United Nations ECE/TRANS/WP.29/GRVA/2020/4

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 a new UN Regulation on uniform provisions concerning the approval of vehicles with regard to software update processes and of software update 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/WP.29/1126, para. 28 and ECE/TRANS/WP.29/1131, para. 27. It is proposing provisions for the approval of software update management systems as well as of vehicles with regard to software update processes.

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.

GE.19-20567(E)
1920567

Draft new UN Regulation on uniform provisions concerning the approval of software update processes

Contents

1. Scope

1.1. This UN Regulation applies to vehicles of Categories M, N, [O, R, S and T] that permit software updates.

2. Definitions

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

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

(b) Essential aspects of the design of the vehicle type with respect to software update processes;

2.2. "*RX Software Identification Number (RXSWIN)*" means a dedicated identifier, defined by the vehicle manufacturer, representing information about the type approval relevant software of the Electronic Control System contributing to the Regulation N° X type approval relevant characteristics of the vehicle.

2.3 "*Software update*" means a package used to upgrade software to a new version including a change of the configuration parameters.

2.4. "*Execution*" means the process of installing and activating an update that has been downloaded.

2.5. "*Software Update Management System (SUMS)*" means a systematic approach defining organizational processes and procedures to comply with the requirements for delivery of software updates according to this Regulation.

2.6. "*Vehicle user*" means a person operating or driving the vehicle, a vehicle owner, an authorised representative or employee of a fleet manager, an authorised representative or employee of the vehicle manufacturer, or an authorized technician.

2.7. "*Safe state*" means an operating mode in case of a failure of an item without an unreasonable level of risk.

2.8. "*Software*" means the part of an Electronic Control System that consists of digital data and instruction.

2.9. "*Over The Air (OTA) update*" means any method of making data transfers wirelessly instead of using a cable or other local connection.

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

2.11. "*Integrity validation data*" means a representation of digital data, against which comparisons can be made to detect errors or changes in the data. This may include checksums and hash values.

3. Application for Approval

3.1. The application for approval of a vehicle type with regard to software update processes 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:

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

3.4. 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.

3.5. The Certificate of Compliance for Software Update Management System according to paragraph 6 of this Regulation.

3.6. A vehicle representative of the vehicle type to be approved shall be submitted to the Technical Service responsible for conducting approval tests.

3.7. 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 software update procedures and processes, 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 ensuring that the manufacturer has put in place satisfactory arrangements and procedures to manage properly the software update processes aspects as covered by this regulation.

6. Certificate of Compliance for Software Update 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 Software Update Management System.

6.2. An application for a Certificate of Compliance for Software Update 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 Software Update 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 software updates 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 SUMS as described in Annex 4 to this Regulation (hereinafter the Certificate of Compliance for SUMS) shall be granted to the manufacturer.

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

6.7. The Approval Authority which has granted the Certificate of Compliance for Software Update Management System may at any time verify its continued compliance. The Certificate of Compliance for Software Update Management System may be withdrawn if the requirements laid down in this Regulation are no longer met.

6.8. 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 Software Update Management System. After consultation with the manufacturer, the Approval Authority or its Technical Service shall decide whether new checks are necessary.

6.9. At the end of the period of validity of the Certificate of Compliance for Software Update Management System, the Approval Authority shall, after a positive assessment, issue a new Certificate of Compliance for Software Update Management System or extends 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.

6.10. Existing vehicle type approvals shall not lose their validity due to the expiration of the manufacturer’s Certificate of Compliance for Software Update Management System.

7. General Specifications

7.1. Requirements for the Software Update Management System of the vehicle manufacturer

7.1.1. Processes to be verified at initial assessment

7.1.1.1. A process whereby information relevant to this Regulation is documented and securely held at the vehicle manufacturer and can be made available to an Approval Authority or its Technical Service upon request;

7.1.1.2. A process whereby information regarding all initial and updated software versions, including integrity validation data, and relevant hardware components of a type approved system can be uniquely identified;

7.1.1.3. A process whereby, for a vehicle type that has an RXSWIN, information regarding the RXSWIN of the vehicle type before and after an update can be accessed and updated. This shall include the ability to update information regarding the software versions and their integrity validation data of all relevant software for each RXSWIN.

7.1.1.4. A process whereby, for a vehicle type that has an RXSWIN, the vehicle manufacturer can verify that the software version(s) present on a component of a type approved system are consistent with those defined by the relevant RXSWIN;

7.1.1.5. A process whereby any interdependencies of the updated system with other systems can be identified;

7.1.1.6. A process whereby the vehicle manufacturer is able to identify target vehicles for a software update;

7.1.1.7. A process to verify, before a software update is issued, the compatibility of possible software/hardware configurations for the registered configuration or last known configuration of the target vehicles with the software update;

7.1.1.8. A process to assess, identify and record whether a software update will affect any type approved systems. This shall consider whether the update will impact or alter any of the parameters used to define the systems the update may affect or whether it may change any of the parameters used to type approve those system (as defined in the relevant legislation);

7.1.1.9. A process to assess, identify and record whether a software update will add, alter or enable any functions that were not present, or enabled, when the vehicle was type approved or alter or disable any other parameters or functions that are defined within legislation. The assessment shall include consideration of whether:

(a) Entries in the information package will need to be modified;

(b) Test results no longer cover the vehicle after modification;

(c) Any modification to functions on the vehicle will affect the vehicle's type approval.

7.1.1.10. A process to assess, identify and record if a software update will affect any other system required for the safe and continued operation of the vehicle or if the update will add or alter functionality of the vehicle compared to when it was registered;

7.1.1.11. A process whereby the vehicle user is able to be informed about updates.

7.1.1.12. A process whereby the vehicle manufacturer shall be able to make the information according to paragraph 7.1.2.3. and 7.1.2.4. available to responsible Authorities or its Technical Services.

7.1.2. The vehicle manufacturer shall record, and store, the following information for each update applied to a given vehicle type:

7.1.2.1. Documentation describing the processes used by the vehicle manufacturer for software updates and any relevant standards used to demonstrate their compliance;

7.1.2.2. Documentation describing the configuration of any relevant type approved systems before and after an update, this shall include unique identification for the type approved system's hardware and software (including software versions) and any relevant vehicle or system parameters;

7.1.2.3. For every RXSWIN, there shall be an auditable register describing all the software relevant to the RXSWIN of the vehicle type before and after an update. This shall include information of the software versions and their integrity validation data for all relevant software for each RXSWIN.

7.1.2.4. Documentation listing target vehicles for the update and verification of the compatibility of the registered configuration or last known configuration of those vehicles with the update.

7.1.2.5. Documentation for all software updates for that vehicle type describing:

(a) The purpose of the update;

(b) What systems or functions of the vehicle the update may affect;

(c) Which of these are type approved (if any);

(d) If applicable, whether the software update affects the fulfilment of any of the relevant requirements of those type approved system;

(e) Whether the software update affects any system type approval parameter;

(f) Whether an approval for the update was sought from an approval body;

(g) How the update may be executed and under what conditions;

(h) Confirmation that the software update will be conducted safely and securely.

(i) Confirmation that the software update has undergone and successfully passed verification and validation procedures.

7.1.3. Security, the vehicle manufacturer shall demonstrate:

7.1.3.1. The process they will use to ensure that software updates will be protected to reasonably prevent manipulation before the update process is initiated.;

7.1.3.2. The update processes used are protected to reasonably prevent them being compromised, including development of the update delivery system;

7.1.3.3. The processes used to verify and validate software functionality and code for the software used in the vehicle are appropriate.

7.1.4. Additional requirements for software updates over the air

7.1.4.1. The vehicle manufacturer shall demonstrate the processes and procedures they will use to assess that over the air updates will not impact safety, if conducted during driving.

7.1.4.2. The vehicle manufacturer shall demonstrate the processes and procedures they will use to ensure that, when an over the air update requires a specific skilled or complex action, for example recalibrate a sensor post-programming, in order to complete the update process, the update can only proceed when a person skilled to do that action is present or is in control of the process.

7.2. Requirements for the Vehicle Type

7.2.1. Requirements for Software updates

7.2.1.1. The authenticity and integrity of software updates shall be protected to reasonably prevent their compromise and reasonably prevent invalid updates.

7.2.1.2. Where a vehicle type uses RXSWIN:

7.2.1.2.1. Each RXSWIN shall be uniquely identifiable. When type approval relevant software is modified by the vehicle manufacturer, the RXSWIN shall be updated if it leads to a type approval extension or to a new type approval.

7.2.1.2.2. Each RXSWIN shall be easily readable in a standardized way via the use of an electronic communication interface, at least by the standard interface (OBD port).

If RXSWINs are not held on the vehicle, the manufacturer shall declare the software version(s) of the vehicle or single ECUs with the connection to the relevant type approvals to the Approval Authority. This declaration shall be updated each time the declared software version(s) is updated. In this case, the software version(s) shall be easily readable in a standardized way via the use of an electronic communication interface, at least by the standard interface (OBD port).

7.2.1.2.3. The vehicle manufacturer shall protect the RXSWINs and/or software version(s) on a vehicle against unauthorised modification. At the time of Type Approval, the means implemented to protect against unauthorized modification of the RXSWIN and/or software version(s) chosen by the vehicle manufacturer shall be confidentially provided.

7.2.2. Additional Requirements for over the air updates

7.2.2.1. The vehicle shall have the following functionality with regards to software updates:

7.2.2.1.1. The vehicle manufacturer shall ensure that the vehicle is able to restore systems to their previous version in case of a failed or interrupted update or that the vehicle can be placed into a safe state after a failed or interrupted update.

7.2.2.1.2. The vehicle manufacturer shall ensure that software updates can only be executed when the vehicle has enough power to complete the update process (including that needed for a possible recovery to the previous version or for the vehicle to be placed into a safe state).

7.2.2.1.3. When the execution of an update may affect the safety of the vehicle, the vehicle manufacturer shall demonstrate how the update will be executed safely. This shall be achieved through technical means that ensures the vehicle is in a state where the update can be executed safely.

7.2.2.2. The vehicle manufacturer shall demonstrate that the vehicle user is able to be informed about an update before the update is executed. The information made available shall contain:

- The purpose of the update. This could include the criticality of the update and if the update is for recall, safety and/or security purposes;
- Any changes implemented by the update on vehicle functions;
- The expected time to complete execution of the update;
- Any vehicle functionalities which may not be available during the execution of the update;
- Any instructions that may help the vehicle user safely execute the update;

In case of groups of updates with a similar content one information may cover a group.

7.2.2.3. In the situation where the execution of an update whilst driving may not be safe, the vehicle manufacturer shall demonstrate how they will:

- Ensure the vehicle cannot be driven during the execution of the update;
- Ensure that the driver is not able to use any functionality of the vehicle that would affect the safety of the vehicle or the successful execution of the update.

7.2.2.4. After the execution of an update the vehicle manufacturer shall demonstrate how the following will be implemented:

- The vehicle user is able to be informed of the success (or failure) of the update;
- The vehicle user is able to be informed about the changes implemented and any related updates to the user manual (if applicable).

[7.2.2.5. Before the software update process starts the vehicle manufacturer shall inspect the vehicle(s) to ensure that the software update can be successfully completed. The vehicle manufacturer shall demonstrate to the satisfaction of the Approval Authority and its Technical Service the measures for managing the situation when the vehicle manufacturer detects that an update should not be initiated.]

8. Modification and extension of the vehicle type

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

8.1.1. Consider that the modifications made still comply with the requirements and documentation of prior 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.

9.1.3. The Approval Authority or its Technical Service shall periodically validate that the processes used and decisions made by the vehicle manufacturer are compliant, particularly for instances where the vehicle manufacturer chose not to notify the Approval Authority or its Technical Service about an update. This may be achieved on a sampling basis.

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 requirement 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): .....

(Type is the type to be approved, commercial description refers to the product in which the approved type is used) .....

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. Software Updates

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

9.2. The number of the Certificate of Compliance for Software Update Management System: .....

9.3. Security measures.

9.3.1. Documents for the vehicle type to be approved describing that the update process will be performed securely .....

9.3.2. Documents for the vehicle type to be approved describing that the RXSWINs on a vehicle are protected against unauthorized manipulation .....

9.4. Software updates over the air

9.4.1. Documents for the vehicle type to be approved describing that the update process will be performed safely .....

9.4.2. How a vehicle user is able to be informed about an update before and after its execution.

Annex 1 - Appendix 1

Model of declaration of compliance for Software Update Management System

Manufacturer's declaration of compliance with the requirements for Software Update Management System

Manufacturer Name: .....

Manufacturer Address: .....

…….. (Manufacturer Name) attests that the necessary processes to comply with the requirements for the Software Update Management System laid down in paragraph 7.1 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)

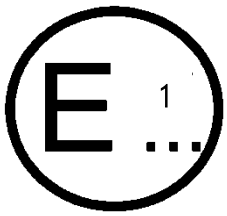
Annex 2

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: .....

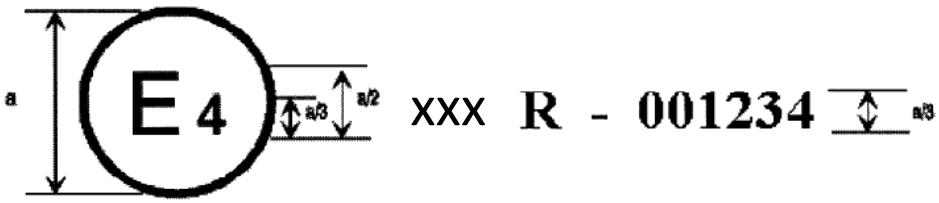
1. Make (trade name of manufacturer): .....
2. Type and general commercial description(s) .....
3. Means of identification of type, if marked on the vehicle: .....
- 3.1. Location of that marking: .....
4. Category(ies) of vehicle: .....
5. Name and address of manufacturer / manufacturer's representative: .....
6. Name(s) and Address(es) of the production plant(s) .....
7. Number of the certificate of compliance for software update management system: ...
8. Software updates over the air included (Yes/no): .....
9. Technical Service responsible for carrying out the tests: .....
10. Date of test report: .....
11. Number of test report: .....
12. Remarks: (if any). .....
13. Place: .....
14. Date: .....
15. Signature: .....
16. 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. xxx, 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 Software Update Management System

CERTIFICATE OF COMPLIANCE FOR SOFTWARE UPDATE 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 Regulation No.[*this Regulation*]

Verifications have been performed on: .....

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

Number of report:.....

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

Done at: [……*Place*]

On: […….*Date*]

[…….*Signature*]

Attachments: description of the Software Update Management System by the manufacturer.