformément au système de gestion de la cybersécurité, il doit démontrer que la cybersécurité a été dûment prise en compte pendant la phase de développement du type de véhicule en question.

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

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

7.3.4 Le constructeur doit protéger le type de véhicule contre les risques répertoriés dans le cadre de son appréciation des risques et, à cette fin, prendre des mesures d'atténuation proportionnées . Celles-ci doivent comprendre toutes les mesures mentionnées dans les parties B et C de l'annexe 5 qui sont pertinentes au regard des risques répertoriés. Toutefois, si une mesure d'atténuation mentionnée dans la partie B ou C de l'annexe 5 n'est pas pertinente ou suffisante au regard du risque répertorié, le constructeur du véhicule doit s'assurer qu'une mesure de remplacement appropriée est mise en œuvre.

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

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

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

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

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

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

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

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

7.4 Dispositions relatives à la communication de l'information

7.4.1 Le constructeur du véhicule doit rendre compte, au moins une fois par an et, si nécessaire, plus fréquemment, à l'autorité d'homologation ou à son service technique des résultats de ses activités de surveillance, telles que définies à

l'alinéa g) du paragraphe 7.2.2.2, notamment en communiquant des informations relatives aux nouvelles cyberattaques. Le constructeur doit également confirmer à l'autorité d'homologation ou à son service technique que les mesures d'atténuation des cyberattaques mises en œuvre pour les types de véhicules concernés demeurent efficaces, et l'informer des mesures supplémentaires éventuellement prises.

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

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

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

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

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

8.1.2 Soit exiger un nouveau procès-verbal du service technique chargé des essais.

8.1.3 La confirmation, l'extension ou le refus de l'homologation, faisant mention des modifications apportées, doit être notifié au moyen d'une fiche de communication conforme au modèle de l'annexe 2 du présent Règlement. L'autorité d'homologation qui délivre une extension d'homologation doit attribuer un numéro de série à ladite extension et en informer les autres Parties à l'Accord de 1958 appliquant le présent Règlement au moyen d'une fiche de communication conforme au modèle de l'annexe 2 dudit Règlement.

9. Conformité de la production

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

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

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

10. Sanctions pour non-conformité de la production

10.1 L'homologation délivrée pour un type de véhicule en application du présent Règlement peut être retirée si les prescriptions énoncées dans ledit Règlement

ne sont pas respectées ou si les véhicules prélevés ne satisfont pas auxdites prescriptions.

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

11. Arrêt définitif de la production

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

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

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

Annexe 1

Fiche de renseignements

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

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

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

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

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

5. Catégorie(s) du véhicule : .....

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

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

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

9. Cybersécurité

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

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

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

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

9.2 Représentation schématique du type de véhicule

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

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

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

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

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

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

Annexe 1 − Appendice 1

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

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

Nom du constructeur : .....

Adresse du constructeur : .....

..... (*nom du constructeur*) atteste que les processus nécessaires pour satisfaire aux prescriptions relatives au système de gestion de la cybersécurité énoncées au paragraphe 7.2 du Règlement ONU nº [15X] sont en place et qu'ils seront maintenus.

Fait à : …… (*lieu*)

Le : .....

Nom du signataire : .....

Fonction du signataire : .....

.....

(*Cachet et signature du représentant du constructeur*)

Annexe 2

Fiche de communication

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

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

concernant[2] : Délivrance d'une homologation
Extension d'homologation
Retrait d'homologation avec effet au jj/mm/aaaa
Refus d'homologation
Arrêt définitif de la production

d'un type de véhicule, conformément au Règlement ONU n° [15X].

N° d'homologation : .....

N° d'extension : .....

Motif de l'extension : .....

1. Marque (raison sociale du constructeur) : .....
2. Type et dénomination(s) commerciale(s) générale(s) : .....
3. Moyen d'identification du type, s'il est indiqué sur le véhicule : .....
- 3.1 Emplacement de cette marque : .....
4. Catégorie(s) du véhicule : .....
5. Nom et adresse du constructeur ou de son représentant : .....
6. Nom(s) et adresse(s) de l'atelier (des ateliers) de montage : .....
7. Numéro du certificat de conformité du système de gestion de la cybersécurité : .....
8. Service technique chargé des essais : .....
9. Date du procès-verbal d'essai : .....
10. Numéro du procès-verbal d'essai : .....
11. Remarques (le cas échéant) : .....
12. Lieu : .....
13. Date : .....
14. Signature : .....
15. On trouvera en annexe la liste des documents du dossier d'homologation déposé auprès de l'autorité d'homologation, qui peut être obtenu sur demande.

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

[2] Biffer la mention inutile.

Annexe 3

Exemple de marque d'homologation

Modèle A
(Voir le paragraphe 4.2 du présent Règlement)

a = 8 mm min.

La marque d'homologation ci-dessus, apposée sur un véhicule, indique que le type de ce véhicule a été homologué aux Pays-Bas (E 4), en application du Règlement nº [15X], sous le numéro d'homologation 001234. Les deux premiers chiffres du numéro d'homologation (00) signifient que l'homologation a été délivrée conformément aux prescriptions dudit Règlement sous sa forme originale.

Annexe 4

Modèle de certificat de conformité du CSMS

Certificat de conformité du système de gestion de la cybersécurité

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

Numéro de certificat [*numéro de référence*]

[……. *autorité d'homologation*]

Certifie que

Nom du constructeur : .....

Adresse du constructeur : .....

est en conformité avec les dispositions du paragraphe 7.2 du Règlement nº [15X].

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

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

Numéro du procès-verbal : .....

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

Fait à : [……*lieu*]

Le : […….*date*]

[…….*signature*]

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

Annexe 5

Liste des menaces et des mesures d'atténuation correspondantes

1. La présente annexe se compose de trois parties. La partie A décrit l'état de référence des menaces, vulnérabilités et méthodes d'attaque. La partie B décrit les mesures d'atténuation des menaces visant les types de véhicule. La partie C décrit les mesures d'atténuation des menaces visant les zones situées en dehors des véhicules, par exemple les systèmes dorsaux.

2. Les parties A, B et C doivent être prises en compte dans le cadre de l'appréciation des risques et des mesures d'atténuation que les constructeurs de véhicules doivent mettre en œuvre.

3. La vulnérabilité de haut niveau et les exemples correspondants ont été indexés dans la partie A. La même indexation a été référencée dans les tableaux des parties B et C pour établir un lien entre chaque attaque ou vulnérabilité et les mesures d'atténuation correspondantes.

4. L'analyse des menaces doit également inclure un examen des éventuelles conséquences d'une attaque. Cet examen peut contribuer à déterminer le degré de risque et à déceler d'autres risques. Une attaque peut :

   a) Compromettre la sécurité d'utilisation du véhicule ;

   b) Interrompre certaines fonctions du véhicule ;

   c) Modifier des logiciels et altérer les performances ;

   d) Modifier des logiciels sans avoir d'effet sur le fonctionnement ;

   e) Compromettre l'intégrité des données ;

   f) Compromettre la confidentialité des données ;

   g) Interdire l'accès aux données ;

   h) Avoir d'autres conséquences, par exemple d'ordre criminel.

Partie A
Vulnérabilités ou méthodes d'attaque liées aux menaces

1. Des descriptions de haut niveau des menaces et des vulnérabilités ou des méthodes d'attaque correspondantes sont présentées dans le tableau A1.

Tableau A1
Liste de vulnérabilités ou de méthodes d'attaque liées aux menaces

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			*Exemple de vulnérabilité ou de méthode d'attaque*	
4.3.1 Menaces concernant les serveurs dorsaux liés aux véhicules en circulation	1	Serveurs dorsaux utilisés pour attaquer un véhicule ou extraire des données	1.1	Abus de privilèges de la part du personnel (**attaque d'initié**)
			1.2	**Accès Internet non autorisé** au serveur (activé par exemple par des portes dérobées, des vulnérabilités logicielles système non corrigées, des attaques SQL ou d'autres moyens)
			1.3	**Accès physique non autorisé** au serveur (au moyen, par exemple, de clefs USB ou d'autres supports connectés au serveur)

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			*Exemple de vulnérabilité ou de méthode d'attaque*	
	2	Services d'un serveur dorsal perturbés, entravant le fonctionnement d'un véhicule	2.1	**Attaque d'un serveur dorsal bloquant son fonctionnement**, par exemple en l'empêchant d'interagir avec les véhicules et de fournir les services dont ils ont besoin
	3	Données liées aux véhicules stockées sur des serveurs dorsaux perdues ou compromises (« violation des données »)	3.1	Abus de privilèges de la part du personnel (**attaque d'initié**)
			3.2	**Perte d'informations dans le « nuage »**. Des données sensibles peuvent être perdues en raison d'attaques ou d'accidents lorsque les données sont stockées par des fournisseurs de services en nuage tiers
			3.3	**Accès Internet non autorisé** au serveur (activé par exemple par des portes dérobées, des vulnérabilités logicielles système non corrigées, des attaques SQL ou d'autres moyens)
			3.4	**Accès physique non autorisé** au serveur (au moyen, par exemple, de clef USB ou d'autres supports connectés au serveur)
			3.5	**Atteinte à la sécurité de l'information** due au partage involontaire de données (par exemple, erreurs administratives)
4.3.2 Menaces pour les véhicules liées à leurs voies de communication	4	Simulation de messages ou de données reçus par le véhicule	4.1	**Simulation de messages** par usurpation d'identité (802.11p V2X en cas de circulation en peloton, messages GNSS, etc.)
			4.2	**Attaque Sybil** (visant à simuler d'autres véhicules pour faire croire qu'il y en a beaucoup sur la route)
	5	Voies de communication utilisées pour effectuer des manipulations, suppressions ou autres modifications non autorisées du code ou des données du véhicule	5.1	Les voies de communication permettent l'**injection de code**, par exemple un code binaire altéré peut être injecté dans le flux de communication
			5.2	Les voies de communication permettent de **manipuler** les données ou le code du véhicule
			5.3	Les voies de communication permettent d'**écraser** les données ou le code du véhicule
			5.4	Les voies de communication permettent d'**effacer** les données ou le code du véhicule
			5.5	Les voies de communication permettent l'introduction de données ou de code dans le véhicule (écriture de données ou de code)
	6	Voies de communication permettant l'acceptation de messages non fiables, ou vulnérables au détournement de session ou aux attaques par	6.1	Acceptation d'informations provenant d'une **source non fiable**
			6.2	**Attaque de l'homme du milieu**/détournement de session

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			*Exemple de vulnérabilité ou de méthode d'attaque*	
		rejeu	6.3	**Attaque par rejeu**, par exemple une attaque contre une passerelle de communication permettant à l'attaquant d'installer une version antérieure du logiciel d'un module de gestion électronique ou du microprogramme de la passerelle
	7	Les informations peuvent être facilement divulguées. Par exemple, les communications peuvent être interceptées ou l'accès non autorisé à des fichiers ou dossiers sensibles peut être rendu possible	7.1	**Interception de l'information**/rayonnements brouilleurs/surveillance des communications
			7.2	Obtention d'un **accès non autorisé** à des fichiers ou à des données
	8	Attaques par déni de service sur les voies de communication pour perturber les fonctions du véhicule	8.1	**Envoi** d'un grand nombre de **données** parasites au système d'information du véhicule, **de sorte qu'il soit incapable de fournir des services** de manière normale
			8.2	**Attaque par trou noir**, visant à perturber la communication entre les véhicules en bloquant les messages entre ceux-ci
	9	Un utilisateur sans privilèges peut obtenir un accès privilégié aux systèmes du véhicule	9.1	Un utilisateur sans privilèges peut **obtenir un accès privilégié**, par exemple un accès racine
	10	Des virus introduits dans les moyens de communication peuvent infecter les systèmes du véhicule	10.1	Un **virus** introduit dans les moyens de communication infecte les systèmes du véhicule
	11	Des messages reçus par le véhicule (par exemple, messages X2V ou de diagnostic), ou transmis à l'intérieur de celui-ci, renferment des contenus malveillants	11.1	**Messages internes** malveillants (par exemple, bus CAN)
			11.2	**Messages V2X** malveillants, par exemple, messages d'infrastructure à véhicule ou de véhicule à véhicule (CAM, DENM, etc.)
			11.3	Messages de diagnostic malveillants
			11.4	**Messages propriétaires** malveillants (par exemple, ceux normalement envoyés par les équipementiers ou les fournisseurs de composants/systèmes/fonctions)
4.3.3. Menaces pour les véhicules liées à leurs procédures de mise à jour	12	Utilisation abusive ou compromission des procédures de mise à jour	12.1	Compromission des **procédures de mise à jour logicielle sans fil**, y compris la fabrication du programme ou du microprogramme de mise à jour du système
			12.2	Compromission des **procédures de mise à jour logicielle locales/physiques**, y compris la fabrication du programme ou du microprogramme de mise à jour du système

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			*Exemple de vulnérabilité ou de méthode d'attaque*	
			12.3	Le **logiciel** est **manipulé avant le processus de mise à jour** (il est donc corrompu), bien que le processus de mise à jour soit intact
			12.4	**Compromission** des clefs cryptographiques du fournisseur du logiciel **visant à permettre une mise à jour non valide**
	13	Possibilité d'empêcher des mises à jour légitimes	13.1	Attaque par déni de service contre le serveur ou le réseau de mise à jour pour **empêcher le déploiement de mises à jour logicielles critiques** et/ou le déverrouillage de fonctionnalités spécifiques au client
4.3.4 Menaces pour les véhicules liées à des actions humaines non intentionnelles qui facilitent les cyberattaques	15	Des acteurs légitimes peuvent prendre des mesures sans avoir conscience que celles-ci sont susceptibles de faciliter une cyberattaque	15.1	Victime innocente (par exemple, propriétaire, opérateur ou ingénieur de maintenance) **amenée par la ruse** et à son insu à charger un logiciel malveillant ou à permettre une attaque
			15.2	Les **procédures de sécurité définies** ne sont pas suivies
4.3.5 Menaces pour les véhicules liées à leur connectivité et à leurs connexions externes	16	La manipulation de la connectivité des fonctions du véhicule permet une cyberattaque, les moyens utilisés comprenant : la télématique, les systèmes permettant des opérations à distance et les systèmes utilisant des communications sans fil à courte portée	16.1	Manipulation des **fonctions conçues pour commander à distance des systèmes**, tels qu'une clef à distance, un dispositif d'immobilisation et une pile de chargement
			16.2	**Manipulation de la télématique du véhicule** (par exemple, manipulation de la mesure de la température de marchandises qui y sont sensibles, déverrouillage à distance des portes de chargement)
			16.3	Interférence avec des **systèmes** ou capteurs **sans fil à courte portée**
	17	Utilisation de logiciels tiers embarqués, comme les applications de divertissement, pour attaquer les systèmes du véhicule	17.1	Utilisation d'**applications corrompues**, ou dont la sécurité logicielle est déficiente, pour attaquer des systèmes du véhicule
	18	Utilisation de dispositifs connectés à des interfaces externes, par exemple des ports USB ou le port OBD, pour attaquer les systèmes du véhicule	18.1	**Interfaces externes** telles que les ports USB ou autres utilisées comme point d'attaque, par exemple par injection de code
			18.2	Support infecté par un **virus** connecté à un système du véhicule
			18.3	**Accès diagnostique (par exemple, dongles dans le port OBD)** utilisé pour faciliter une attaque, comme la manipulation (directe ou indirecte) des paramètres du véhicule
4.3.6 Menaces pour les données ou le code du véhicule	19	Extraction des données ou du code du véhicule	19.1	Extraction de logiciels soumis à des droits d'auteur ou propriétaires des systèmes du véhicule (**piratage** de produits)

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			*Exemple de vulnérabilité ou de méthode d'attaque*	
			19.2	Accès non autorisé aux **données personnelles du propriétaire**, notamment concernant son identité, son compte de paiement, son carnet d'adresses, sa localisation, l'identifiant électronique du véhicule, etc.
			19.3	Extraction de clefs cryptographiques
	20	Manipulation des données ou du code du véhicule	20.1	Modifications illicites/non autorisées de l'**identifiant électronique du véhicule**
			20.2	**Usurpation d'identité**. Par exemple, si un utilisateur souhaite afficher une autre identité lorsqu'il communique avec les systèmes de péage, le système dorsal du constructeur
			20.3	Mesure visant à **contourner les systèmes de surveillance** (par exemple, piratage/altération/blocage de messages tels que les données ODR Tracker ou le nombre de passages)
			20.4	Manipulation des données visant à **falsifier les données de conduite du véhicule** (kilométrage, vitesse de conduite, itinéraire, etc.)
			20.5	Modifications non autorisées des **données de diagnostic du système**
	21	Effacement des données ou du code	21.1	Effacement/manipulation non autorisé(e) des **journaux d'événements du système**
	22	Introduction de logiciels malveillants	22.2	Introduire un **logiciel malveillant** ou une activité logicielle malveillante
	23	Introduction de nouveaux logiciels ou écrasement de logiciels existants	23.1	**Fabrication du logiciel** du système de commande ou d'information du véhicule
	24	Perturbation des systèmes ou des opérations	24.1	**Déni de service** que l'on peut, par exemple, déclencher sur le réseau interne en inondant un bus CAN, ou en provoquant des pannes sur un module de gestion électronique par l'envoi d'un grand nombre de messages
	25	Manipulation des paramètres du véhicule	25.1	Accès non autorisé visant à **falsifier les paramètres de configuration** des fonctions critiques du véhicule, telles que les données de freinage, le seuil de déploiement du coussin gonflable, etc.
			25.2	Accès non autorisé visant à **falsifier les paramètres de charge**, tels que la tension de charge, la puissance de charge, la température de la batterie, etc.
4.3.7 Vulnérabilités potentielles susceptibles d'être	26	Les technologies cryptographiques peuvent être compromises ou ne sont pas	26.1	L'utilisation de courtes **clefs cryptographiques** ayant une longue période de validité permet à l'attaquant de casser le cryptage

Descriptions de haut niveau et de sous-niveau de la vulnérabilité/menace			*Exemple de vulnérabilité ou de méthode d'attaque*	
exploitées si elles ne sont pas suffisamment protégées ou réduites		suffisamment appliquées	26.2	Recours insuffisant aux algorithmes cryptographiques pour protéger les systèmes vulnérables
			26.3	Utilisation d'**algorithmes cryptographiques** obsolètes ou sur le point de l'être
	27	Des pièces ou des fournitures pourraient être compromises afin que les véhicules puissent être attaqués	27.1	**Matériel ou logiciel que l'on modifie pour permettre une attaque** ou qui ne répond pas aux critères de conception permettant de bloquer une attaque
	28	La conception des logiciels ou du matériel est à l'origine de vulnérabilités	28.1	**Bogues logiciels**. La présence de bogues logiciels peut être la cause de vulnérabilités potentiellement exploitables, en particulier si l'on n'a pas contrôlé le logiciel pour vérifier l'absence de mauvais code ou de bogues connus et pour réduire le risque de leur présence.
			28.2	**L'utilisation des restes** de la phase de développement (ports de débogage, ports JTAG, microprocesseurs, certificats de développement, mots de passe des développeurs, etc.) peut permettre l'accès aux modules de gestion électronique ou permettre à des attaquants d'obtenir des privilèges plus élevés
	29	La conception des réseaux introduit des vulnérabilités	29.1	**Ports Internet superflus laissés ouverts**, donnant accès aux systèmes réseau
			29.2	Contourner la **séparation réseau** pour en prendre le contrôle. Par exemple, en utilisant des passerelles non protégées, ou des points d'accès (tels que les passerelles camion-remorque), pour contourner les protections et accéder à d'autres segments du réseau en vue de commettre des actes malveillants, comme l'envoi de messages arbitraires sur le bus CAN
	31	Le transfert involontaire de données est possible	31.1	Atteinte à la sécurité de l'information. Des données personnelles peuvent être divulguées lorsque la **voiture change de main** (par exemple, en cas de vente ou d'utilisation comme véhicule de location par de nouveaux clients)
	32	La manipulation physique des systèmes peut permettre une attaque	32.1	**Manipulation du matériel électronique**, par exemple ajout de matériel non autorisé à un véhicule pour permettre une attaque de « l'homme du milieu » **Remplacement de matériel électronique autorisé** (par exemple capteurs) par du matériel électronique non autorisé **Manipulation des informations** recueillies par un capteur (par exemple utilisation d'un aimant pour altérer le capteur à effet Hall relié à la boîte de vitesses)

Partie B
Mesures d'atténuation des menaces visant les véhicules

1. Mesures d'atténuation − « Voies de communication des véhicules »

Les mesures d'atténuation des menaces liées aux voies de communication des véhicules sont indiquées dans le tableau B1.

Tableau B1
Mesures d'atténuation des menaces liées aux voies de communication des véhicules

Référence du tableau A1	*Menace liée aux voies de communication des véhicules*	*Réf.*	*Mesure d'atténuation*
4.1	Simulation de messages (par exemple, 802.11p V2X en cas de circulation en peloton, messages GNSS, etc.) par usurpation d'identité	M10	Le véhicule doit vérifier l'authenticité et l'intégrité des messages qu'il reçoit.
4.2	Attaque Sybil (visant à simuler d'autres véhicules pour faire croire qu'il y en a beaucoup sur la route)	M11	Des contrôles de sécurité doivent être mis en œuvre pour le stockage des clefs cryptographiques (par exemple au moyen de modules matériels de sécurité).
5.1	Les voies de communication permettent l'injection de code dans les données ou le code du véhicule, par exemple un code binaire altéré peut être injecté dans le flux de communication	M10 M6	Le véhicule doit vérifier l'authenticité et l'intégrité des messages qu'il reçoit. La sécurité doit être prise en compte dans la conception des systèmes afin que les risques soient réduits au minimum.
5.2	Les voies de communication permettent de manipuler les données ou le code du véhicule	M7	Des techniques et des conceptions de contrôle de l'accès doivent être utilisées aux fins de la protection des données ou du code du système
5.3	Les voies de communication permettent d'écraser les données ou le code du véhicule		
5.4 21.1	Les voies de communication permettent d'effacer les données ou le code du véhicule		
5.5	Les voies de communication permettent l'introduction de données ou de code dans les systèmes du véhicule (écriture de données ou de code)		
6.1	Acceptation d'informations provenant d'une source non fiable	M10	Le véhicule doit vérifier l'authenticité et l'intégrité des messages qu'il reçoit.
6.2	Attaque de l'homme du milieu/ détournement de session	M10	Le véhicule doit vérifier l'authenticité et l'intégrité des messages qu'il reçoit.
6.3	Attaque par rejeu, par exemple une attaque contre une passerelle de communication permettant à l'attaquant d'installer une version antérieure du logiciel d'un module de gestion électronique ou du microprogramme de la passerelle		
7.1	Interception de l'information/rayonnements brouilleurs/surveillance des communications	M12	Les données confidentielles reçues et transmises par le véhicule doivent être protégées.

Référence du tableau A1	*Menace liée aux voies de communication des véhicules*	*Réf.*	*Mesure d'atténuation*
7.2	Obtention d'un accès non autorisé à des fichiers ou à des données	M8	La conception du système et le contrôle de l'accès devraient empêcher que des personnes non autorisées puissent accéder à des données personnelles ou à des données critiques du système. Pour des exemples de contrôles de sécurité, voir OWASP.
8.1	Envoi d'un grand nombre de données parasites au système d'information du véhicule, de sorte qu'il soit incapable de fournir des services de manière normale	M13	Des mesures visant à détecter une attaque par déni de service et à s'en remettre doivent être mises en œuvre.
8.2	Attaque par trou noir, perturbation de la communication entre les véhicules par blocage du transfert de messages vers d'autres véhicules	M13	Des mesures visant à détecter une attaque par déni de service et à s'en remettre doivent être mises en œuvre.
9.1	Un utilisateur sans privilèges peut obtenir un accès privilégié, par exemple un accès racine	M9	Des mesures visant à empêcher et à détecter les accès non autorisés doivent être mises en œuvre.
10.1	Un virus introduit dans les moyens de communication infecte les systèmes du véhicule	M14	Des mesures de protection des systèmes contre les virus/logiciels malveillants intégrés devraient être envisagées.
11.1	Messages internes malveillants (par exemple, bus CAN)	M15	Des mesures de détection des messages ou activités internes malveillant(e)s devraient être envisagées.
11.2	Messages V2X malveillants, par exemple, messages d'infrastructure à véhicule ou de véhicule à véhicule (CAM, DENM, etc.)	M10	Le véhicule doit vérifier l'authenticité et l'intégrité des messages qu'il reçoit.
11.3	Messages de diagnostic malveillants		
11.4	Messages propriétaires malveillants (par exemple, ceux normalement envoyés par les équipementiers ou les fournisseurs de composants/systèmes/fonctions)		

2. Mesures d'atténuation – « Processus de mise à jour »

Les mesures d'atténuation des menaces liées au processus de mise à jour sont indiquées dans le tableau B2.

Tableau B2
Mesures d'atténuation des menaces liées au processus de mise à jour

Référence du tableau A1	*Menace liée au processus de mise à jour*	*Réf.*	*Mesure d'atténuation*
12.1	Compromission des procédures de mise à jour logicielle sans fil, y compris la fabrication du programme ou du microprogramme de mise à jour du système	M16	Des procédures sécurisées de mise à jour logicielle doivent être utilisées.
12.2	Compromission des procédures de mise à jour logicielle locales/physiques, y compris la fabrication du programme ou du microprogramme de mise à jour du système		

Référence du tableau A1	*Menace liée au processus de mise à jour*	*Réf.*	*Mesure d'atténuation*
12.3	Le logiciel est manipulé avant le processus de mise à jour (il est donc corrompu), bien que le processus de mise à jour soit intact		
12.4	Compromission des clefs cryptographiques du fournisseur du logiciel visant à permettre une mise à jour non valide	M11	Des contrôles de sécurité doivent être mis en œuvre pour le stockage des clefs cryptographiques.
13.1	Attaque par déni de service contre le serveur ou le réseau de mise à jour pour empêcher le déploiement de mises à jour logicielles critiques et/ou le déverrouillage de fonctionnalités spécifiques au client	M3	Des contrôles de sécurité doivent être réalisés sur les systèmes dorsaux. Lorsque les serveurs dorsaux sont essentiels à la prestation des services, des mesures de rétablissement sont disponibles en cas de panne du système. Pour des exemples de contrôles de sécurité, voir OWASP.

3. Mesures d'atténuation – « Actions humaines non intentionnelles qui facilitent les cyberattaques »

Les mesures d'atténuation des menaces liées aux actions humaines non intentionnelles qui facilitent les cyberattaques sont indiquées dans le tableau B3.

Tableau B3
Mesures d'atténuation des menaces liées aux actions humaines non intentionnelles qui facilitent les cyberattaques

Référence du tableau A1	*Menace liée aux actions humaines non intentionnelles*	*Réf.*	*Mesure d'atténuation*
15.1	Victime innocente (par exemple, propriétaire, opérateur ou ingénieur de maintenance) amenée par la ruse et à son insu à charger un logiciel malveillant ou à permettre une attaque	M18	Des mesures visant à définir et à contrôler les rôles des utilisateurs et les privilèges d'accès doivent être mises en œuvre selon le principe du moindre privilège.
15.2	Les procédures de sécurité définies ne sont pas suivies	M19	Les entreprises doivent s'assurer que les procédures de sécurité sont définies et suivies, notamment pour ce qui est du journal d'actions et des accès réservés à la gestion des fonctions de sécurité.

4. Mesures d'atténuation – « Connectivité et connexions externes »

Les mesures d'atténuation des menaces liées à la connectivité et aux connexions externes sont indiquées dans le tableau B4.

Tableau B4
Mesures d'atténuation des menaces liées à la connectivité et aux connexions externes

Référence du tableau A1	*Menace liée à la connectivité et aux connexions externes*	*Réf.*	*Mesure d'atténuation*
16.1	Manipulation des fonctions conçues pour commander à distance des systèmes du véhicule, tels qu'une clef à distance, un dispositif d'immobilisation et une pile de chargement	M20	Des contrôles de sécurité doivent être réalisés sur les systèmes qui ont un accès à distance.

Référence du tableau A1	*Menace liée à la connectivité et aux connexions externes*	*Réf.*	*Mesure d'atténuation*
16.2	Manipulation de la télématique du véhicule (par exemple, manipulation de la mesure de la température de marchandises qui y sont sensibles, déverrouillage à distance des portes de chargement)		
16.3	Interférence avec des systèmes ou capteurs sans fil à courte portée		
17.1	Utilisation d'applications corrompues, ou dont la sécurité logicielle est déficiente, pour attaquer des systèmes du véhicule	M21	Les logiciels doivent faire l'objet d'une évaluation de sécurité, ils doivent être authentifiés et leur intégrité doit être protégée. Des contrôles de sécurité doivent être réalisés de façon à ce que le risque lié aux logiciels tiers destinés à être installés sur le véhicule ou vraisemblablement susceptibles de l'être soit réduit au minimum.
18.1	Interfaces externes telles que les ports USB ou autres utilisées comme point d'attaque, par exemple par injection de code	M22	Des contrôles de sécurité doivent être réalisés sur les interfaces externes.
18.2	Support infecté par des virus connecté au véhicule		
18.3	Accès diagnostique (par exemple, dongles dans le port OBD) utilisé pour faciliter une attaque, comme la manipulation (directe ou indirecte) des paramètres du véhicule	M22	Des contrôles de sécurité doivent être réalisés sur les interfaces externes.

5. Mesures d'atténuation – « Cibles ou motivations potentielles d'une attaque »

Les mesures d'atténuation des menaces liées aux cibles ou motivations potentielles d'une attaque sont indiquées dans le tableau B5.

Tableau B5
Mesures d'atténuation des menaces liées aux cibles ou motivations potentielles d'une attaque

Référence du tableau A1	*Menace liée aux cibles ou motivations potentielles d'une attaque*	*Réf.*	*Mesure d'atténuation*
19.1	Extraction de logiciels soumis à des droits d'auteur ou propriétaires des systèmes du véhicule (piratage de produits/logiciel volé)	M7	Des techniques et des conceptions de contrôle de l'accès doivent être utilisées pour protéger les données ou le code du système. Pour des exemples de contrôles de sécurité, voir OWASP.
19.2	Accès non autorisé aux données personnelles du propriétaire, notamment concernant son identité, son compte de paiement, son carnet d'adresses, sa localisation, l'identifiant électronique du véhicule, etc.	M8	La conception du système et le contrôle de l'accès devraient empêcher que des personnes non autorisées puissent accéder à des données personnelles ou à des données critiques du système. Pour des exemples de contrôles de sécurité, voir OWASP.
19.3	Extraction de clefs cryptographiques	M11	Des contrôles de sécurité doivent être mis en œuvre pour le stockage des clefs cryptographiques, par exemple des modules de sécurité.

Référence du tableau A1	*Menace liée aux cibles ou motivations potentielles d'une attaque*	*Réf.*	*Mesure d'atténuation*
20.1	Modifications illicites/non autorisées de l'identifiant électronique du véhicule	M7	Des techniques et des conceptions de contrôle de l'accès doivent être utilisées pour protéger les données ou le code du système. Pour des exemples de contrôles de sécurité, voir OWASP.
20.2	Usurpation d'identité. Par exemple, si un utilisateur souhaite afficher une autre identité lorsqu'il communique avec les systèmes de péage, le système dorsal du constructeur		
20.3	Mesure visant à contourner les systèmes de surveillance (par exemple, piratage/ altération/ blocage de messages tels que les données ODR Tracker ou le nombre de passages)	M7	Des techniques et des conceptions de contrôle de l'accès doivent être utilisées afin que les données ou le code du système soient protégés. Pour des exemples de contrôles de sécurité, voir OWASP. Il est possible d'atténuer les attaques qui consistent à manipuler des données et ciblent des capteurs ou des données transmises grâce à un recoupement des données provenant de différentes sources d'information.
20.4	Manipulation des données visant à falsifier les données de conduite du véhicule (kilométrage, vitesse de conduite, itinéraire, etc.)		
20.5	Modifications non autorisées des données de diagnostic du système		
21.1	Effacement/manipulation non autorisé(e) des journaux d'événements du système	M7	Des techniques et des conceptions de contrôle de l'accès doivent être utilisées pour protéger les données ou le code du système. Pour des exemples de contrôles de sécurité, voir OWASP.
22.2	Introduire un logiciel malveillant ou une activité logicielle malveillante	M7	Des techniques et des conceptions de contrôle de l'accès doivent être utilisées afin que les données ou le code du système soient protégés. Pour des exemples de contrôles de sécurité, voir OWASP.
23.1	Fabrication du logiciel du système de commande ou d'information du véhicule		
24.1	Déni de service que l'on peut, par exemple, déclencher sur le réseau interne en inondant un bus CAN, ou en provoquant des pannes sur un module de gestion électronique par l'envoi d'un grand nombre de messages	M13	Des mesures visant à détecter une attaque par déni de service et à s'en remettre doivent être mises en œuvre.
25.1	Accès non autorisé visant à falsifier les paramètres de configuration des fonctions critiques du véhicule, telles que les données de freinage, le seuil de déploiement du coussin gonflable, etc.	M7	Des techniques et des conceptions de contrôle de l'accès doivent être utilisées afin que les données ou le code du système soient protégés. Pour des exemples de contrôles de sécurité, voir OWASP.
25.2	Accès non autorisé visant à falsifier les paramètres de charge, tels que la tension de charge, la puissance de charge, la température de la batterie, etc.		

6. Mesures d'atténuation – « Vulnérabilités potentielles susceptibles d'être exploitées si elles ne sont pas suffisamment protégées ou réduites »

Les mesures d'atténuation des menaces liées aux vulnérabilités potentielles susceptibles d'être exploitées si elles ne sont pas suffisamment protégées ou réduites sont indiquées dans le tableau B6.

Tableau B6
Mesures d'atténuation des menaces liées aux vulnérabilités potentielles susceptibles d'être exploitées si elles ne sont pas suffisamment protégées ou réduites

Référence du tableau A1	*Menace liée aux vulnérabilités potentielles susceptibles d'être exploitées si elles ne sont pas suffisamment protégées ou réduites*	*Réf.*	*Mesure d'atténuation*
26.1	L'utilisation de courtes clefs cryptographiques ayant une longue période de validité permet à l'attaquant de casser le cryptage	M23	Les meilleures pratiques de cybersécurité doivent être suivies dans le cadre du développement des logiciels et du matériel.
26.2	Recours insuffisant aux algorithmes cryptographiques pour protéger les systèmes vulnérables		
26.3	Utilisation d'algorithmes cryptographiques obsolètes		
27.1	Matériel ou logiciel que l'on modifie pour permettre une attaque ou qui ne répond pas aux critères de conception permettant de bloquer une attaque	M23	Les meilleures pratiques de cybersécurité doivent être suivies dans le cadre du développement des logiciels et du matériel.
28.1	La présence de bogues logiciels peut être la cause de vulnérabilités potentiellement exploitables, en particulier si l'on n'a pas testé le logiciel pour vérifier l'absence de mauvais code ou de bogues connus et pour réduire le risque de leur présence.	M23	Les meilleures pratiques de cybersécurité doivent être suivies lors du développement des logiciels et du matériel. Les contrôles en matière de cybersécurité doivent avoir une portée suffisante.
28.2	L'utilisation des restes de la phase de développement (ports de débogage, ports JTAG, microprocesseurs, certificats de développement, mots de passe des développeurs, etc.) peut permettre à un attaquant d'accéder aux modules de gestion électronique ou d'obtenir des privilèges plus élevés		
29.1	Ports Internet superflus laissés ouverts, donnant accès aux systèmes réseau		
29.2	Contourner la séparation réseau pour en prendre le contrôle. Par exemple, en utilisant des passerelles non protégées, ou des points d'accès (tels que les passerelles camion-remorque), pour contourner les protections et accéder à d'autres segments du réseau en vue de commettre des actes malveillants, comme l'envoi de messages arbitraires sur le bus CAN	M23	Les meilleures pratiques de cybersécurité doivent être suivies lors du développement des logiciels et du matériel. Les meilleures pratiques de cybersécurité en matière de conception et d'intégration des systèmes doivent être suivies.

7. Mesures d'atténuation − « Perte de données/violation des données du véhicule »

Les mesures d'atténuation des menaces liées à la perte de données ou à la violation des données du véhicule sont indiquées dans le tableau B7.

Tableau B7
Mesures d'atténuation des menaces liées à la perte de données ou à la violation des données du véhicule

Référence du tableau A1	*Menace liée à la perte de données/ou à la violation des données du véhicule*	*Réf.*	*Mesure d'atténuation*
31.1	Atteinte à la sécurité de l'information. Des données personnelles ou confidentielles peuvent être divulguées lorsque la voiture change de main (par exemple, en cas de vente ou d'utilisation comme véhicule de location par de nouveaux clients)	M24	Les meilleures pratiques de protection de l'intégrité et de la confidentialité des données doivent être suivies pour le stockage des données personnelles.

8. Mesures d'atténuation − « Manipulation physique des systèmes en vue de permettre une attaque »

Les mesures d'atténuation des menaces liées à la manipulation physique des systèmes en vue de permettre une attaque sont indiquées dans le tableau B8.

Tableau B8
Mesures d'atténuation des menaces liées à la manipulation physique des systèmes en vue de permettre une attaque

Référence du tableau A1	*Menace liée à la manipulation physique des systèmes en vue de permettre une attaque*	*Réf.*	*Mesure d'atténuation*
32.1	Manipulation du matériel électronique, par exemple ajout de matériel non autorisé à un véhicule pour permettre une attaque de l'homme du milieu	M9	Des mesures visant à empêcher et à détecter les accès non autorisés doivent être prises.

Partie C
Mesures d'atténuation des menaces visant les zones situées en dehors des véhicules

1. Mesures d'atténuation − « Serveurs dorsaux »

Les mesures d'atténuation des menaces liées aux serveurs dorsaux sont indiquées dans le tableau C1.

Tableau C1
Mesures d'atténuation des menaces liées aux serveurs dorsaux

Référence du tableau A1	*Menace liée aux serveurs dorsaux*	*Réf.*	*Mesure d'atténuation*
1.1 et 3.1	Abus de privilèges de la part du personnel (attaque d'initié)	M1	Des contrôles de sécurité doivent être réalisés sur les systèmes dorsaux afin que le risque d'attaques d'initié soit réduit au minimum.
1.2 et 3.3	Accès Internet non autorisé au serveur (activé par exemple par des portes dérobées, des vulnérabilités logicielles système non corrigées, des attaques SQL ou d'autres moyens)	M2	Des contrôles de sécurité doivent être réalisés sur les systèmes dorsaux afin que les accès non autorisés soient réduits au minimum. Pour des exemples de contrôles de sécurité, voir OWASP.
1.3 et 3.4	Accès physique non autorisé au serveur (au moyen, par exemple, de clefs USB ou d'autres supports connectés au serveur)	M8	La conception du système et le contrôle de l'accès devraient empêcher que des personnes non autorisées puissent accéder à des données personnelles ou des données critiques du système.

Référence du tableau A1	*Menace liée aux serveurs dorsaux*	*Réf.*	*Mesure d'atténuation*
2.1	Attaque d'un serveur dorsal bloquant son fonctionnement, par exemple en l'empêchant d'interagir avec les véhicules et de fournir les services dont ils ont besoin	M3	Des contrôles de sécurité doivent être réalisés sur les systèmes dorsaux. Lorsque les serveurs dorsaux sont essentiels à la prestation des services, des mesures de rétablissement doivent être disponibles en cas de panne du système. Pour des exemples de contrôles de sécurité, voir OWASP.
3.2	Perte d'informations dans le « nuage ». Des données sensibles peuvent être perdues en raison d'attaques ou d'accidents lorsque les données sont stockées par des fournisseurs de services en nuage tiers	M4	Des contrôles de sécurité doivent être réalisés pour que les risques associés à l'informatique en nuage soient réduits au minimum. Pour des exemples de contrôles de sécurité, voir OWASP et les orientations NCSC sur l'informatique en nuage.
3.5	Atteinte à la sécurité de l'information due au partage involontaire de données (par exemple, erreurs administratives, stockage des données sur des serveurs situés dans des garages)	M5	Des contrôles de sécurité visant à éviter les atteintes à la sécurité des données doivent être réalisés sur les systèmes dorsaux. Pour des exemples de contrôles de sécurité, voir OWASP.

2. Mesures d'atténuation – « Actions humaines non intentionnelles »

Les mesures d'atténuation des menaces liées aux actions humaines non intentionnelles sont indiquées dans le tableau C2.

Tableau C2
Mesures d'atténuation des menaces liées aux actions humaines non intentionnelles

Référence du tableau A1	*Menace liée aux actions humaines non intentionnelles*	*Réf.*	*Mesure d'atténuation*
15.1	Victime innocente (par exemple, propriétaire, opérateur ou ingénieur de maintenance) amenée par la ruse et à son insu à charger un logiciel malveillant ou à permettre une attaque	M18	Des mesures visant à définir et à contrôler les rôles des utilisateurs et les privilèges d'accès doivent être mises en œuvre selon le principe du moindre privilège.
15.2	Les procédures de sécurité définies ne sont pas suivies	M19	Les entreprises doivent s'assurer que les procédures de sécurité sont définies et suivies, notamment pour ce qui est du journal d'actions et des accès réservés à la gestion des fonctions de sécurité.

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

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

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

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

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

[RUSSIAN TEXT – TEXTE RUSSE]

Предложение по новым правилам о единообразных предписаниях, касающихся официального утверждения транспортных средств в отношении кибербезопасности и системы обеспечения кибербезопасности

Представлено Рабочей группой по автоматизированным/автономным и подключенным транспортным средствам*

Воспроизведенный ниже текст, в котором предлагаются новые правила ООН о единообразных предписаниях, касающихся официального утверждения транспортных средств в отношении кибербезопасности и системы обеспечения кибербезопасности, был подготовлен Целевой группой по вопросам кибербезопасности и беспроводной связи и рассмотрен GRVA. Он был подготовлен в соответствии с Рамочным документом о безопасности автоматизированных транспортных средств ECE/TRANS/WP.29/2019/34 с внесенными в него изменениями. Он был принят Рабочей группой по автоматизированным/автономным и подключенным транспортным средствам на ее пятой сессии (см. ECE/TRANS/WP.29/GRVA/6, пункт 23) на основе документа ECE/TRANS/WP29/GRVA/2020/3 с поправками, внесенными в него в соответствии с документом GRVA-06-19-Rev.1. Этот текст представлен Всемирному форуму для согласования правил в области транспортных средств (WP.29) и его Административному комитету Соглашения 1958 года (AC.1) для рассмотрения и голосования на их сессиях в июне 2020 года.

* В соответствии с программой работы Комитета по внутреннему транспорту на 2020 год, изложенной в предлагаемом бюджете по программам на 2020 год (A/74/6 (часть V, раздел 20), пункт 20.37), Всемирный форум будет разрабатывать, согласовывать и обновлять Правила Организации Объединенных Наций в целях повышения эффективности автотранспортных средств. Настоящий документ представлен в соответствии с этим мандатом.

GRVA не смогла завершить работу над пунктом 5.3 из-за нехватки времени. Договаривающиеся Стороны, выразившие свою позицию по этому пункту, вызвались продолжить обсуждение после сессии и подготовить документ с целью решения проблемы, связанной с пунктом 5.3 и подпунктами, в дополнение к настоящему документу. Этот документ имеет условное обозначение ECE/TRANS/WP.29/2020/97.

Правила ООН о единообразных предписаниях, касающихся официального утверждения транспортных средств в отношении кибербезопасности и их систем обеспечения кибербезопасности

Содержание

** Номера страниц будут добавлены позднее.

1. Сфера применения

1.1 Настоящие Правила применяются к транспортным средствам категорий M и N в отношении кибербезопасности.

Настоящие Правила применяются также к транспортным средствам категории O, если они оснащены по меньшей мере одним электронным блоком управления.

1.2 Настоящие Правила применяются также к транспортным средствам категорий L_6 и L_7, если они оснащены автоматизированной функцией управления транспортным средством, начиная с уровня 3 и выше, как это определено в справочном документе с определениями термина «автоматизированное вождение» в рамках WP.29 и Общих принципах для разработки правил ООН, касающихся автоматизированных транспортных средств (ECE/TRANS/WP.29/1140).

1.3 Настоящие Правила применяются без ущерба для иных правил ООН, а равно регионального или национального законодательства, регулирующих доступ уполномоченных сторон к транспортному средству, его бортовым данным, функциям и ресурсам, а также условия такого доступа. Они также применяются без ущерба для национального и регионального законодательства, регулирующего неприкосновенность частной жизни и защиты физических лиц в части обработки их персональных данных.

1.4 Настоящие Правила применяются без ущерба для иных Правил ООН, а равно национального или регионального законодательства, регулирующих разработку и установку/системную интеграцию запасных частей и компонентов, как физических, так и цифровых, в части кибербезопасности.

2. Определения

Для целей настоящих Правил применяются следующие определения:

2.1 «*Тип транспортного средства*» означает транспортные средства, не имеющие различий в отношении следующих основных аспектов:

a) обозначения изготовителя данного типа транспортного средства;

b) основных аспектов электрической/электронной архитектуры и внешних интерфейсов применительно к кибербезопасности.

2.2 «*Кибербезопасность*» означает состояние, в котором транспортные средства и их функции защищены от киберугроз, которым могут подвергаться электрические или электронные компоненты.

2.3 «*Система обеспечения кибербезопасности (СОКиБ)*» означает систематический подход на основе оценки риска, определяющий организационные процессы, обязанности и методы обработки риска, связанного с киберугрозами, которым подвергаются транспортные средства, и их защиты от кибератак.

2.4 «*Система*» означает совокупность компонентов и/или подсистем, реализующих соответствующую функцию или функции.

2.5 «*Этап разработки*» означает период до официального утверждения данного типа транспортного средства.

2.6 «*Этап производства*» означает продолжительность производства соответствующего типа транспортного средства.

2.7 «*Этап после производства*» означает период, в течение которого данный тип транспортного средства более не производится до окончания срока службы всех транспортных средств данного типа. Транспортные средства, включающие конкретный тип транспортного средства, будут эксплуатироваться на этом этапе, но производиться больше не будут. Данный этап заканчивается в тот момент, когда в эксплуатации больше нет никаких транспортных средств, относящихся к конкретному типу транспортного средства.

2.8 «*Смягчение последствий*» означает соответствующую меру, которая позволяет изменить уровень риска.

2.9 «*Риск*» означает вероятность того, что какая-либо угроза реализуется на практике вследствие уязвимостей того или иного транспортного средства и тем самым причинит вред организации или отдельному лицу.

2.10 «*Оценка риска*» означает всесторонний процесс выявления, распознавания и описания рисков (идентификация риска) в целях понимания характера риска и определения его уровня (анализ риска) и сопоставления результатов анализа риска с критериями риска в порядке выяснения того факта, является ли данный риск и/или его масштаб приемлемым или допустимым (оценка риска).

2.11 «*Управление риском*» означает согласованные действия по руководству и управлению соответствующей организацией в связи с риском.

2.12 «*Угроза*» означает потенциальную причину нежелательного инцидента, который может нанести ущерб системе или организации.

2.13 «*Уязвимость*» означает слабость какого-либо материального объекта или средства смягчения последствий, которая дает возможность реализации одной или нескольких угроз.

3. Заявка на официальное утверждение

3.1 Заявка на официальное утверждение типа транспортного средства в отношении кибербезопасности подается изготовителем транспортного средства или его должным образом уполномоченным представителем.

3.2 К заявке прилагаются перечисленные ниже документы в трех экземплярах и следующие дополнительные сведения:

3.2.1 описание типа транспортного средства с указанием данных, предусмотренных в приложении 1 к настоящим Правилам;

3.2.2 в тех случаях, когда указано, что информация защищена правами интеллектуальной собственности или относится к разряду специальных научных знаний изготовителя или его поставщиков, изготовитель или его поставщики предоставляют достаточную информацию, позволяющую надлежащим образом провести проверки, указанные в настоящих Правилах. С такой информацией обращаются на конфиденциальной основе;

3.2.3 свидетельство о соответствии СОКиБ на основании пункта 6 настоящих Правил.

3.3 Должна быть доступна документация следующих двух видов:

a) официальный набор документов для официального утверждения, содержащий материалы, указанные в приложении 1, которые передаются органу по официальному утверждению или технической службе в момент подачи заявки на официальное утверждение типа. Этот набор документации используется органом по официальному утверждению или его технической службой в качестве основного справочного материала для

процесса официального утверждения. Орган по официальному утверждению или его техническая служба обеспечивает доступность этого набора документации в течение 10 лет начиная с момента окончательного прекращения производства данного типа транспортного средства;

b) дополнительные материалы, относящиеся к требованиям настоящих Правил, могут оставаться на хранении у изготовителя, но должны предоставляться для проверки во время официального утверждения типа. Изготовитель обеспечивает доступность любых материалов, предоставляемых для проверки в ходе официального утверждения, в течение не менее 10 лет начиная с момента окончательного прекращения производства данного типа транспортного средства.

4. Маркировка

4.1 На каждом транспортном средстве, соответствующем типу транспортного средства, официально утвержденному на основании настоящих Правил, проставляется на видном и легкодоступном месте, указанном в регистрационной карточке официального утверждения, международный знак официального утверждения, состоящий из:

4.1.1 круга с проставленной в нем буквой «E», за которой следует отличительный номер страны, предоставившей официальное утверждение;

4.1.2 номера настоящих Правил, за которым следуют буква «R», тире и номер официального утверждения, проставленные справа от круга, предусмотренного в пункте 4.1.1, выше.

4.2 Если транспортное средство соответствует типу транспортного средства, официально утвержденному на основании одного или нескольких других прилагаемых к Соглашению правил в той же стране, которая предоставила официальное утверждение на основании настоящих Правил, то обозначение, предписанное в пункте 4.1.1, выше, повторять не нужно; в таком случае номера правил и официального утверждения, а также дополнительные обозначения всех правил, на основании которых было предоставлено официальное утверждение в стране, предоставившей официальное утверждение на основании настоящих Правил, должны быть расположены в вертикальных колонках справа от обозначения, предписанного в пункте 4.1.1, выше.

4.3 Знак официального утверждения должен быть четким и нестираемым.

4.4 Знак официального утверждения помещается рядом с прикрепляемой изготовителем табличкой, на которой приведены характеристики транспортного средства, или наносится на эту табличку.

4.5 В приложении 3 к настоящим Правилам в качестве примера приведены схемы знаков официального утверждения.

5. Официальное утверждение

5.1 Органы по официальному утверждению предоставляют в надлежащих случаях официальное утверждение типа в отношении кибербезопасности только таким типам транспортных средств, которые удовлетворяют требованиям настоящих Правил.

5.1.1 Орган по официальному утверждению или техническая служба проверяет посредством ознакомления с документацией, что

изготовителем транспортного средства приняты необходимые меры, имеющие отношение к данному типу транспортного средства, в целях:

a) сбора и проверки информации, требуемой на основании настоящих Правил в пределах производственно-сбытовой цепочки, чтобы продемонстрировать, что риски, связанные с поставщиками, выявлены и управляются;

b) документального оформления оценки рисков (проводимой на этапе разработки или ретроспективно), результатов испытаний и мер по смягчению последствий применительно к данному типу транспортного средства, включая проектную информацию, подтверждающую оценку рисков;

c) принятия надлежащих мер по обеспечению кибербезопасности конструкции данного типа транспортного средства;

d) обнаружения возможных атак на кибербезопасность и реагирования на них;

e) регистрации данных для поддержки обнаружения кибератак и обеспечения возможностей криминалистической экспертизы данных для анализа предпринятых попыток проведения кибератак или успешных кибератак.

5.1.2 Орган по официальному утверждению или техническая служба проводит проверку путем испытания транспортного средства данного типа с целью убедиться в том, что изготовитель данного транспортного средства принял надлежащие меры кибербезопасности и документально зафиксировал их. Испытания проводятся органом по официальному утверждению или самой технической службой либо в сотрудничестве с изготовителем транспортного средства путем отбора образцов. Отбор образцов должен быть сфокусирован на рисках, которые оцениваются как высокие в ходе оценки рисков, но не ограничиваться ими.

5.1.3 Орган по официальному утверждению или техническая служба отказывает в предоставлении официального утверждения типа в отношении кибербезопасности, если изготовитель транспортного средства не выполнил одно или несколько требований, упомянутых в пункте 7.3, в частности:

a) изготовитель транспортного средства не провел исчерпывающей оценки риска, упомянутой в пункте 7.3.3; в том числе в тех случаях, когда изготовитель не учел все риски, связанные с угрозами, указанными в части A приложения 5;

b) изготовитель транспортного средства не обеспечил защиты данного типа транспортного средства от рисков, выявленных в ходе оценки риска изготовителем данного транспортного средства, или не были приняты соразмерные меры по смягчению последствий согласно требованиям пункта 7;

c) изготовитель транспортного средства не принял надлежащих и соразмерных мер для обеспечения безопасности специальных объектов (если таковые предусмотрены) в целях хранения и реализации программного обеспечения, услуг, приложений или данных в интересах вторичного рынка применительно к данному типу транспортного средства;

d) изготовитель транспортного средства не провел, до официального утверждения, надлежащих и достаточных испытаний для проверки эффективности принятых мер безопасности.

5.1.4 Оценивающий орган по официальному утверждению отказывает также в предоставлении официального утверждения типа в отношении кибербезопасности, если орган по официальному утверждению или техническая служба не получили от изготовителя транспортного средства достаточной информации для оценки кибербезопасности данного типа транспортного средства.

5.2 Стороны Соглашения 1958 года, применяющие настоящие Правила, уведомляются об официальном утверждении, распространении официального утверждения или отказе в официальном утверждении типа транспортного средства на основании настоящих Правил посредством карточки, соответствующей образцу, приведенному в приложении 2 к настоящим Правилам.

5.3 Органы по официальному утверждению не предоставляют никакого официального утверждения типа, не убедившись в том, что изготовитель ввел в действие удовлетворительные механизмы и процедуры, позволяющие надлежащим образом регулировать аспекты кибербезопасности, охватываемые настоящими Правилами.

5.3.1–5.3.7 (Зарезервировано.)

5.4 Для целей пункта 7.2 настоящих Правил изготовитель обеспечивает реализацию на практике всех аспектов кибербезопасности, охватываемых настоящими Правилами.

6. Свидетельство о соответствии системы обеспечения кибербезопасности

6.1 Договаривающиеся стороны назначают орган по официальному утверждению для оценки изготовителя и выдачи свидетельства о соответствии СОКиБ.

6.2 Заявка на получение свидетельства о соответствии системы обеспечения кибербезопасности подается изготовителем транспортного средства или его должным образом уполномоченным представителем.

6.3 К заявке прилагаются перечисленные ниже документы в трех экземплярах и следующие дополнительные сведения:

6.3.1 документация с описанием системы обеспечения кибербезопасности;

6.3.2 подписанное заявление в соответствии с образцом, определенным в добавлении 1 к приложению 1.

6.4 В контексте этой оценки изготовитель заявляет в соответствии с образцом, определенным в добавлении 1 к приложению 1, и подтверждает к удовлетворению органа по официальному утверждению или его технической службы, что у него налажены необходимые процедуры соблюдения всех требований в отношении кибербезопасности в соответствии с настоящими Правилами.

6.5 После удовлетворительного завершения этой оценки и получения подписанного заявления от изготовителя в соответствии с образцом, определенным в добавлении 1 к приложению 1, изготовителю выдается соответствующее свидетельство под названием «свидетельство о соответствии СОКиБ», описанное в приложении 4 к настоящим Правилам (здесь и далее – свидетельство о соответствии СОКиБ).

6.6 Орган по официальному утверждению или его техническая служба использует для выдачи свидетельства о соответствии СОКиБ образец, содержащийся в приложении 4 к настоящим Правилам.

6.7 Свидетельство о соответствии СОКиБ остается действительным в течение не более трех лет со дня его выдачи, если только оно не будет отозвано.

6.8 Орган по официальному утверждению, который выдал свидетельство о соответствии СОКиБ, может в любое время проверить, продолжают ли удовлетворяться предъявляемые к нему требования. Орган по официальному утверждению отзывает свидетельство о соответствии СОКиБ, если требования, предусмотренным в настоящих Правилах, больше не соблюдаются.

6.9 Изготовитель информирует орган по официальному утверждению или его техническую службу о любом изменении, которое повлияет на применимость свидетельства о соответствии СОКиБ. После консультации с изготовителем орган по официальному утверждению или его техническая служба принимает решение о том, нужны ли новые проверки.

6.10 В конце срока действия свидетельства о соответствии СОКиБ орган по официальному утверждению выдает, на основании соответствующей положительной оценки, новое свидетельство о соответствии СОКиБ или продлевает срок его действия еще на три года. Орган по официальному утверждению выдает новое свидетельство в тех случаях, когда до его сведения или до сведения его технической службы были доведены соответствующие изменения и когда повторная оценка этих изменений дала положительные результаты.

6.11 Истечение срока действия или отзыв свидетельства о соответствии СОКиБ, выданного изготовителю, рассматривается, в отношении типов транспортных средств, к которым имела отношение соответствующая СОКиБ, как изменение официального утверждения, указанное в пункте 8.

7. Технические требования

7.1 Общие технические требования

7.1.1 Требования настоящих Правил не ограничивают действие положений или предписаний других правил ООН.

7.2 Требования, предъявляемые к системе обеспечения кибербезопасности

7.2.1 В целях оценки орган по официальному утверждению или его техническая служба удостоверяется в том, что у изготовителя транспортного средства есть соответствующая система обеспечения кибербезопасности, и удостоверяется в ее соответствии настоящим Правилам.

7.2.2 Система обеспечения кибербезопасности охватывает следующие аспекты:

7.2.2.1 Изготовитель транспортного средства подтверждает органу по официальному утверждению или его технической службе, что их система обеспечения кибербезопасности применяется к следующим этапам:

a) этап разработки;

b) этап реализации;

c) этап после реализации.

7.2.2.2 Изготовитель транспортного средства подтверждает, что процессы, используемые в рамках его системы обеспечения кибербезопасности, позволяют надлежащим образом учитывать вопросы безопасности,

включая риски и меры по смягчению последствий, перечисленные в приложении 5. Они включают следующее:

a) процессы, используемые в организации изготовителя в целях управления системой кибербезопасности;

b) процессы, используемые для выявления рисков, которым подвергаются транспортные средства. В рамках этих процессов рассматриваются угрозы, указанные в части A приложения 5, и другие соответствующие угрозы;

c) процессы, используемые для оценки, классификации и обработки выявленных рисков;

d) процессы, введенные в действие с целью удостовериться, что выявленные риски устраняются надлежащим образом;

e) процессы, используемые для проверки кибербезопасности типа транспортного средства;

f) процессы, используемые с целью обеспечить постоянное обновление оценки рисков;

g) процессы, используемые для мониторинга кибератак, киберугроз и факторов уязвимости соответствующих типов транспортных средств, их обнаружения и реагирования на них, и процессы, используемые для оценки того, являются ли принимаемые меры кибербезопасности по-прежнему эффективными в свете новых киберугроз и факторов уязвимости, которые были выявлены;

h) Процессы, используемые для предоставления соответствующих данных с целью поддержки анализа предпринятых попыток проведения кибератак или успешных кибератак.

7.2.2.3 Изготовитель транспортного средства подтверждает, что процессы, используемые в рамках его системы обеспечения кибербезопасности, будут обеспечивать, на основе классификации, упомянутой в подпунктах c) и g) пункта 7.2.2.2.2, смягчение в разумные сроки последствий киберугроз и факторов уязвимости, требующих реагирования со стороны изготовителя транспортного средства.

7.2.2.4 Изготовитель транспортного средства подтверждает, что процессы, используемые в рамках его системы обеспечения кибербезопасности, будут обеспечивать непрерывный мониторинг, упомянутый в подпункте g) пункта 7.2.2.2. Они включают следующее:

a) транспортные средства после первой регистрации в рамках мониторинга;

b) возможности анализа и обнаружения киберугроз, факторов уязвимости и кибератак на основе данных о транспортном средстве и журналов учета использования транспортного средства. Эти возможности используются с соблюдением пункта 1.3 и права владельцев или водителей автомобилей на неприкосновенность частной жизни, особенно в том, что касается согласия.

7.2.2.5 Изготовитель транспортного средства должен продемонстрировать, каким образом его система обеспечения кибербезопасности будет регулировать соответствующие аспекты взаимозависимости, которая может существовать с поставщиками изделий и услуг, с которыми заключены соответствующие контракты, или с его суборганизациями в связи с требованиями пункта 7.2.2.2.

7.3 Требования, предъявляемые к типам транспортных средств

7.3.1 Изготовитель должен иметь действующее свидетельство соответствия системы обеспечения кибербезопасности, относящееся к официально утверждаемому типу транспортного средства.

Однако, в случае официальных утверждений типа до 1 июля 2024 года, если изготовитель транспортного средства может продемонстрировать, что данный тип транспортного средства не мог быть разработан в соответствии с СОКиБ, то изготовитель транспортного средства должен продемонстрировать, что на этапе разработки соответствующего типа транспортного средства была должным образом учтена кибербезопасность.

7.3.2 Изготовитель транспортного средства идентифицирует, в отношении официально утверждаемого типа транспортного средства, риски, связанные с поставщиками, и управляет ими.

7.3.3 Изготовитель транспортного средства идентифицирует критические элементы данного типа транспортных средств и проводит исчерпывающую оценку рисков для данного типа транспортных средств, а также надлежащим образом обрабатывает выявленные риски/управляет выявленными рисками. При оценке рисков учитываются отдельные элементы типа транспортного средства и их взаимодействия. В ходе оценки рисков учитываются, кроме того, взаимодействия с любыми внешними системами. При оценке рисков изготовитель транспортного средства учитывает риски, связанные со всеми угрозами, указанными в части A приложения 5, а также любой другой соответствующий риск.

7.3.4 Изготовитель транспортного средства защищает тип транспортного средства от рисков, выявленных в ходе оценки рисков изготовителем транспортного средства. Для защиты типа транспортного средства принимаются соразмерные меры по смягчению последствий. Осуществляемые меры по смягчению последствий включают все меры по смягчению последствий, о которых говорится в частях B и C приложения 5 и которые касаются выявленных рисков. Однако, если та или иная мера по смягчению последствий, упомянутая в части B или C приложения 5, не имеет отношения к выявленному риску или является недостаточной, изготовитель транспортного средства обеспечивает осуществление какой-либо другой соответствующей меры по смягчению последствий.

В частности, в случае официальных утверждений типа до 1 июля 2024 года, изготовитель транспортного средства обеспечивает осуществление какой-либо другой соответствующей меры по смягчению последствий, если та или иная мера по смягчению последствий, упомянутая в части B или C приложения 5, технически неосуществима. Соответствующая оценка технической осуществимости предоставляется изготовителем органу по официальному утверждению.

7.3.5 Изготовитель транспортного средства принимает надлежащие и соразмерные меры для обеспечения безопасности специальных объектов (если таковые предусмотрены) в целях хранения и реализации программного обеспечения, услуг, приложений или данных в интересах вторичного рынка применительно к данному типу транспортного средства.

7.3.6 Изготовитель транспортного средства проводит, до официального утверждения, надлежащие и достаточные испытания для проверки эффективности принятых мер безопасности.

7.3.7 Изготовитель транспортного средства принимает в отношении данного типа транспортного средства соответствующие меры с целью:

a) обнаружения и предотвращения кибератак на транспортные средства данного типа;

b) поддержки возможностей мониторинга, осуществляемого изготовителем транспортного средства для обнаружения угроз, факторов уязвимости и кибератак, относящихся к данному типу транспортного средства;

c) предоставления возможностей криминалистической экспертизы данных для анализа предпринятых попыток проведения кибератак или успешных кибератак.

7.3.8 Криптографические модули, используемые для целей настоящих Правил, должны соответствовать согласованным стандартам. Если используемые криптографические модули не соответствуют согласованным стандартам, то изготовитель транспортного средства должен обосновать их использование.

7.4 Положения об отчетности

7.4.1 Изготовитель транспортного средства предоставляет по меньшей мере один раз в год или чаще, если это необходимо, органу по официальному утверждению или технической службе отчет о результатах своей деятельности по мониторингу, как она определена в подпункте g) пункта 7.2.2.2, который должен включать соответствующую информацию о новых кибератаках. Изготовитель транспортного средства также сообщает и подтверждает органу по официальному утверждению или технической службе, что меры по смягчению последствий рисков для кибербезопасности, применяемые в отношении его типов транспортных средств, по-прежнему эффективны, а также любые дополнительные меры, принятые в этой связи.

7.4.2 Орган по официальному утверждению или техническая служба проверяет представленную информацию и в случае необходимости требует от изготовителя транспортного средства устранить любую выявленную неэффективность.

Если отчетность или ответ недостаточны, орган по официальному утверждению может принять решение об отзыве СОКиБ в соответствии с пунктом 6.8.

8. Модификация и распространение официального утверждения типа транспортного средства

8.1 Любая модификация типа транспортного средства, которая сказывается на его технических характеристиках в части кибербезопасности и/или документации, требуемой в соответствии с настоящими Правилами, доводится до сведения органа по официальному утверждению, предоставившего официальное утверждение данного типа транспортного средства. Орган по официальному утверждению может либо:

8.1.1 прийти к заключению, что внесенные изменения все еще удовлетворяют действующим требованиям и документации, относящейся к существующему официальному утверждению типа; либо

8.1.2 потребовать от технической службы, ответственной за проведение испытаний, новый протокол испытания.

8.1.3 Сообщение о подтверждении официального утверждения, о распространении официального утверждения или об отказе в официальном утверждении доводится до сведения посредством карточки

сообщения, соответствующей образцу, приведенному в приложении 2 к настоящим Правилам. Орган по официальному утверждению, распространивший официальное утверждение, присваивает такому распространению соответствующий серийный номер и уведомляет об этом другие Стороны Соглашения 1958 года, применяющие настоящие Правила, посредством карточки сообщения, соответствующей образцу, приведенному в приложении 2 к настоящим Правилам.

9. Соответствие производства

9.1 Процедуры обеспечения соответствия производства должны соответствовать процедурам, изложенным в приложении 1 к Соглашению 1958 года (E/ECE/TRANS/505/Rev.3), с учетом следующих требований:

9.1.1 Держатель официального утверждения обеспечивает регистрацию данных, полученных в результате испытаний на проверку соответствия производства, а также доступ к прилагаемым документам в течение периода, определенного по договоренности с органом по официальному утверждению или его технической службой. Такой период не должен превышать 10 лет, считая с момента окончательного прекращения производства.

9.1.2 Орган по официальному утверждению, предоставивший официальное утверждение типа, может в любое время проверить методы контроля за соответствием производства, применяемые на каждом производственном объекте. Обычно такие проверки проводят один раз в три года.

10. Санкции, налагаемые за несоответствие производства

10.1 Официальное утверждение типа транспортного средства, предоставленное на основании настоящих Правил, может быть отменено, если не соблюдаются требования, изложенные в настоящих Правилах, или если образцы транспортного средства не соответствуют требованиям настоящих Правил.

10.2 Если орган по официальному утверждению отзывает предоставленное им ранее официальное утверждение, то он немедленно уведомляет об этом Договаривающиеся стороны, применяющие настоящие Правила, посредством карточки сообщения, соответствующей образцу, приведенному в приложения 2 к настоящим Правилам.

11. Окончательное прекращение производства

11.1 Если держатель официального утверждения полностью прекращает производство типа транспортного средства, официально утвержденного на основании настоящих Правил, то он информирует об этом орган, предоставивший официальное утверждение. По получении соответствующего сообщения данный орган информирует о нем другие Договаривающиеся стороны Соглашения, применяющие настоящие Правила, посредством копии карточки официального утверждения, в конце которой крупным шрифтом делают отметку «ПРОИЗВОДСТВО ПРЕКРАЩЕНО» и проставляют подпись и дату.

12. Названия и адреса технических служб, ответственных за проведение испытания для официального утверждения, и органов по официальному утверждению типа

12.1 Стороны Соглашения, применяющие настоящие Правила, сообщают в Секретариат Организации Объединенных Наций названия и адреса технических служб, ответственных за проведение испытания для официального утверждения, а также органов по официальному утверждению типа, которые предоставляют официальное утверждение и которым надлежит направлять выдаваемые в других странах карточки, подтверждающие официальное утверждение, распространение официального утверждения, отказ в официальном утверждении или отзыв официального утверждения.

Приложение 1

Информационный документ

Когда это применимо, должна предоставляться нижеследующая информация в трех экземплярах, включая оглавление. Любые чертежи представляют в соответствующем масштабе, в достаточно подробном виде и в формате A4 или в кратном ему формате. Фотографии, если они имеются, должны быть достаточно четкими.

1. Марка (торговое наименование изготовителя): .....

2. Тип и общее(ие) коммерческое(ие) описание(я): .....

3. Средства идентификации типа, если такая маркировка имеется на транспортном средстве: .....

4. Место нанесения маркировки: .....

5. Категория(и) транспортного средства: .....

6. Фамилия и адрес изготовителя/представителя изготовителя: .....

7. Название(я) и адрес(а) сборочного(ых) предприятия(й): .....

8. Фотография(и) и/или чертеж(и) репрезентативного транспортного средства: .....

9. Кибербезопасность

9.1 Общие характеристики конструкции типа транспортного средства, включая:

a) системы транспортных средств, которые имеют отношение к кибербезопасности данного типа транспортного средства;

b) компоненты тех систем, которые имеют отношение к кибербезопасности;

c) взаимодействие этих систем с другими системами, относящимися к данному типу транспортного средства, и с внешними интерфейсами транспортного средства.

9.2 Схематическое изображение типа транспортного средства

9.3 Номер свидетельства о соответствии СОБиК: .....

9.4 Документы для официального утверждения типа транспортного средства с описанием результатов оценки рисков и выявленных рисков: .....

9.5 Документы для официального утверждения типа транспортного средства с описанием мер по смягчению последствий, которые были осуществлены на перечисленных системах, и того, каким образом они позволяют устранить указанные риски: .....

9.6 Документы для официального утверждения типа транспортного средства с описанием специальных объектов для хранения и реализации программного обеспечения, услуг, приложений или данных в интересах вторичного рынка: .....

9.7 Документы для официального утверждения типа транспортного средства с описанием испытаний, которые были проведены для проверки кибербезопасности данного типа транспортного средства и его систем, и результатов этих испытаний: .....

9.8 Описание факторов, связанных с цепочкой поставок, с точки зрения кибербезопасности: .....

Приложение 1 – Добавление 1

Образец заявления изготовителя о соответствии СОКиБ

Заявление изготовителя о соблюдении требований, предъявляемых к системе обеспечения кибербезопасности

Наименование изготовителя: .....

Адрес изготовителя: .....

..... (*Наименование изготовителя*) подтверждает, что процессы, необходимые для соблюдения требований, касающихся системы обеспечения кибербезопасности, изложенные в пункте 7.2 Правил ООН [15X], налажены и будут поддерживаться.

Совершено в: ..... (*место*)

Дата: .....

Имя подписавшего лица: .....

Функция подписавшего лица: .....

.....

(*Штамп и подпись представителя изготовителя*)

Приложение 2

Сообщение

(Максимальный формат: A4 (210×297 мм))

направленное: Название административного органа:
.....
.....
.....

Касающееся[2]: предоставления официального утверждения
распространения официального утверждения
отзыва официального утверждения начиная с дд/мм/гггг
отказа в официальном утверждении
окончательного прекращения производства

типа транспортного средства на основании Правил № ООН [15X]

Официальное утверждение №: .....

Распространение №: .....

Основание для распространения: .....

1. Марка (торговое наименование изготовителя): .....
2. Тип и общее(ие) коммерческое(ие) описание(я): .....
3. Средства идентификации типа, если такая маркировка имеется на транспортном средстве: .....

3.1 Место нанесения маркировки: .....

4. Категория(и) транспортного средства: .....
5. Фамилия и адрес изготовителя/представителя изготовителя: .....
6. Название(я) и адрес(а) производственного(ых) предприятия(й): .....
7. Номер свидетельства о соответствии системы обеспечения кибербезопасности: .....
8. Техническая служба, ответственная за проведение испытаний: .....
9. Дата протокола испытания: .....
10. Номер протокола испытания: .....
11. Замечания: (при наличии). .....
12. Место: .....
13. Дата: .....
14. Подпись: .....
15. К настоящему прилагается указатель информационной документации, которая была сдана органу по официальному утверждению и которая может быть получена по запросу.

---

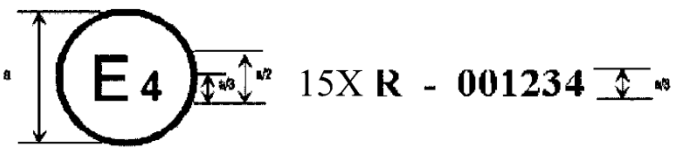
[1] Отличительный номер страны, которая предоставила/распространила официальное утверждение/отказала в официальном утверждении/отозвала официальное утверждение (см. положения настоящих Правил, касающиеся официального утверждения).

[2] Ненужное вычеркнуть.

Приложение 3

Схема знака официального утверждения

Образец A
(См. пункт 4.2 настоящих Правил.)



a = 8 мм мин.

Приведенный выше знак официального утверждения, проставленный на транспортном средстве, указывает, что этот тип транспортного средства был официально утвержден в Нидерландах (E 4) на основании Правил № [15X] и под номером официального утверждения 001234. Первые две цифры номера официального утверждения указывают на то, что официальное утверждение было предоставлено в соответствии с предписаниями настоящих Правил в их первоначальном варианте (00).

Приложение 4

Образец свидетельства о соответствии СОКиБ

Свидетельство о соответствии системы обеспечения кибербезопасности

Правилам ООН № [*настоящим Правилам*]

номер свидетельства [*идентификационный номер*]

[……. *орган по официальному утверждению*]

удостоверяет, что

Изготовитель: .....

Адрес изготовителя: .....

соблюдает положения пункта 7.2 Правил № [15X].

Проверки проведены (дата): .....

(кем) (название и адрес органа по официальному утверждению или технической службы): .....

Номер протокола испытания: .....

Свидетельство действительно до […… *дата*]

Совершено в […… *место*]

[…… *дата*]

[……. *подпись*]

Приложения: описание системы обеспечения кибербезопасности изготовителем.

Приложение 5

Перечень угроз и соответствующих мер по смягчению последствий

1. Настоящее приложение состоит из трех частей. В части A настоящего приложения описываются исходные данные об угрозах, факторах уязвимостях и методах атаки. В части B настоящего приложения описываются меры по смягчению последствий угроз, которые предназначены для типов транспортных средств. В части C описываются меры по смягчению последствий угроз, которые предназначены для зон, расположенных за пределами транспортных средств, например внутренних серверов.

2. Части A, B и C рассматриваются на предмет оценки рисков и мер по смягчению их последствий, которые должны применяться изготовителями транспортных средств.

3. Высокий уровень уязвимости и соответствующие примеры проиндексированы в части A. Та же система индексации используется и в таблицах, содержащихся в частях B и C, с целью увязать каждый случай атаки/фактор уязвимости с перечнем соответствующих мер по смягчению их последствий.

4. Анализ угроз должен также учитывать последствия возможных атак. Это может помочь определить степень риска и выявить дополнительные риски. Возможные последствия атак могут включать следующее:

   a) нарушение безопасной работы транспортного средства;

   b) отказ некоторых функций транспортного средства;

   c) модификацию программного обеспечения, снижение эффективности;

   d) модификацию программного обеспечения, но без последствий для эксплуатации;

   e) нарушение целостности данных;

   f) нарушение конфиденциальности данных;

   g) утрату возможности вывода данных;

   h) прочие последствия, включая преступные действия.

Часть A
Факторы уязвимости или методы атаки, связанные с угрозами

1. Высокоуровневые описания угроз и связанных с ними факторов уязвимости или методов атаки приведены в таблице A1.

Таблица A1
Перечень факторов уязвимости или методов атак, связанных с угрозами

Высокоуровневые и подуровневые описания уязвимости/угрозы			*Пример уязвимости или метода атаки*	
4.3.1 Угрозы в отношении внутренних серверов, связанных с транспортными средствами на местах	1	Внутренние серверы, используемые в качестве средства кибератаки на транспортное средство или извлечения данных	1.1	Злоупотребление привилегиями штатными сотрудниками (**внутренняя атака**)
			1.2	**Несанкционированный доступ через Интернет** к серверу (который возможен, например, в результате обхода системы защиты, не устраненных факторов уязвимости системы программного обеспечения, атаки методом использования языка структурированных запросов SQL или иными способами)

Высокоуровневые и подуровневые описания уязвимости/угрозы			*Пример уязвимости или метода атаки*	
			1.3	**Несанкционированный физический доступ** к серверу (например, с помощью USB-накопителей или иных средств, подключаемых к серверу)
	2	Нарушение работы внутренних серверов, которое отрицательно сказывается на эксплуатации транспортного средства	2.1	**Атака на внутренний сервер, который прекращает работу**: она, например, не дает ему возможности взаимодействовать с транспортными средствами и оказывать услуги, которые нужны для их работы
	3	Относящиеся к транспортному средству данные, хранящиеся на внутренних серверах, утеряны или скомпрометированы («утечка данных»)	3.1	Злоупотребление привилегиями штатными сотрудниками (**внутренняя атака**)
			3.2	**Потеря информации в облаке**. Конфиденциальные данные могут быть потеряны из-за атак или аварий при хранении данных сторонними поставщиками облачных услуг
			3.3	**Несанкционированный доступ через Интернет к серверу** (который возможен, например, в результате обхода системы защиты, не устраненных факторов уязвимости системы программного обеспечения, атаки методом использования языка структурированных запросов SQL или иными способами)
			3.4	**Несанкционированный физический доступ к серверу** (например, с помощью USB-накопителей или иных средств, подключаемых к серверу)
			3.5	**Утечка информации** в результате непреднамеренного обмена данными (например, ошибки на уровне администрации)
4.3.2 Угрозы в отношении транспортных средств, касающиеся их каналов передачи данных	4	Умышленное искажение сообщений или данных, полученных транспортным средством	4.1	**Спуфинг сообщений** в результате атаки путем подмены участника (например, 802.11p V2X в ходе формирования автоколонн, сообщения ГНСС и т. д.)
			4.2	**Атака Сибиллы** (для того, чтобы спуфировать другие транспортные средства, как будто на дороге много транспортных средств)
	5	Каналы передачи данных, используемые для осуществления несанкционированных действий, удаления или внесения других изменений в бортовой код/данные транспортного средства	5.1	Каналы передачи данных допускают **внедрение кода**, например в коммуникационный канал может быть внедрен подложный двоичный код программного обеспечения
			5.2	Каналы передачи данных допускают **манипулирование** бортовым кодом/данными транспортного средства
			5.3	Каналы передачи данных допускают **наложение других данных** на бортовой код/данные транспортного средства
			5.4	Каналы передачи данных допускают **стирание** бортового кода/данных транспортного средства

Высокоуровневые и подуровневые описания уязвимости/угрозы			*Пример уязвимости или метода атаки*	
			5.5	Каналы передачи данных допускают внедрение данных/кода в систему транспортного средства (запись данных/кода)
	6	Каналы передачи данных допускают прием недостоверных/ненадежных сообщений или уязвимы в случае сеансов связи/атаки с повторным навязыванием сообщения	6.1	Прием информации из **ненадежного или недостоверного источника**
			6.2	Атака **через посредника**/перехват сеанса
			6.3	**Атака с повторным навязыванием сообщения**, например атака на коммуникационный шлюз позволяет злоумышленнику снизить эффективность программного обеспечения ЭБУ или встроенных программ шлюза
	7	Информацию можно легко раскрыть. Например, путем подслушивания сообщений или несанкционированного доступа к конфиденциальным файлам или папкам	7.1	**Перехват информации**/помехи в результате излучения/отслеживание сообщений
			7.2	Получение **несанкционированного доступа** к файлам или данным
	8	Атаки по каналам передачи данных в целях нарушения функций транспортного средства в виде отказа в обслуживании	8.1	**Отправка** большого количества ненужных **данных** в информационную систему транспортного средства, **чтобы она не могла предоставлять услуги** в обычном режиме
			8.2	**Атака методом переполнения**: с целью нарушить передачу данных между транспортными средствами злоумышленник может заблокировать передачу сообщений между транспортными средствами
	9	Пользователь со стороны может получить привилегированный доступ к системам транспортного средства	9.1	Пользователь со стороны может **получить привилегированный доступ**, например доступ с полномочиями суперпользователя
	10	Вирусы, занесенные в коммуникационную среду, могут инфицировать системы транспортного средства	10.1	**Вирус**, занесенный в коммуникационную среду, инфицирует системы транспортного средства
	11	Сообщения, полученные транспортным средством (например, X2V или диагностические сигналы) или переданные вместе с ним, содержат вредоносный контент	11.1	Вредоносные **внутренние** (например, местная контроллерная сеть – CAN) **сообщения**
			11.2	Вредоносные **сообщения V2X**, например сообщения «объект инфраструктуры – транспортное средство» или «транспортное средство – транспортное средство» (например, CAM, DENM)
			11.3	Вредоносные диагностические сигналы
			11.4	Вредоносные **частные сообщения** (например, те, которые обычно направляются OEM или поставщиком компонента/системы/функции)

Высокоуровневые и подуровневые описания уязвимости/угрозы			*Пример уязвимости или метода атаки*	
4.3.3. Угрозы в отношении транспортных средств, касающиеся их процедур обновления	12	Злоупотребление процедурами обновления или их нарушение	12.1	Нарушение **процедур обновления программного обеспечения по каналу беспроводной связи**. Это включает подделку программы обновления системы или встроенных программ
			12.2	Нарушение **процедур обновления локального/физического программного обеспечения**. Это включает подделку программы обновления системы или встроенных программ
			12.3	**Манипулирование программным обеспечением до процесса обновления** (и, как следствие, его нарушение), хотя сам процесс обновления не нарушается
			12.4	**Нарушение** криптографических ключей провайдера программного обеспечения **с целью допустить неполноценное обновление**
	13	Возможность отказа в правомерных обновлениях	13.1	Атака в виде отказа в обслуживании сервера или сети с целью **воспрепятствовать обновлениям важнейшего программного обеспечения** и/или разблокировки конкретных функций пользователя
4.3.4 Угрозы транспортным средствам в связи с непреднамеренным и действиями человека, способствующими кибератаке	15	Правомерные субъекты способны принимать меры, которые могут невольно облегчить кибератаку	15.1	Невинная жертва (например, владелец, оператор или инженер по техническому обслуживанию) **путем обмана предпринимает действия** с целью непреднамеренной загрузки вредоносного ПО или проведения атаки
			15.2	**Заданные процедуры обеспечения** безопасности не соблюдаются
4.3.5 Угрозы транспортным средствам в отношении их внешних подключений и соединений	16	Манипулирование функциями подключения транспортного средства позволяет осуществить кибератаку: это может включать средства телематики; системы, которые дают возможность осуществления дистанционных операций; и системы, использующие средства беспроводной связи ближнего радиуса действия	16.1	Манипулирование **функциями, предназначенными для дистанционного управления системами**, такими как дистанционный ключ, иммобилизатор и уличная зарядка
			16.2	**Манипулирование средствами телематики транспортного средства** (например, измерением температуры грузов, требующих особого обращения, дистанционным открытием дверей грузового отделения)
			16.3	Помехи в работе **систем беспроводной связи ближнего радиуса действия** или датчиков
	17	Размещение программного обеспечения третьей стороной, например развлекательных прикладных программ, используемых в качестве одного из средств для атаки систем транспортных средств	17.1	**Поврежденные приложения** или приложения со слабой программной защитой, используемые в качестве метода атаки на системы транспортных средств

Высокоуровневые и подуровневые описания уязвимости/угрозы			*Пример уязвимости или метода атаки*	
	18	Устройства, подключенные к внешним интерфейсам, например USB-порты, БД-порт, используемые в качестве средства атаки на системы транспортных средств	18.1	**Внешние интерфейсы**, такие как USB или другие порты, используемые в качестве точки атаки, например путем внедрения кода.
			18.2	Программные средства инфицированы **вирусом**, занесенным в систему транспортного средства
			18.3	**Точки диагностического контроля (например, программные ключи, вставляемые в БД-порт)**, которые используются для облегчения атаки, например для манипулирования параметрами транспортного средства (напрямую или опосредованно)
4.3.6 Угрозы данным/коду транспортного средства	19	Извлечение данных/кода транспортного средства	19.1	Извлечение патентованного или собственного программного обеспечения из систем транспортного средства (**фальсификация** продукта)
			19.2	Несанкционированный доступ к такой **персональной информации владельца**, как удостоверение личности, платежные реквизиты, адресная книга, информации о местоположении, электронная идентификация транспортного средства и т. д.
			19.3	Извлечение криптографических ключей
	20	Манипулирование данными/ кодом транспортных средств	20.1	Противоправные/несанкционированные изменения в **электронной идентификации транспортного средства**
			20.2	**Мошенничество с использованием персональных данных**. Например, если пользователь желает выдать себя за другое лицо при установлении связи с системами взимания автодорожных сборов или серверным приложением изготовителя
			20.3	Действия с целью **обхода систем мониторинга** (например, взлом/подделка/блокирование таких сообщений, как данные системы регистрации ODR или количество рейсов)
			20.4	Манипулирование данными в целях **фальсификации данных об управлении транспортным средством** (например, данных о пробеге, скорости, направлении движения и т. д.)
			20.5	Несанкционированные изменения **данных системы диагностики**
	21	Стирание данных/кода	21.1	Несанкционированное удаление **журналов регистрации системных событий**/ манипулирование **журналами регистрации системных событий**
	22	Внедрение вредоносных программ	22.2	Внедрение **вредоносного программного обеспечения** или создание условий для злонамеренной работы вредоносных программ

Высокоуровневые и подуровневые описания уязвимости/угрозы			*Пример уязвимости или метода атаки*	
	23	Введение в действие нового программного обеспечения или затирание существующего программного обеспечения	23.1	**Фабрикация программного обеспечения** системы контроля или информационный системы транспортного средства
	24	Нарушение работы систем или операций	24.1	**Отказ в обслуживании**: это, например, может быть инициировано во внутренней сети путем лавинного распространения данных по шине сети локальных контроллеров CAN или посредством провоцирования сбоев в ЭБУ вследствие большого количества сообщений
	25	Манипулирование параметрами транспортного средства	25.1	Несанкционированный доступ в целях **фальсификации параметров конфигурации** основных функций транспортного средства, таких как данные о тормозах, пороговом уровне срабатывания подушки безопасности и т. д.
			25.2	Несанкционированный доступ в целях **фальсификации параметров зарядки**, таких как напряжение зарядки, расход энергии на подзарядку, температура батареи и т. д.
4.3.7 Потенциальные факторы уязвимости, которыми можно воспользоваться в случае недостаточной защиты или надежности	26	Криптографические технологии, которые могут быть нарушены или которые применяются недостаточно	26.1	Сочетание коротких **ключей шифрования данных** и длительных сроков их действия дает взломщикам возможность сломать шифровальный код
			26.2	Недостаточное использование шифровальных алгоритмов для защиты чувствительных систем
			26.3	Использование **криптографических алгоритмов**, которые уже устарели или устареют в скором времени
	27	Части или принадлежности компонентов, которые могут быть нарушены в целях создания возможности для атаки транспортных средств	27.1	**Аппаратное или программное обеспечение, разработанное таким образом, что оно создает возможность для атаки** или не удовлетворяет конструктивным критериям для прекращения атаки
	28	Разработка программного обеспечения или аппаратных средств, которая создает возможность возникновения факторов уязвимости	28.1	**Ошибки в программном обеспечении**. Наличие ошибок в программном обеспечении может явиться причиной возникновения потенциальных факторов уязвимости, которыми можно воспользоваться. Это особенно верно в том случае, если программное обеспечение не было протестировано с целью убедиться в том, что известного неудовлетворительного кода/ошибок нет, и снизить риск наличия неизвестного неудовлетворительного кода/ошибок

Высокоуровневые и подуровневые описания уязвимости/угрозы			*Пример уязвимости или метода атаки*	
			28.2	**Использование остаточных устройств и материалов** после разработки (например, отладочных портов, портов JTAG, микропроцессоров, сертификатов разработки, паролей разработчиков и т. д.) может обеспечить доступ к ЭБУ или дать возможность взломщикам получить более высокий статус привилегий
	29	Дизайн сети, который допускает возникновение факторов уязвимости	29.1	**Лишние интернет-порты оставлены открытыми**, что обеспечивает доступ к сетевым системам
			29.2	Обход **разделения сети** для получения контроля. Конкретным примером является использование незащищенных шлюзов или точек доступа (например, шлюзы «грузовой автомобиль – прицеп») для обхода защиты и получения доступа к другим сегментам сети, что позволяет производить злоумышленные действия, такие как передача произвольных сообщений на шину сети локальных контроллеров (CAN)
	31	Может произойти непреднамеренная передача данных	31.1	Утечка информации. В случае **смены пользователя автомобиля** может произойти утечка персональных данных (например, если автомобиль продан или используется напрокат другими лицами)
	32	Физическое манипулирование системами, которое может создать возможность для атаки	32.1	**Манипулирование электронной аппаратурой**, например установка на транспортное средство несанкционированной электронной аппаратуры, что создает возможность для проведения атаки через посредника **Замена санкционированной электронной аппаратуры** (например, датчиков) несанкционированной электронной аппаратурой **Манипулирование информацией**, собираемой датчиком (например, использование магнита для вмешательства в работу датчика, основанного на эффекте Холла и подключенного к коробке передач)

Часть B
Меры по смягчению последствий угроз, предназначенные для транспортных средств

1. Меры по смягчению последствий в случае «Каналов передачи данных транспортных средств»

Меры по смягчению последствий угроз, которые связаны с «Каналами передачи данных транспортных средств», перечислены в таблице B1.

Таблица B1
Смягчение последствий угроз, которые связаны с «Каналами передачи данных транспортных средств»

Ссылка на таблицу A1	*Угрозы, связанные с «Каналами передачи данных транспортных средств»*	*Ссылка*	*Смягчение последствий*
4.1	Спуфинг сообщений (например, 802.11p V2X в ходе формирования автоколонн, сообщения ГНСС и т. д.) в результате атаки путем подмены участника	M10	Транспортное средство проверяет подлинность и целостность сообщений, которые оно получает
4.2	Атака Сибиллы (для того, чтобы спуфировать другие транспортные средства, как будто на дороге много транспортных средств)	M11	В целях хранения криптографических ключей обеспечиваются соответствующие средства контроля защиты (например, использование аппаратных модулей безопасности)
5.1	Каналы передачи данных допускают внедрение кода/данных: например, в коммуникационный канал может быть внедрен подложный двоичный код программного обеспечения	M10 M6	Транспортное средство проверяет подлинность и целостность сообщений, которые оно получает В целях сведения рисков к минимуму защита систем обеспечивается ее конструкцией
5.2	Каналы передачи данных допускают манипулирование бортовым кодом/ данными транспортного средства	M7	В целях защиты данных/кода системы применяют соответствующие методы контроля за доступом и соответствующие конструктивные особенности
5.3	Каналы передачи данных допускают наложение других данных на бортовой код/данные транспортного средства		
5.4 21.1	Каналы передачи данных допускают стирание бортового кода/данных транспортного средства		
5.5	Каналы передачи данных допускают внедрение данных/кода в систему транспортного средства (запись данных/кода)		
6.1	Прием информации из ненадежного или недостоверного источника	M10	Транспортное средство проверяет подлинность и целостность сообщений, которые оно получает

Ссылка на таблицу A1	*Угрозы, связанные с «Каналами передачи данных транспортных средств»*	*Ссылка*	*Смягчение последствий*
6.2	Атака через посредника/перехват сеанса	M10	Транспортное средство проверяет подлинность и целостность сообщений, которые оно получает
6.3	Атака с повторным навязыванием сообщения, например атака на коммуникационный шлюз позволяет злоумышленнику снизить эффективность программного обеспечения ЭБУ или встроенных программ шлюза		
7.1	Перехват информации/помехи в результате излучения/отслеживание сообщений	M12	Конфиденциальные данные, передаваемые на транспортное средство или транспортным средством, подлежат соответствующей защите
7.2	Получение несанкционированного доступа к файлам или данным	M8	Заблокировать доступ неуполномоченному персоналу к персональным данным или важнейшим системным данным можно с помощью соответствующей конструкции системы и контроля за доступом. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)
8.1	Отправка большого количества ненужных данных в информационную систему транспортного средства, чтобы она не могла предоставлять услуги в обычном режиме	M13	Принимают меры по выявлению атаки на функцию отказа в обслуживании и по восстановлению системы
8.2	Атака методом переполнения, нарушение связи между транспортными средствами в результате блокировки передачи сообщений между транспортными средствами	M13	Принимают меры по выявлению атаки на функцию отказа в обслуживании и по восстановлению системы
9.1	Пользователь со стороны может получить привилегированный доступ, например доступ с полномочиями суперпользователя	M9	Применяют меры по предупреждению и выявлению случаев несанкционированного доступа
10.1	Вирус, занесенный в коммуникационную среду, инфицирует системы транспортного средства	M14	Меры по защите от внедренных вирусов/вредоносных программ подлежат рассмотрению
11.1	Вредоносные внутренние (например, местная контроллерная сеть – CAN) сообщения	M15	Меры по выявлению злонамеренных внутренних сообщений или деятельности подлежат рассмотрению

Ссылка на таблицу A1	*Угрозы, связанные с «Каналами передачи данных транспортных средств»*	*Ссылка*	*Смягчение последствий*
11.2	Вредоносные сообщения V2X, например сообщения «объект инфраструктуры-транспортное средство» или «транспортное средство-транспортное средство» (например, CAM, DENM)	M10	Транспортное средство проверяет подлинность и целостность сообщений, которые оно получает
11.3	Вредоносные диагностические сигналы		
11.4	Вредоносные частные сообщения (например, те, которые обычно направляются OEM или поставщиком компонента/системы/функции)		

2. Меры по смягчению последствий в случае «Процесса обновления»

Меры по смягчению последствий угроз, которые связаны с «Процессом обновления», перечислены в таблице B2.

Таблица B2
Меры по смягчению последствий угроз, которые связаны с «Процессом обновления»

Ссылка на таблицу A1	*Угрозы, связанные с «Процессом обновления»*	*Ссылка*	*Смягчение последствий*
12.1	Нарушение процедур обновления программного обеспечения по каналу беспроводной связи. Это включает подделку программы обновления системы или встроенных программ	M16	Применяют безопасные процедуры обновления программного обеспечения
12.2	Нарушение процедур обновления локального/физического программного обеспечения. Это включает подделку программы обновления системы или встроенных программ		
12.3	Манипулирование программным обеспечением до процесса обновления (и, как следствие, его нарушение), хотя сам процесс обновления не нарушается		
12.4	Нарушение криптографических ключей провайдера программного обеспечения с целью допустить неполноценное обновление	M11	В целях хранения криптографических ключей обеспечиваются соответствующие средства контроля защиты
13.1	Атака в виде отказа в обслуживании сервера или сети с целью воспрепятствовать обновлению важнейшего программного обеспечения и/или разблокировки конкретных функций пользователя	M3	Средства контроля защиты применяют к внутренним системам. Там, где внутренние серверы имеют исключительно важное значение для обеспечения обслуживания, можно использовать в случае сбоев в работе системы соответствующие меры по восстановлению. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)

3. Меры по смягчению последствий в случае «Непреднамеренных действий человека, способствующих кибератаке»

Меры по смягчению последствий угроз, которые связаны с «Непреднамеренными действиями человека, способствующими кибератаке», перечислены в таблице B3.

Таблица B3
Меры по смягчению последствий угроз, которые связаны с «Непреднамеренными действиями человека, способствующими кибератаке»

Ссылка на таблицу A1	*Угрозы, связанные с «Непреднамеренными действиями человека»*	*Ссылка*	*Смягчение последствий*
15.1	Невинная жертва (например, владелец, оператор или инженер по техническому обслуживанию) путем обмана предпринимает действия с целью непреднамеренной загрузки вредоносного ПО или проведения атаки	M18	В целях определения и проверки ролей пользователей и привилегий доступа, основанных на принципе наименьшей привилегии доступа, принимают соответствующие меры
15.2	Заданные процедуры обеспечения безопасности не соблюдаются	M19	Организации обеспечивают определение и соблюдение процедур безопасности, включая регистрацию действий и доступа, связанных с управлением функциями безопасности

4. Меры по смягчению последствий в случае «Внешних подключений и соединений»

Меры по смягчению последствий угроз, которые связаны с «Внешними подключениями и соединениями», перечислены в таблице B4.

Таблица B4
Меры по смягчению последствий угроз, которые связаны с «Внешними подключениями и соединениями»

Ссылка на таблицу A1	*Угрозы, связанные с «Внешними подключениями и соединениями»*	*Ссылка*	*Смягчение последствий*
16.1	Манипулирование функциями, предназначенными для дистанционного управления такими системами, как дистанционный ключ, иммобилизатор и уличная зарядка	M20	В случае систем, оснащенных функцией дистанционного доступа, применяют соответствующие средства контроля защиты
16.2	Манипулирование средствами телематики транспортного средства (например, измерением температуры грузов, требующих особого обращения, дистанционным открытием дверей грузового отделения)		
16.3	Помехи в работе систем беспроводной связи ближнего радиуса действия или датчиков		

Ссылка на таблицу A1	*Угрозы, связанные с «Внешними подключениями и соединениями»*	*Ссылка*	*Смягчение последствий*
17.1	Поврежденные приложения или приложения со слабой программной защитой, используемые в качестве метода атаки на системы транспортных средств	M21	Программное обеспечение оценивают с точки зрения безопасности, удостоверяют его подлинность и обеспечивают защиту его целостности Для сведения к минимуму риска, связанного с использованием программного обеспечения третьей стороны, которое предназначено для размещения на транспортном средстве, применяют средства контроля защиты
18.1	Внешние интерфейсы, такие как USB или другие порты, используемые в качестве точки атаки, например путем внедрения кода	M22	К внешним интерфейсам применяют соответствующие средства контроля защиты
18.2	Программные средства инфицированы вирусами, занесенными в транспортное средство		
18.3	Точки диагностического контроля (например, программные ключи, вставляемые в БД-порт), которые используются для облегчения атаки, например для манипулирования параметрами транспортного средства (напрямую или опосредованно)	M22	К внешним интерфейсам применяют соответствующие средства контроля защиты

5. Меры по смягчению последствий в случае «Потенциальных целей или мотивировки атаки»

Меры по смягчению последствий угроз, которые связаны с «Потенциальными целями или мотивировкой атаки», перечислены в таблице B5.

Таблица B5
Меры по смягчению последствий угроз, которые связаны с «Потенциальными целями или мотивировкой атаки»

Ссылка на таблицу A1	*Угрозы, связанные с «Потенциальными целями или мотивировкой атаки»*	*Ссылка*	*Смягчение последствий*
19.1	Извлечение патентованного или собственного программного обеспечения из систем транспортного средства (фальсификация продукта/хищение программного обеспечения)	M7	В целях защиты данных/кода системы применяют соответствующие методы контроля за доступом и соответствующие конструктивные особенности. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)
19.2	Несанкционированный доступ к такой персональной информации владельца, как удостоверение личности, платежные реквизиты, адресная книга, информации о местоположении, электронная идентификация транспортного средства и т. д.	M8	Заблокировать доступ неуполномоченному персоналу к персональным данным или важнейшим системным данным можно с помощью соответствующей конструкции системы и контроля за доступом. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)

Ссылка на таблицу A1	*Угрозы, связанные с «Потенциальными целями или мотивировкой атаки»*	*Ссылка*	*Смягчение последствий*
19.3	Извлечение криптографических ключей	M11	В целях хранения криптографических ключей обеспечиваются соответствующие средства контроля защиты, например модули безопасности
20.1	Противоправные/несанкционированные изменения в электронной идентификации транспортного средства	M7	В целях защиты данных/кода системы применяют соответствующие методы контроля за доступом и соответствующие конструктивные особенности. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)
20.2	Мошенничество с использованием персональных данных. Например, если пользователь желает выдать себя за другое лицо при установлении связи с системами взимания автодорожных сборов или серверным приложением изготовителя		
20.3	Действия с целью обхода систем мониторинга (например, взлом/ подделка/ блокирование таких сообщений, как данные системы регистрации ODR или количество рейсов)	M7	В целях защиты данных/кода системы применяют соответствующие методы контроля за доступом и соответствующие конструктивные особенности. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP). Атаки на датчики с целью манипулирования данными или последствия для передаваемых данных можно смягчить путем сопоставления данных, полученных из различных источников информации
20.4	Манипулирование данными в целях фальсификации данных об управлении транспортным средством (например, данных о пробеге, скорости, направлении движения и т. д.)		
20.5	Несанкционированные изменения данных системы диагностики		
21.1	Несанкционированное удаление журналов регистрации системных событий/манипулирование журналами регистрации системных событий	M7	В целях защиты данных/кода системы применяют соответствующие методы контроля за доступом и соответствующие конструктивные особенности. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)
22.2	Внедрение вредоносного программного обеспечения или создание условий для злонамеренной работы вредоносных программ	M7	В целях защиты данных/кода системы применяют соответствующие методы контроля за доступом и соответствующие конструктивные особенности. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)
23.1	Фабрикация программного обеспечения системы контроля или информационный системы транспортного средства		
24.1	Отказ в обслуживании: это, например, может быть инициировано во внутренней сети путем лавинного распространения данных по шине сети локальных контроллеров CAN или посредством провоцирования сбоев в ЭБУ вследствие большого количества сообщений	M13	Принимают меры по выявлению атаки на функцию отказа в обслуживании и по восстановлению системы

Ссылка на таблицу A1	*Угрозы, связанные с «Потенциальными целями или мотивировкой атаки»*	*Ссылка*	*Смягчение последствий*
25.1	Несанкционированный доступ в целях фальсификации параметров конфигурации основных функций транспортного средства, таких как данные о тормозах, пороговом уровне срабатывания подушки безопасности и т. д.	M7	В целях защиты данных/кода системы применяют соответствующие методы контроля за доступом и соответствующие конструктивные особенности. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)
25.2	Несанкционированный доступ в целях фальсификации параметров зарядки, таких как напряжение зарядки, расход энергии на подзарядку, температура батареи и т. д.		

6. Меры по смягчению последствий в случае «Потенциальных факторов уязвимости, которыми можно воспользоваться в случае недостаточной защиты или надежности»

Меры по смягчению последствий угроз, которые связаны с «Потенциальными факторами уязвимости, которыми можно воспользоваться в случае недостаточной защиты или надежности», перечислены в таблице B6.

Таблица B6

Меры по смягчению последствий угроз, которые связаны с «Потенциальными факторами уязвимости, которыми можно воспользоваться в случае недостаточной защиты или надежности»

Ссылка на таблицу A1	*Угрозы, связанные с «Потенциальными факторами уязвимости, которыми можно воспользоваться в случае недостаточной защиты или надежности»*	*Ссылка*	*Смягчение последствий*
26.1	Сочетание коротких ключей шифрования данных и длительных сроков их действия дает взломщикам возможность сломать шифровальный код	M23	В процессе разработки программного обеспечения и аппаратных средств соблюдают современные виды практики в области кибербезопасности
26.2	Недостаточное использование шифровальных алгоритмов для защиты чувствительных систем		
26.3	Использование устаревших криптографических алгоритмов		
27.1	Аппаратное или программное обеспечение, разработанное таким образом, что оно создает возможность для атаки или не удовлетворяет конструктивным критериям для прекращения атаки	M23	В процессе разработки программного обеспечения и аппаратных средств соблюдают современные виды практики в области кибербезопасности

Ссылка на таблицу A1	*Угрозы, связанные с «Потенциальными факторами уязвимости, которыми можно воспользоваться в случае недостаточной защиты или надежности»*	*Ссылка*	*Смягчение последствий*
28.1	Наличие ошибок в программном обеспечении может явиться причиной возникновения потенциальных факторов уязвимости, которыми можно воспользоваться. Это особенно верно в том случае, если программное обеспечение не было протестировано с целью убедиться в том, что известного неудовлетворительного кода/ошибок нет, и снизить риск наличия неизвестного неудовлетворительного кода/ошибок	M23	В процессе разработки программного обеспечения и аппаратных средств соблюдают современные виды практики в области кибербезопасности. Тестирование кибербезопасности с достаточным покрытием
28.2	Использование остаточных устройств и материалов после разработки (например, отладочных портов, портов JTAG, микропроцессоров, сертификатов разработки, паролей разработчиков и т. д.) может обеспечить взломщику доступ к ЭБУ или дать ему возможность получить более высокий статус привилегий		
29.1	Лишние интернет-порты оставлены открытыми, что обеспечивает доступ к сетевым системам		
29.2	Обход разделения сети для получения контроля. Конкретным примером является использование незащищенных шлюзов или точек доступа (например, шлюзы «грузовой автомобиль – прицеп») для обхода защиты и получения доступа к другим сегментам сети, что позволяет производить злоумышленные действия, такие как передача произвольных сообщений на шину сети локальных контроллеров (CAN)	M23	В процессе разработки программного обеспечения и аппаратных средств соблюдают современные виды практики в области кибербезопасности. В процессе проектирования системы и системной интеграции соблюдают современные виды практики в области кибербезопасности

7. Меры по смягчению последствий в случае «Потери данных/утечки данных из транспортного средства»

Смягчение последствий угроз, которые связаны с «Потерей данных/утечкой данных из транспортного средства», перечислены в таблице B7.

Таблица B7

Смягчение последствий угроз, которые связаны с «Потерей данных/утечкой данных из транспортного средства»

Ссылка на таблицу A1	*Угрозы, связанные с «Потерями данных/утечкой данных из транспортного средства»*	*Ссылка*	*Смягчение последствий*
31.1	Утечка информации. В случае смены пользователя автомобиля может произойти утечка персональных данных (например, если автомобиль продан или используется напрокат другими лицами)	M24	При хранении персональных данных необходимо следовать передовым методам защиты целостности и конфиденциальности данных

8. Меры по смягчению последствий в случае «Физического манипулирования системами, которое может создать возможность для атаки»

Меры по смягчению последствий угроз, связанных с «Физическим манипулированием системами, которое может создать возможность для атаки», перечислены в таблице B8.

Таблица B8
Меры по смягчению последствий угроз, связанных с «Физическим манипулированием системами, которое может создать возможность для атаки»

Ссылка на таблицу A1	*Угрозы, связанные с «Физическим манипулированием системами, которое может создать возможность для атаки»*	*Ссылка*	*Смягчение последствий*
32.1	Манипулирование электронной аппаратурой, например установка на транспортное средство несанкционированной электронной аппаратуры, что создает возможность для проведения атаки через посредника	M9	Применяют меры по предупреждению и выявлению случаев несанкционированного доступа

Часть C
Меры по смягчению последствий угроз за пределами транспортных средств

1. Меры по смягчению последствий в случае «Внутренних серверов»

Меры по смягчению последствий угроз, которые связаны с «Внутренними серверами», перечислены в таблице C1.

Таблица C1
Меры по смягчению последствий угроз, которые связаны с «Внутренними серверами»

Ссылка на таблицу A1	*Угрозы, связанные с «Внутренними серверами»*	*Ссылка*	*Смягчение последствий*
1.1 и 3.1	Злоупотребление привилегиями штатными сотрудниками (внутренняя атака)	M1	Средства контроля защиты применяют к внутренним системам в целях сведения к минимуму риска угрозы со стороны штатных сотрудников
1.2 и 3.3	Несанкционированный доступ через Интернет к серверу (который возможен, например, в результате обхода системы защиты, не устраненных факторов уязвимости системы программного обеспечения, атаки методом использования языка структурированных запросов SQL или иными способами)	M2	Средства контроля защиты применяют к внутренним системам в целях сведения к минимуму несанкционированного доступа. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)
1.3 и 3.4	Несанкционированный физический доступ к серверу (например, с помощью USB-накопителей или иных средств, подключаемых к серверу)	M8	Заблокировать доступ неуполномоченному персоналу к персональным данным или важнейшим системным данным можно с помощью соответствующей конструкции системы и контроля за доступом

Ссылка на таблицу A1	*Угрозы, связанные с «Внутренними серверами»*	*Ссылка*	*Смягчение последствий*
2.1	Атака на внутренний сервер, который прекращает работу: она, например, не дает ему возможности взаимодействовать с транспортными средствами и оказывать услуги, которые нужны для их работы	M3	Средства контроля защиты применяют к внутренним системам. Там, где внутренние серверы имеют исключительно важное значение для обеспечения обслуживания, можно использовать в случае сбоев в работе системы соответствующие меры по восстановлению. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)
3.2	Потеря информации в облаке. Конфиденциальные данные могут быть потеряны из-за атак или аварий при хранении данных сторонними поставщиками облачных услуг	M4	Средства контроля защиты применяют к внутренним системам в целях сведения к минимуму рисков, связанных с облачной обработкой данных. Примеры средств контроля защиты можно найти в проекте OWASP и в руководстве по облачной обработке данных NCSC.
3.5	Утечка информации в результате непреднамеренного обмена данными (например, ошибки на уровне администрации, хранение данных на серверах в гаражах)	M5	Средства контроля защиты применяют к внутренним системам в целях предотвращения утечек данных. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)

2. Меры по смягчению последствий в случае «Непреднамеренных действий человека»

Меры по смягчению последствий угроз, которые связаны с «Непреднамеренными действиями человека», перечислены в таблице C2.

Таблица C2

Меры по смягчению последствий угроз, которые связаны с «Непреднамеренными действиями человека»

Ссылка на таблицу A1	*Угрозы, связанные с «Непреднамеренными действиями человека»*	*Ссылка*	*Смягчение последствий*
15.1	Невинная жертва (например, владелец, оператор или инженер по техническому обслуживанию) путем обмана предпринимает действия с целью непреднамеренной загрузки вредоносного ПО или проведения атаки	M18	В целях определения и проверки ролей пользователей и привилегий доступа, основанных на принципе наименьшей привилегии доступа, принимают соответствующие меры
15.2	Заданные процедуры обеспечения безопасности не соблюдаются	M19	Организации обеспечивают определение и соблюдение процедур безопасности, включая регистрацию действий и доступа, связанных с управлением функциями безопасности

3. Меры по смягчению последствий в случае «Физической потери данных»

Меры по смягчению последствий угроз, которые связаны с «Физической потерей данных», перечислены в таблице С3.

Таблица С3

Меры по смягчению последствий угроз, которые связаны с «Физической потерей данных»

Ссылка на таблицу А1	*Угрозы, связанные с «Физической потерей данных»*	*Ссылка*	*Смягчение последствий*
30.1	Ущерб, причиненный третьей стороной. В случае дорожно-транспортного происшествия или кражи конфиденциальные данные могут быть утеряны или скомпрометированы в результате физических повреждений.	M24	При хранении персональных данных необходимо следовать передовым методам защиты целостности и конфиденциальности данных. Примеры средств контроля защиты можно найти в ISO/SC27/WG5
30.2	Утрата в результате коллизий на уровне УЦР (управление цифровыми правами). Данные пользователя могут быть удалены в случае проблем с УЦП		
30.3	Целостность конфиденциальных данных или сами данные могут быть утеряны в случае морального и физического износа компонентов, что вызовет потенциальный каскадный эффект (например, в случае изменения ключа)		

*DRAFT REGULATION NO. [155]**

Receipt by the Secretary-General of the United Nations: 3 July 2020

**No UNTS volume number has yet been determined for this record.*

*ENTRY INTO FORCE OF UNITED NATIONS REGULATION NO. 155**

Notification effected on the Secretary-General of the United Nations: 22 January 2021

**No UNTS volume number has yet been determined for this record.*

*AMENDMENTS TO UNITED NATIONS REGULATION NO. 155**

Notification effected on the Secretary-General of the United Nations: 8 October 2022

**No UNTS volume number has yet been determined for this record.*

*APPLICATION OF REGULATION**

Uganda

Notification effected on the Secretary-General of the United Nations: 23 August 2022

**No UNTS volume number has yet been determined for this record.*

PROJET DE RÈGLEMENT N° [155]

Réception par le Secrétaire général de l'Organisation des Nations Unies : 3 juillet 2020

**Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

ENTRÉE EN VIGUEUR DU RÈGLEMENT DE L'ONU N° 155

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

**Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

AMENDEMENTS AU RÈGLEMENT DE L'ONU N° 155

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 8 octobre 2022

**Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION DU RÈGLEMENT

Ouganda

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 23 août 2022

**Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Albania

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Albanie

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Armenia

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Arménie

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Australia

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Australie

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Austria

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Autriche

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Azerbaijan

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Azerbaïdjan

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Belarus

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Bélarus

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Belgium

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Belgique

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Bosnia and Herzegovina

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Bosnie-Herzégovine

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Bulgaria

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Bulgarie

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Croatia

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Croatie

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Czech Republic

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

République tchèque

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Denmark

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Danemark

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Egypt

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Égypte

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Estonia

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Estonie

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

European Union

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Union européenne

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Finland

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Finlande

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

France

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

France

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Georgia

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Géorgie

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Germany

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Allemagne

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Greece

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Grèce

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Hungary

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Hongrie

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Italy

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Italie

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Japan

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Japon

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Kazakhstan

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Kazakhstan

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Latvia

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Lettonie

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Lithuania

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Lituanie

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Luxembourg

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Luxembourg

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Malaysia

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Malaisie

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Montenegro

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Monténégro

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Netherlands

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Pays-Bas

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

New Zealand

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Nouvelle-Zélande

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Nigeria

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Nigéria

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

North Macedonia

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Macédoine du Nord

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Norway

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Norvège

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Pakistan

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Pakistan

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Poland

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Pologne

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Portugal

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Portugal

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Republic of Korea

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

République de Corée

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Republic of Moldova

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

République de Moldova

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Romania

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Roumanie

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Russian Federation

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Fédération de Russie

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

San Marino

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Saint-Marin

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Serbia

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Serbie

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Slovakia

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Slovaquie

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Slovenia

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Slovénie

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

South Africa

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Afrique du Sud

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Spain

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Espagne

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Sweden

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Suède

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Switzerland

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Suisse

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Thailand

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Thaïlande

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Tunisia

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Tunisie

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Turkey

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Turquie

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Ukraine

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Ukraine

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

United Kingdom of Great Britain and Northern Ireland

Notification effected on the Secretary-General of the United Nations: 22 January 2021

Date of effect: 22 January 2021

Registration with the Secretariat of the United Nations: ex officio, 22 January 2021

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Royaume-Uni de Grande-Bretagne et d'Irlande du Nord

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 22 janvier 2021

Date de prise d'effet : 22 janvier 2021

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 22 janvier 2021

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*

APPLICATION OF REGULATION[*]

Philippines

Notification effected on the Secretary-General of the United Nations: 3 November 2022

Date of effect: 2 January 2023

Registration with the Secretariat of the United Nations: ex officio, 3 November 2022

[*]*No UNTS volume number has yet been determined for this record.*

APPLICATION DU RÈGLEMENT

Philippines

Notification effectuée le Secrétaire général de l'Organisation des Nations Unies : 3 novembre 2022

Date de prise d'effet : 2 janvier 2023

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : d'office, 3 novembre 2022

[*]*Le numéro de volume RTNU n'a pas encore été établie pour ce dossier.*