United Nations ECE/TRANS/WP.29/GRVA/2020/3

Economic and Social Council

Distr.: General
2 December 2019

Original: English

Economic Commission for Europe

Inland Transport Committee

World Forum for Harmonization of Vehicle Regulations

Working Party on Automated/Autonomous and Connected Vehicles*

Fifth session
Geneva, 10-14 February 2020
Item 5 (a) of the provisional agenda
Connected vehicles:
Cyber security and date protection as well as software updates

Proposal for the 01 series of amendments to the new UN Regulation on uniform provisions concerning the approval of vehicles with regard to cyber security and of cybersecurity management systems

Submitted by the Task Force on Cyber Security and Over- the-Air issues **

This proposal was prepared by the experts of the Task Force on Cyber Security and Over-The-Air Software issues in response to the mandate agreed by the World Forum for Harmonization of Vehicle Regulations (WP.29) as reflected in ECE/TRANS/WP29/1126, para. 28 and ECE/TRANS/WP29/1131, para. 27. It is proposing provisions for the approval of cybersecurity management systems as well as of vehicles with regard to cyber security.

The document contains provisions that are in square brackets.

* Formerly: **Working Party on Brakes and Running Gear (GRRF)**.

** 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.

I. Proposal

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

Contents

1. Scope

1.1. This Regulation applies to vehicles, with regard to cyber security, of the categories M, N, O [and, R, S and T].

1.2. This regulation also applies to vehicles of Categories L_6 and L_7 if equipped with automated driving functionalities

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.

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 after which a vehicle type is no longer produced. 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 definitely 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 definitely 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.

5.2. 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.

5.4. 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. Existing vehicle type approvals shall not lose their validity due to the expiration of the manufacturer's Certificate of Compliance for CSMS.

7. Specifications

7.1. General specifications

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

7.1.2. The vehicle manufacturer may refer to [the Resolution on Cyber Security and Interpretation Document on Cyber Security] in their assessment of cyber security risks and the mitigations, as well as when describing the processes employed.

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 considers the following phases:

- Development phase;
- Production phase;
- 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. 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 [section IV and Annex B of the Resolution on Cyber Security] 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;

7.2.2.3. 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. Before the assessment of a vehicle type for the purpose of type approval is carried out the vehicle manufacturer shall demonstrate to the Approval Authority or its Technical Service that their Cyber Security Management System has a valid Certificate of Compliance for CSMS and that the CSMS is relevant to the vehicle type being approved.

7.3.2. The Approval Authority or its Technical Service shall verify by means of document checks that the 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;

(b) Document risk assessment, 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 and its systems;

7.3.3. The vehicle manufacturer shall demonstrate to the satisfaction of the Approval Authority or its Technical Service the risk assessment for the vehicle type **[**and how the risks have been treated/managed**]**. The risk assessment shall consider the systems of the vehicle type and their interactions. The risk assessment shall further consider interactions with any external system.

7.3.4. The vehicle manufacturer shall demonstrate to the satisfaction of the Approval Authority or its Technical Service that critical elements of the vehicle type are protected against risks identified in the vehicle manufacturer's risk assessment. Proportionate mitigations shall be implemented to protect such elements.

7.3.5. The vehicle manufacturer shall demonstrate to the satisfaction of the Approval Authority or its Technical Service that appropriate and proportionate measures have been put in place 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 describe what testing has been performed and the outcome of those tests to verify the effectiveness of the security measures implemented.

[7.3.7. The Approval Authority or its Technical Service shall verify by testing of a sample vehicle that the vehicle manufacturer has implemented the cyber security measures they have documented. This may be achieved through sampling.]

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.

[13. Transitional provisions

13.1. As from the official date of entry into force of the 01 series of amendments, no Contracting Party applying this Regulation shall refuse to grant or refuse to accept type approvals under this Regulation as amended by the 01 series of amendments.

13.2. As from 1 September [2022], Contracting Parties applying this Regulation shall not be obliged to accept type approvals to the 00 series of amendments, first issued after 1 September [2022].

13.3. Contracting Parties applying this Regulation shall continue to accept type approvals issued according to the 00 series of amendments to this Regulation first issued before 1 September [2022].

13.4. Contracting Parties applying this Regulation shall not refuse to grant type approvals according to any preceding series of amendments to this Regulation or extensions thereof.

13.5. Notwithstanding paragraph 12.3, as from 1 September [2028], Contracting Parties applying this Regulation shall not be obliged to accept type approvals to the 00 series of amendments for vehicle types incorporating capabilities for receiving over the air software updates, which may impact type approved systems.]

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 [*this Regulation*] 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*)

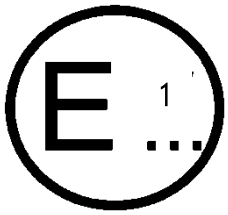
Annex 2

Communication form

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. [*this Regulation*]

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.

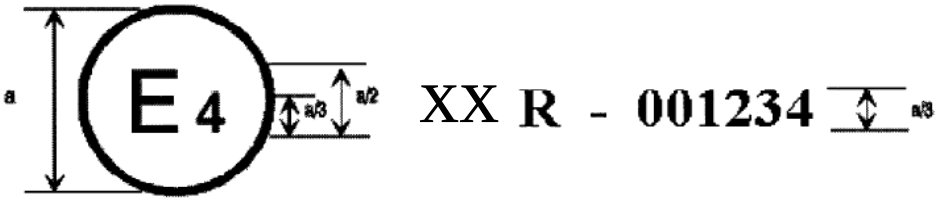
[1] Distinguishing number of the country which has granted/extended/refused/withdrawn approval (see approval provisions in the Regulation).

[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. xx, 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. [*This Regulation*]

Verifications 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.