

Official Journal of the European Union

L 82



English edition

Legislation

Volume 64

9 March 2021

Contents

II *Non-legislative acts*

ACTS ADOPTED BY BODIES CREATED BY INTERNATIONAL AGREEMENTS

★ UN Regulation No 153 – Uniform provisions concerning the approval of vehicles with regard to fuel system integrity and safety of electric power train in the event of a rear-end collision [2021/386]	1
★ UN Regulation No 155 – Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system [2021/387]	30
★ UN Regulation No 156 – Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system [2021/388]	60
★ UN Regulation No 157 – Uniform provisions concerning the approval of vehicles with regards to Automated Lane Keeping Systems [2021/389]	75

EN

Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.

The titles of all other acts are printed in bold type and preceded by an asterisk.

II

*(Non-legislative acts)***ACTS ADOPTED BY BODIES CREATED BY
INTERNATIONAL AGREEMENTS**

Only the original UN/ECE texts have legal effect under international public law. The status and date of entry into force of this Regulation should be checked in the latest version of the UN/ECE status document

TRANS/WP.29/343, available at:

<http://www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29docstts.html>

UN Regulation No 153 – Uniform provisions concerning the approval of vehicles with regard to fuel system integrity and safety of electric power train in the event of a rear-end collision [2021/386]

Date of entry into force: 22 January 2021

This document is meant purely as documentation tool. The authentic and legally binding text is: ECE/TRANS/WP.29/2020/76.

CONTENTS

REGULATION

1. Scope
2. Definitions
3. Application for approval
4. Approval
5. Requirements
6. Test
7. Modification and extension of approval of a vehicle type
8. Conformity of production
9. Penalties for non-conformity of production
10. Production definitively discontinued
11. Names and addresses of the Technical Services responsible for conducting approval tests and of the Type Approval Authorities

ANNEXES

- 1 Communication
- 2 Examples of arrangements of approval marks
- 3 Procedure for rear-end impact test
- 4 Test conditions and procedures for the assessment of post-crash hydrogen fuel system
- 5 Test procedures for vehicles equipped with electric power train

1. SCOPE

This Regulation applies to vehicles of category M₁ ⁽¹⁾ with a total permissible mass not exceeding 3 500 kg and to vehicles of category N₁ with regard to fuel system integrity and safety of electric power train operating on high voltage in the event of a rear-end collision.

2. DEFINITIONS

For the purpose of this Regulation:

2.1. 'Vehicle type' means a category of power-driven vehicles which do not differ in such essential respects as:

2.1.1. The length and width of the vehicle in so far as they have an effect on the results of the impact test prescribed in this Regulation.

2.1.2. The structure, dimensions, lines and materials of the part of the vehicle rearward of the transverse plane through the 'R' point of the rearmost seat.

2.1.3. The lines and inside dimensions of the passenger compartment in so far as they have an effect on the results of the impact test prescribed in this Regulation.

2.1.4. The siting (front, rear or centre) and the orientation (transversal or longitudinal) of the engine, in so far as they have a negative effect on the result of the impact test procedure as prescribed in this Regulation.

2.1.5. The unladen mass, in so far as there is a negative effect on the result of the impact test prescribed in this Regulation.

2.1.6. The locations of the REESS, in so far as they have a negative effect on the result of the impact test prescribed in this Regulation.

2.1.7. The structure, shape, dimensions and materials (metal/plastic) of the tank(s).

2.1.8. The position of the tank(s) in the vehicle in so far as it has a negative effect on the requirements of paragraph 5.2.1.

2.1.9. The characteristics and location of the fuel feed system (pump, filters, etc.).

2.2. 'Passenger compartment' means the space for occupant accommodation, bounded by the roof, floor, side walls, doors, outside glazing, front bulkhead and rear bulkhead, or rear gate, as well as by the electrical protection barriers and enclosures provided for protecting the occupants from direct contact with high voltage live parts.

2.3. 'Unladen mass' means the mass of the vehicle in running order, unoccupied and unladen but complete with fuel, coolant, lubricant, tools and a spare wheel (if provided as standard equipment by the vehicle manufacturer).

2.4. 'Tank' means the tank(s) designed to contain the liquid fuel, as defined in paragraph 2.6 or compressed hydrogen gas, used primarily for the propulsion of the vehicle excluding its accessories (filler pipe, if it is a separate element, filler hole, cap, gauge, connections to the engine or to compensate interior excess pressure, etc.);

⁽¹⁾ As defined in the Consolidated Resolution on the Construction of Vehicles (R.E.3.), document ECE/TRANS/WP.29/78/Rev.6, para. 2. – www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29resolutions.html

- 2.5. 'Capacity of the fuel tank' means the fuel-tank capacity as specified by the manufacturer.
- 2.6. 'Liquid fuel' means a fuel which is liquid in normal conditions of temperature and pressure.
- 2.7. 'High voltage' means the classification of an electric component or circuit, if its working voltage is > 60 V and $\leq 1\,500$ V direct current (DC) or > 30 V and $\leq 1\,000$ V alternating current (AC) root – mean – square (rms).
- 2.8. 'Rechargeable electrical energy storage system (REESS)' means the rechargeable energy storage system that provides electric energy for propulsion.
- A battery whose primary use is to supply power for starting the engine and/or lighting and/or other vehicle auxiliary systems is not considered as a REESS [Primary use in this context means that more than 50 per cent of the energy from the battery is used for starting the engine and/or lighting and/or other vehicle auxiliary systems over an appropriate driving cycle, e.g. WLTC for M_1 and N_1].
- 2.9. 'Electrical protection barrier' means the part providing protection against any direct contact to the high voltage live parts.
- 2.10. 'Electric power train' means the electrical circuit which includes the traction motor(s), and may also include the REESS, the electric energy conversion system, the electronic converters, the associated wiring harness and connectors, and the coupling system for charging the REESS.
- 2.11. 'Live parts' means conductive part(s) intended to be electrically energized under normal operating conditions.
- 2.12. 'Exposed conductive part' means the conductive part which can be touched under the provisions of the protection degree IPXXB which is not normally energized, but which can become electrically energized under isolation failure conditions. This includes parts under a cover that can be removed without using tools.
- 2.13. 'Direct contact' means the contact of persons with high voltage live parts.
- 2.14. 'Indirect contact' means the contact of persons with exposed conductive parts.
- 2.15. 'Protection degree IPXXB' means protection from contact with high voltage live parts provided by either an electrical protection barrier or an enclosure and tested using a Jointed Test Finger (protection degree IPXXB) as described in paragraph 4 of Annex 5.
- 2.16. 'Working voltage' means the highest value of an electrical circuit voltage root-mean-square (rms), specified by the manufacturer, which may occur between any conductive parts in open circuit conditions or under normal operating conditions. If the electrical circuit is divided by galvanic isolation, the working voltage is defined for each divided circuit, respectively.
- 2.17. 'Coupling system for charging the Rechargeable Electrical Energy Storage System (REESS)' means the electrical circuit used for charging the REESS from an external electrical power supply including the vehicle inlet.
- 2.18. 'Electrical chassis' means a set made of conductive parts electrically linked together, whose electrical potential is taken as reference.
- 2.19. 'Electrical circuit' means an assembly of connected high voltage live parts which is designed to be electrically energized in normal operation.
- 2.20. 'Electric energy conversion system' means a system (e.g. fuel cell) that generates and provides electric energy for electric propulsion.

- 2.21. 'Electronic converter' means a device capable of controlling and/or converting electric power for electric propulsion.
- 2.22. 'Enclosure' means the part enclosing the internal units and providing protection against any direct contact.
- 2.23. 'High Voltage Bus' means the electrical circuit, including the coupling system for charging the REESS that operates on a high voltage. Where electrical circuits are galvanically connected to each other and fulfil the specific voltage condition, only the components or parts of the electric circuit that operate on high voltage are classified as a high voltage bus.
- 2.24. 'Solid insulator' means the insulating coating of wiring harnesses, provided in order to cover and prevent the high voltage live parts from any direct contact.
- 2.25. 'Automatic disconnect' means a device that when triggered, conductively separates the electrical energy sources from the rest of the high voltage circuit of the electric power train.
- 2.26. 'Open type traction battery' means a type of battery requiring liquid and generating hydrogen gas released to the atmosphere.
- 2.27. 'Aqueous electrolyte' means an electrolyte based on water solvent for the compounds (e.g. acids, bases) which provides conducting ions after its dissociation.
- 2.28. 'Electrolyte leakage' means the escape of electrolyte from REESS in the form of liquid.
- 2.29. 'Non-aqueous electrolyte' means an electrolyte not based on water as the solvent.
- 2.30. 'Normal operating conditions' includes operating modes and conditions that can reasonably be encountered during normal operation of the vehicle including driving at legal speeds, parking or idling in traffic, as well as, charging using chargers that are compatible with the specific charging ports installed on the vehicle. It does not include, conditions where the vehicle is damaged, either by a crash, road debris or vandalism, subjected to fire or water submersion, or in a state where service and or maintenance is needed or being performed.
- 2.31. 'Specific voltage condition' means the condition that the maximum voltage of a galvanically connected electrical circuit between a DC live part and any other live part (DC or AC) is ≤ 30 V AC (rms) and ≤ 60 V DC.
- Note:* When a DC live part of such an electrical circuit is connected to chassis and the specific voltage condition applies, the maximum voltage between any live part and the electrical chassis is ≤ 30 V AC (rms) and ≤ 60 V DC.

3. APPLICATION FOR APPROVAL

- 3.1. The application for approval of a vehicle type with regard to fuel system integrity and with regard to the safety of electric power train operating on high voltage in the event of rear-end collision shall be submitted by the vehicle manufacturer or by their duly accredited representative in accordance with the procedure set out in Schedule 3 of the Agreement (E/ECE/TRANS/505/Rev.3).
- 3.2. A model of the information document is given in Annex 1 – Appendix 1.

4. APPROVAL

- 4.1. If the vehicle submitted for approval pursuant to this Regulation meets the requirements of this Regulation, approval of that vehicle type shall be granted.
- 4.1.1. The Technical Service appointed in accordance with paragraph 11 below shall check whether the required conditions have been satisfied.
- 4.1.2. In case of doubt, account shall be taken, when verifying the conformity of the vehicle to the requirements of this Regulation, of any data or test results provided by the manufacturer which can be taken into consideration in validating the approval test carried out by the Technical Service.
- 4.2. An approval number shall be assigned to each type approved in accordance with Schedule 4 of the Agreement (E/ECE/TRANS/505/Rev.3).
- 4.3. Notice of approval or of extension or of refusal or withdrawal of approval or production definitely discontinued of a vehicle type pursuant to this Regulation shall be communicated to the Contracting Parties to the Agreement which apply this Regulation by means of a form conforming to the model in Annex 1 to this Regulation.
- 4.4. 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 conforming to the model given in Annex 2 consisting of:
- 4.4.1. A circle surrounding the letter 'E' followed by the distinguishing number of the country which has granted approval ⁽²⁾;
- 4.4.2. the number of this Regulation, followed by the letter 'R', a dash and the approval number to the right of the circle prescribed in paragraph 4.4.1.
- 4.5. If the vehicle conforms to a vehicle type approved, under one or more other UN Regulations annexed to the Agreement, in the country which has granted approval under this Regulation, the symbol prescribed in paragraph 4.4.1 need not be repeated; in such a case the additional numbers and symbols of all the UN 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 4.4.1.
- 4.6. The approval mark shall be clearly legible and be indelible.

5. REQUIREMENTS

- 5.1. When the vehicle has undergone the test referred to in paragraph 6 below, the provisions in paragraph 5.2 shall be fulfilled.
- A vehicle with all parts of the fuel system installed in front of the midpoint of the wheelbase is deemed to fulfil the provisions in paragraph 5.2.1.
- A vehicle with all parts of the electric power train operating on high voltage installed in front of the midpoint of the wheelbase is deemed to fulfil the provisions in paragraph 5.2.2.
- 5.2. Following the test conducted in accordance with the procedure laid down in Annex 3, Annex 4 and Annex 5 to this Regulation, following provisions with regard to fuel system integrity and safety of electric power train shall be fulfilled:

⁽²⁾ The distinguishing numbers of the Contracting Parties to the 1958 Agreement are reproduced in Annex 3 to the Consolidated Resolution on the Construction of Vehicles (R.E.3), document ECE/TRANS/WP.29/78/Rev. 6, Annex 3- www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29resolutions.html.

5.2.1. In the case of a vehicle propelled by liquid fuel, compliance with paragraphs 5.2.1.1 to 5.2.1.2 shall be shown.

In case of compressed hydrogen-fuelled vehicles, compliance with paragraphs 5.2.1.3 to 5.2.1.5 shall be shown.

5.2.1.1. No more than slight leakage of liquid from the fuel-feed installation shall occur on collision.

5.2.1.2. If there is continuous leakage of liquid from the fuel-feed installation after the collision, the rate of leakage shall not exceed 30 g/min; if the liquid from the fuel-feed system mixes with liquids from the other systems and the various liquids cannot easily be separated and identified, all the liquids collected shall be taken into account in evaluating the continuous leakage.

5.2.1.3. The hydrogen leakage rate (V_{H_2}) determined in accordance with either, paragraph 4 of Annex 4 for hydrogen, or paragraph 5 of Annex 4 for helium, shall not exceed an average of 118 NL per minute for the time interval, Δt minutes, after the crash.

5.2.1.4. The gas (hydrogen or helium as applicable) concentration by volume in air values determined for the passenger and luggage compartments in accordance with paragraph 6 of Annex 4, shall not exceed 4,0 per cent for hydrogen or 3,0 per cent for helium, at any time throughout the 60 minute post-crash measurement period. This requirement is satisfied if it is confirmed that the shut-off valve of each hydrogen storage system has closed within 5 seconds of first vehicle contact with the impactor and there is no leakage from the hydrogen storage system(s).

5.2.1.5. The container(s) (for hydrogen storage) shall remain attached to the vehicle at a minimum of one attachment point.

5.2.2. In case of a vehicle equipped with an electric power train operating on high voltage, the electric power train and the high voltage systems which are galvanically connected to the high voltage bus of the electric power train shall meet the requirements in paragraphs 5.2.2.1 to 5.2.2.3.:

5.2.2.1. Protection against electrical shock

After the impact, the high voltage buses shall meet at least one of the four criteria specified in paragraph 5.2.2.1.1 through paragraph 5.2.2.1.4.2 below.

If the vehicle has an automatic disconnect function, or device(s) that conductively divide the electric power train circuit during driving condition, at least one of the following criteria shall apply to the disconnected circuit or to each divided circuit individually after the disconnect function is activated.

However, criteria defined in 5.2.2.1.4. below shall not apply if more than a single potential of a part of the high voltage bus is not protected under the conditions of protection degree IPXXB.

In the case that the crash test is performed under the condition that part(s) of the high voltage system are not energized and with the exception of any coupling system for charging the REESS which is not energized during driving, the protection against electrical shock shall be proved by either paragraph 5.2.2.1.3 or paragraph 5.2.2.1.4 for the relevant part(s).

5.2.2.1.1. Absence of high voltage

The voltages U_b , U_1 and U_2 of the high voltage buses shall be equal or less than 30 VAC or 60 VDC within 60 s after the impact when measured in accordance with paragraph 2 of Annex 5.

5.2.2.1.2. Low electrical energy

The Total Energy (TE) on the high voltage buses shall be less than 0,2 J when measured according to the test procedure as specified in paragraph 3 of Annex 5 with the formula (a). Alternatively, the Total Energy (TE) may be calculated by the measured voltage U_b of the high voltage bus and the capacitance of the X-capacitors (Cx) specified by the manufacturer according to formula (b) of paragraph 3 of Annex 5.

The energy stored in the Y-capacitors (TEy1, TEy2) shall also be less than 0,2 J. This shall be calculated by measuring the voltages U_1 and U_2 of the high voltage buses and the electrical chassis, and the capacitance of the Y-capacitors specified by the manufacturer according to formula (c) of paragraph 3 of Annex 5.

5.2.2.1.3. Physical protection

For protection against direct contact with high voltage live parts, the protection degree IPXXB shall be provided.

The assessment shall be conducted in accordance with paragraph 4 of Annex 5.

In addition, for protection against electrical shock which could arise from indirect contact, the resistance between all exposed conductive parts of electrical protection barriers/enclosures and the electrical chassis shall be lower than 0,1 Ω and the resistance between any two simultaneously reachable exposed conductive parts of electrical protection barriers/enclosures that are less than 2,5 m from each other shall be less than 0,2 Ω when there is current flow of at least 0,2 A. This resistance may be calculated using the separately measured resistances of the relevant parts of electric path.

This requirement is satisfied if the galvanic connection has been made by welding. In case of doubt or the connection is established by means other than welding, measurement shall be made by using one of the test procedures described in paragraph 4 of Annex 5.

5.2.2.1.4. Isolation resistance

The criteria specified in the paragraphs 5.2.2.1.4.1 and 5.2.2.1.4.2 below shall be met.

The measurement shall be conducted in accordance with paragraph 5 of Annex 5.

5.2.2.1.4.1. Electric power train consisting of separate DC- or AC-buses

If the AC high voltage buses and the DC high voltage buses are galvanically isolated from each other, isolation resistance between the high voltage bus and the electrical chassis (R_i , as defined in paragraph 5 of Annex 5) shall have a minimum value of 100 Ω/V of the working voltage for DC buses, and a minimum value of 500 Ω/V of the working voltage for AC buses.

5.2.2.1.4.2. Electric power train consisting of combined DC- and AC-buses

If the AC high voltage buses and the DC high voltage buses are conductively connected, they shall meet one of the following requirements:

- (a) Isolation resistance between the high voltage bus and the electrical chassis shall have a minimum value of 500 Ω/V of the working voltage;
- (b) Isolation resistance between the high voltage bus and the electrical chassis shall have a minimum value of 100 Ω/V of the working voltage and the AC bus meets the physical protection as described in paragraph 5.2.2.1.3;
- (c) Isolation resistance between the high voltage bus and the electrical chassis shall have a minimum value of 100 Ω/V of the working voltage and the AC bus meets the absence of high voltage as described in paragraph 5.2.2.1.1.

5.2.2.2. Electrolyte leakage

5.2.2.2.1. In case of aqueous electrolyte REESS.

For a period from the impact until 60 minutes after the impact, there shall be no electrolyte leakage from the REESS into the passenger compartment and no more than 7 per cent by volume of the REESS electrolyte with a maximum of 5,0 l leaked from the REESS to the outside of the passenger compartment. The leaked amount of electrolyte can be measured by the usual techniques of determining liquid volumes after its collection. For containers containing Stoddard, coloured coolant and electrolyte, the fluids shall be allowed to separate by specific gravity then measured.

5.2.2.2.2. In case of non-aqueous electrolyte REESS.

For a period from the impact until 60 minutes after the impact, there shall be no liquid electrolyte leakage from the REESS into the passenger compartment or luggage compartment and no liquid electrolyte leakage to outside the vehicle. This requirement shall be verified by visual inspection without disassembling any part of the vehicle.

The manufacturer shall demonstrate compliance in accordance with paragraph 6 of Annex 5.

5.2.2.3. REESS retention

REESS shall remain attached to the vehicle by at least one component anchorage, bracket, or any structure that transfers loads from REESS to the vehicle structure, and REESS located outside the passenger compartment shall not enter the passenger compartment.

The manufacturer shall demonstrate compliance in accordance with paragraph 7 of Annex 5.

6. TEST

6.1. The vehicle's compliance with the requirements of paragraph 5 above shall be checked by the method set out in Annex 3, Annex 4 and Annex 5 to this Regulation

7. MODIFICATIONS AND EXTENSION OF APPROVAL OF THE VEHICLE TYPE

7.1. Every modification of the vehicle type with regard to this Regulation shall be notified to the Type Approval Authority which approved that vehicle type. The Type Approval Authority may then either:

- (a) Decide, in consultation with the manufacturer, that a new type approval is to be granted; or
- (b) Apply the procedure contained in paragraph 7.1.1 (Revision) and, if applicable, the procedure contained in paragraph 7.1.2 (Extension).

7.1.1. Revision

When particulars recorded in the information documents of Annex 1 – Appendix 1 have changed and the Type Approval Authority considers that the modifications made are unlikely to have appreciable adverse effect, and that in any case the vehicle still meets the requirements, the modification shall be designated a 'revision'.

In such a case, the Type Approval Authority shall issue the revised pages of the information documents of Annex 1 – Appendix 1 as necessary, marking each revised page to show clearly the nature of the modification and the date of re-issue. A consolidated, updated version of the information documents of Annex 1 – Appendix 1, accompanied by a detailed description of the modification, shall be deemed to meet this requirement.

7.1.2. Extension

The modification shall be designated an 'extension' if, in addition to the change of the particulars recorded in the information folder:

- (a) Further inspections or tests are required; or
- (b) Any information on the communication document (with the exception of its attachments) has changed; or
- (c) Approval to a later series of amendments is requested after its entry into force.

7.2. Notice of confirmation, extension, or refusal of approval shall be communicated by the procedure specified in paragraph 4.3 above, to the Contracting Parties to the Agreement applying this Regulation. In addition, the index to the information documents and to the test reports, attached to the communication document of Annex 1, shall be amended accordingly to show the date of the most recent revision or extension.

7.3. The Type Approval Authority issuing the extension of approval shall assign a series number to each communication form drawn up for such an extension.

8. CONFORMITY OF PRODUCTION

The conformity of production procedures shall comply with those set out in the Agreement, Schedule 1 (E/ECE/TRANS/505/Rev.3), with the following requirements:

8.1. Every vehicle bearing an approval mark as prescribed under this Regulation shall conform to the vehicle type approved by meeting the requirements set out in paragraph 5 above.

9. PENALTIES FOR NON-CONFORMITY OF PRODUCTION

9.1. The approval granted in respect of a vehicle type pursuant to this Regulation may be withdrawn if the requirements laid down in paragraph 8.1 above is not complied with.

9.2. If a Contracting Party to the Agreement which applies this Regulation withdraws an approval it has previously granted, it shall forthwith notify the other Contracting Parties applying this Regulation by means of a copy of the approval form bearing at the end, in large letters, the signed and dated annotation 'APPROVAL WITHDRAWN'.

10. PRODUCTION DEFINITELY DISCONTINUED

If the holder of the approval completely ceases to manufacture the vehicle type approved in accordance with this Regulation, he shall so inform the Type Approval Authority which granted the approval. Upon receiving the relevant communication that Type Approval Authority shall inform thereof the other Contracting Parties 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'.

11. NAMES AND ADDRESSES OF TECHNICAL SERVICES RESPONSIBLE FOR CONDUCTING APPROVAL TESTS AND OF TYPE APPROVAL AUTHORITIES

The Contracting Parties to the Agreement applying this Regulation shall communicate to the Secretariat of the United Nations 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 refusal, or extension or withdrawal of approval, issued in the other countries, are to be sent.

ANNEX 1

Communication

(Maximum format: A4 (210 × 297 mm))



Issued by:

Name of administration:

.....

.....

.....

Concerning ⁽²⁾ :

Approval granted

Approval extended

Approval refused

Approval withdrawn

Production definitively discontinued

of a vehicle type with regard to fuel system integrity and with regard to the safety of electric power train in a rear-end collision, pursuant to UN Regulation 153

Approval No Extension No:

1. Trade name or mark of the power-driven vehicle

2. Vehicle type

3. Manufacturer's name and address

.....

4. If applicable, name and address of manufacturer's representative:

.....

.....

5. Brief description of the vehicle type

.....

5.1. Description of the fuel system installed in the vehicle

.....

5.2. Description of the electric power train

.....

6. Site of engine: forward/rear/central ⁽²⁾7. Drive: front-wheel/rear-wheel ⁽²⁾

8. Mass of vehicle submitted for testing:

Front axle:

Rear axle:

Total:

9. Vehicle submitted for approval on
 10. Technical Service responsible for conducting approval tests
 11. Date of report issued by that Service
 12. Number of reports issued by that Service
 13. Approval granted/refused/extended/withdrawn ^(?)
 14. Position of approval mark on vehicle
 15. Place
 16. Date
 17. Signature
 18. The following documents, bearing the approval number shown above, are annexed to this communication:
 19. Remarks (e.g. alternative test method according to Annex 3, paragraph 3 applied.)
- (Photographs and/or diagrams and drawings permitting the basic identification of the type(s) of vehicle and its possible variants which are covered by the approval)

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

⁽²⁾ Strike out what does not apply

*Appendix 1 to Annex 1***Information document**

0. GENERAL

0.1. Make (trade name of manufacturer):

0.2. Type:

0.2.1. Commercial name(s) (if available):

0.3. Means of identification of type, if marked on the vehicle ⁽¹⁾:

0.3.1. Location of that marking:

0.4. Category of vehicle ⁽²⁾:

0.5. Company name and address of manufacturer:

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

0.9. Name and address of the manufacturer's representative (if any):

1. GENERAL CONSTRUCTION CHARACTERISTICS OF THE VEHICLE

1.1. Photographs and/or drawings of a representative vehicle

1.3. Number of axles and wheels:

1.3.3. Powered axles (number, position, interconnection):

1.6. Position and arrangement of the engine:

2. MASSES AND DIMENSIONS (in kg and mm) (Refer to drawing where applicable)

2.1. Wheelbase(s) (fully loaded)

2.1.1. Two-axle vehicles:

2.1.2. Vehicles with three or more axles

2.1.2.2. Total axle spacing:

2.4. Range of vehicle dimensions (overall)

2.4.1. For chassis without bodywork

2.4.1.1. Length (mm):

2.4.1.2. Width (mm):

2.4.2. For chassis with bodywork

2.4.2.1. Length (mm):

2.4.2.2. Width (mm)

- 2.6. Mass in running order (kg):
- 3. PROPULSION ENERGY CONVERTER
 - 3.2.2. Fuel
 - 3.2.2.1. Light-duty vehicles: Diesel/Petrol/LPG/NG or Biomethane/Ethanol (E 85)/Biodiesel/Hydrogen
 - 3.2.3. Fuel tank(s)
 - 3.2.3.1. Service fuel tank(s)
 - 3.2.3.1.1. Number and capacity of each tank:
 - 3.2.3.1.1.1. Material
 - 3.2.3.1.2. Drawing and technical description of the tank(s) with all connections and all lines of the breathing and venting system, locks, valves, fastening devices
 - 3.2.3.1.3. Drawing clearly showing the position of the tank(s) in the vehicle
 - 3.2.3.2. Reserve fuel tank(s)
 - 3.2.3.2.1. Number and capacity of each tank:
 - 3.2.3.2.1.1. Material
 - 3.2.3.2.2. Drawing and technical description of the tank(s) with all connections and all lines of the breathing and venting system, locks, valves, fastening devices
 - 3.2.3.2.3. Drawing clearly showing the position of the tank(s) in the vehicle
 - 3.3.2. REESS
 - 3.3.2.4. Position
- 3.4. Combinations of propulsion energy converters
 - 3.4.1. Hybrid electric vehicle: yes/no
 - 3.4.2. Category of hybrid electric vehicle: off-vehicle charging/not off-vehicle charging:

(¹) If the means of identification of type contains characters which are not relevant to describing the vehicle, i.e. types covered by the type-approval certificate, such characters shall be represented in the documentation by the symbol '?' (e.g. ABC??123??).

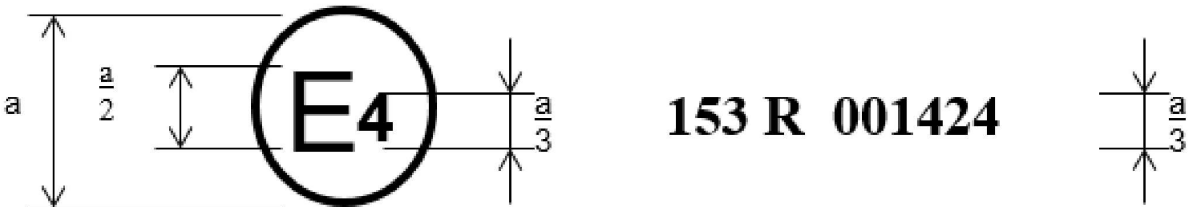
(²) As defined in the Consolidated Resolution on the Construction of Vehicles (R.E.3.), document ECE/TRANS/WP.29/78/Rev.6, para. 2. – www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29resolutions.html

ANNEX 2

Arrangements of approval marks

MODEL A

(See paragraph 4.4 of this Regulation)

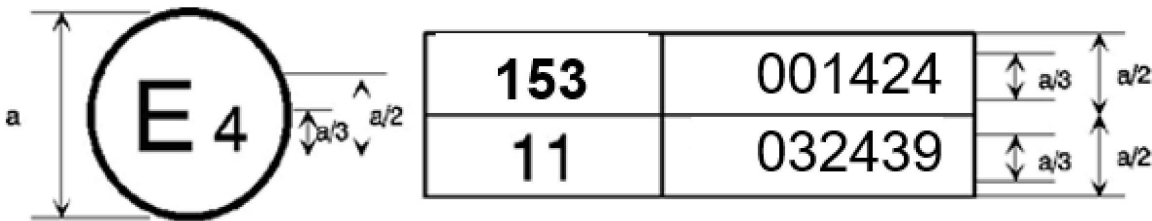


a = 8 mm min.

The above approval mark affixed to a vehicle shows that the vehicle type concerned has, with regard to the protection of the occupants in the event of a rear-end collision, been approved in the Netherlands (E 4) pursuant to UN Regulation No 153 under approval number 001424. The approval number indicates that the approval was granted in accordance with the requirements of UN Regulation No 153 in its original form.

MODEL B

(See paragraph 4.5 of this Regulation)



a = 8 mm min.

The first two digits of the approval numbers indicate that, at the dates when the respective approvals were granted, UN Regulation No 153 was in its original version and UN Regulation No 11 incorporated the 03 series of amendments

ANNEX 3

Procedure for rear-end impact test

1. Purpose

- 1.1. The purpose of the test is to simulate the conditions of rear-end impact by another vehicle in motion.

2. Installations, procedures and measuring instruments

2.1. Testing ground

The test area shall be large enough to accommodate the impactor (striker) propulsion system and to permit after-impact displacement of the vehicle impacted and installation of the test equipment. The part of which vehicle impact and displacement occur shall be horizontal, flat and smooth and representative of a normal, dry, uncontaminated road surface.

2.2. Impactor (striker)

- 2.2.1. The impactor shall be of steel and of rigid construction.

- 2.2.2. The impacting surface shall be flat, not less than 2 500 mm wide, and 800 mm high, and its edges shall be rounded to a radius of curvature of between 40 and 50 mm. It shall be covered with plywood boards 20 ± 2 mm thick.

- 2.2.3. At the moment of impact, the following requirements shall be met:

- 2.2.3.1. The impacting surface shall be vertical and perpendicular to the median longitudinal plane of the impacted vehicle;

- 2.2.3.2. The direction of movement of the impactor shall be substantially horizontal and parallel to the median longitudinal plane of the impacted vehicle;

- 2.2.3.3. The maximum lateral deviation tolerated between the median vertical line of the surface of the impactor and the median longitudinal plane of the impacted vehicle shall be 300 mm. In addition, the impacting surface shall extend over the entire width of the impacted vehicle;

- 2.2.3.4. The ground clearance of the lower edge of the impact surface shall be 175 ± 25 mm.

2.3. Propulsion of the impactor

The impactor shall be secured to a carriage (movable barrier).

2.4. Provisions for a movable barrier test

- 2.4.1. If the impactor is secured to a carriage (movable barrier) by a restraining element, the latter must be rigid and be incapable of being deformed by the impact; the carriage shall at the moment of impact be capable of moving freely and no longer be subject to the action of the propelling device.

- 2.4.2. The velocity of the impact shall be $50,0 \pm 2,0$ km/h.

- 2.4.3. The aggregate mass of carriage and impactor shall be $1\,100 \pm 20$ kg.

2.5. General provisions on the mass and velocity of the impactor

If the test has been conducted at an impact velocity higher than those prescribed in paragraph 2.4.2 and the vehicle has met the requirements prescribed, the test shall be considered satisfactory.

2.6. State of vehicle under test

2.6.1. The vehicle under test shall either be fitted with all the normal components and equipment included in its unladen mass or be in such condition as to fulfil this requirement so far as the components and equipment of concern to the passenger compartment and the distribution of the weight of the vehicle as a whole, in running order, are concerned.

2.6.2. The tank for liquid fuel shall be filled to at least 90 per cent of its capacity either with fuel or with a non-flammable liquid having a density and a viscosity close to those of the fuel normally used. All other systems (brake-fluid header tanks, radiator, Selective Catalytic Reduction reagents, etc.) may be empty.

The compressed hydrogen storage system(s) and enclosed spaces of compressed hydrogen-fuelled vehicles shall be prepared in accordance with paragraph 3 of Annex 4.

2.6.3 The parking brake is disengaged and the transmission/gear lever is in neutral.

2.6.4. If the manufacturer so requests, the following derogations shall be permitted:

2.6.4.1. The technical service responsible for conducting the test may allow the same vehicle as is used for test prescribed by other UN Regulations (including tests capable of affecting its structure) to be used for the tests prescribed by this Regulation.

2.6.4.2. The vehicle may be weighted to an extent not exceeding 10 per cent of its unladen mass with additional masses rigidly secured to the structure in such a way as not to affect the fuel system integrity and the safety of electric power train during the test.

2.6.5. Electric power train adjustment

2.6.5.1. The REESS shall be at any state of charge, which allows the normal operation of the power train as recommended by the manufacturer.

2.6.5.2. The electric power train shall be energized with or without the operation of the original electrical energy sources (e.g. engine-generator, REESS or electric energy conversion system), however:

2.6.5.2.1. By the agreement between Technical Service and manufacturer it shall be permissible to perform the test with all or parts of the electric power train not being energized insofar as there is no negative influence on the test result. For parts of the electric power train not energized, the protection against electrical shock shall be proved by either physical protection or isolation resistance and appropriate additional evidence.

2.6.5.2.2. In the case where an automatic disconnect is provided, at the request of the manufacturer, it shall be permissible to perform the test with the automatic disconnect being triggered. In this case it shall be demonstrated that the automatic disconnect would have operated during the impact test. This includes the automatic activation signal as well as the galvanic separation considering the conditions as seen during the impact.

2.7. Measuring Instruments

The instruments used to record the speed referred to in paragraph 2.4.2 above shall be accurate to within 1 per cent.

3. Alternative test methods

At the request of manufacturer, the following test method may be used as an alternative to the test method prescribed in paragraph 2 above.

3.1. An offset rear impact test with a movable deformable barrier is accepted as alternative to the procedure described in paragraph 2 of this annex if the conditions laid down in paragraphs 3.1.1 to 3.1.3 are fulfilled.

3.1.1. Impact speed

The impact speed shall be between 78,5 km/h and 80,1 km/h.

3.1.2. Offset vehicle to barrier

The overlap between car and barrier shall be 70 per cent.

3.1.3. Movable Deformable Barrier (MDB)

The movable deformable barrier shall meet following specifications:

- (a) The total weight of MDB with impact face shall be $1\,361 \pm 4,5$ kg;
- (b) The overall length of MDB with impact face shall be $4\,115 \text{ mm} \pm 25 \text{ mm}$;
- (c) The overall length of MDB excluding impact face shall be $3\,632 \text{ mm}$ (includes 50,8 mm thick mounting block);
- (d) The overall width of framework carriage shall be $1\,251 \text{ mm}$;
- (e) The tracking width (centreline to centreline of front or rear wheels) shall be $1\,880 \text{ mm}$;
- (f) The wheelbase for framework carriage shall be $2\,591 \text{ mm} \pm 25 \text{ mm}$;
- (g) Inertial properties of the MDB (with two cameras and camera mounts and a light trap vane and ballast reduced); the centre of gravity (CG) is as follows:

$X = (1\,123 \pm 25) \text{ mm}$ rear of front axle

$Y = (7,6 \pm 25) \text{ mm}$ left of longitudinal centreline

$Z = (450 \pm 25) \text{ mm}$ from ground

Moments of inertia (tolerance 5 per cent for testing purposes) are as follows:

Pitch = $2\,263 \text{ kg-m}^2$

Roll = 508 kg-m^2

Yaw = $2\,572 \text{ kg-m}^2$

(h) Shape of honeycomb impact face:

Width = $1\,676 \text{ mm} \pm 6 \text{ mm}$

Height = $559 \text{ mm} \pm 6 \text{ mm}$

Ground Clearance = $229 \text{ mm} \pm 3 \text{ mm}$

Depth at Bumper Height = $483 \text{ mm} \pm 6 \text{ mm}$

Depth at upper impact face = $381 \text{ mm} \pm 6 \text{ mm}$

- (i) Force-deflection properties (crush strength) for honeycomb impact face shall be $310 \text{ kPa} \pm 17 \text{ kPa}$ and $1\,690 \text{ kPa} \pm 103 \text{ kPa}$ for the bumper.

Other parameters and settings may be similar to the definitions in paragraph 2 of this Regulation.

3.2. If a method other than that described in paragraph 2 or paragraph 3.1 above is used, its equivalence shall be demonstrated.

ANNEX 4

Test conditions and procedures for the assessment of post-crash hydrogen fuel system integrity

1. Purpose

Determination of compliance with the requirements of paragraph 5.2.1 of this Regulation.

2. Definitions

For the purposes of this annex:

- 2.1. 'Enclosed spaces' indicates the special volumes within the vehicle (or the vehicle outline across openings) that are external to the hydrogen system (storage system, fuel cell system and fuel flow management system) and its housings (if any) where hydrogen may accumulate (and thereby pose a hazard), such as the passenger compartment, luggage compartment and space under the hood.
- 2.2. 'Luggage compartment' is the space in the vehicle for luggage and/or goods accommodation, bounded by the roof, hood, floor, side walls, being separated from the passenger compartment by the front bulkhead or the rear bulkhead.
- 2.3. 'Nominal working pressure (NWP)' is the gauge pressure that characterizes typical operation of a system. For compressed hydrogen gas containers, NWP is the settled pressure of compressed gas in a fully fuelled container or storage system at a uniform temperature of 15 °C.

3. Preparation, instrumentation and test conditions

3.1. Compressed hydrogen storage systems and downstream piping

- 3.1.1. Prior to conducting the crash test, instrumentation is installed in the hydrogen storage system to perform the required pressure and temperature measurements if the standard vehicle does not already possess instrumentation with the required accuracy.
- 3.1.2. The hydrogen storage system is then purged, if necessary, following manufacturer directions to remove impurities from the container before filling the storage system with compressed hydrogen or helium gas. Since the storage system pressure varies with temperature, the targeted fill pressure is a function of the temperature. The target pressure shall be determined from the following equation:

$$P_{\text{target}} = \text{NWP} \times (273 + T_o) / 288$$

where NWP is the nominal working pressure (MPa), T_o is the ambient temperature to which the storage system is expected to settle, and P_{target} is the targeted fill pressure after the temperature settles.

- 3.1.3. The container is filled to a minimum of 95 per cent of the targeted fill pressure and allowed to settle (stabilize) prior to conducting the crash test.
- 3.1.4. The main stop valve and shut-off valves for hydrogen gas, located in the downstream hydrogen gas piping, are in normal driving condition immediately prior to the impact.

3.2. Enclosed spaces

- 3.2.1. Sensors are selected to measure either the build-up of the hydrogen or helium gas or the reduction in oxygen (due to displacement of air by leaking hydrogen/helium).

3.2.2. Sensors are calibrated to traceable references to ensure an accuracy of ± 5 per cent at the targeted criteria of 4 per cent hydrogen or 3 per cent helium by volume in air, and a full scale measurement capability of at least 25 per cent above the target criteria. The sensor shall be capable of a 90 per cent response to a full scale change in concentration within 10 seconds.

3.2.3. Prior to the crash impact, the sensors are located in the passenger and luggage compartments of the vehicle as follows:

- (a) At a distance within 250 mm of the headliner above the driver's seat or near the top centre of the passenger compartment;
- (b) At a distance within 250 mm of the floor in front of the rear (or rear most) seat in the passenger compartment; and
- (c) At a distance within 100 mm of the top of luggage compartments inside the vehicle that are not directly affected by the particular crash impact to be conducted.

3.2.4. The sensors are securely mounted on the vehicle structure or seats and protected for the planned crash test from debris, air bag exhaust gas and projectiles. The measurements following the crash are recorded by instruments located in the vehicle or by remote transmission.

3.2.5. The test may be conducted either outdoors in an area protected from the wind and possible solar effects, or indoors in a space that is large enough or ventilated to prevent the build-up of hydrogen to more than 10 per cent of the targeted criteria in the passenger and luggage compartments.

4. Post-crash leak test measurement for a compressed hydrogen storage system filled with compressed hydrogen

4.1. The hydrogen gas pressure, P_0 (MPa), and temperature, T_0 (°C), are measured immediately before the impact and then at a time interval, Δt (min), after the impact.

4.1.1. The time interval, Δt , starts when the vehicle comes to rest after the impact and continues for at least 60 minutes.

4.1.2. The time interval, Δt shall be increased if necessary in order to accommodate measurement accuracy for a storage system with a large volume operating up to 70 MPa; in that case, Δt can be calculated from the following formula:

$$\Delta t = V_{\text{CHSS}} \times \text{NWP} / 1\,000 \times ((-0,027 \times \text{NWP} + 4) \times R_s - 0,21) - 1,7 \times R_s$$

where $R_s = P_s / \text{NWP}$, P_s is the pressure range of the pressure sensor (MPa), NWP is the Nominal Working Pressure (MPa), V_{CHSS} is the volume of the compressed hydrogen storage system (L), and Δt is the time interval (min).

4.1.3. If the calculated value of Δt is less than 60 minutes, Δt is set to 60 minutes.

4.2. The initial mass of hydrogen in the storage system can be calculated as follows:

$$P_o' = P_o \times 288 / (273 + T_o)$$

$$\rho_o' = -0,0027 \times (P_o')^2 + 0,75 \times P_o' + 0,5789$$

$$M_o = \rho_o' \times V_{\text{CHSS}}$$

4.3. Correspondingly, the final mass of hydrogen in the storage system, M_f , at the end of the time interval, Δt , can be calculated as follows:

$$P_f' = P_f \times 288 / (273 + T_f)$$

$$\rho_f' = -0,0027 \times (P_f')^2 + 0,75 \times P_f' + 0,5789$$

$$M_f = \rho_f' \times V_{\text{CHSS}}$$

where P_f is the measured final pressure (MPa) at the end of the time interval, and T_f is the measured final temperature (°C).

- 4.4. The average hydrogen flow rate over the time interval is therefore:

$$V_{H_2} = (M_f - M_o) / \Delta t \times 22,41 / 2,016 \times (P_{\text{target}} / P_o)$$

where V_{H_2} is the average volumetric flow rate (NL/min) over the time interval and the term (P_{target}/P_o) is used to compensate for differences between the measured initial pressure (P_o) and the targeted fill pressure (P_{target}).

5. Post-crash leak test measurement for a compressed hydrogen storage system filled with compressed helium
- 5.1. The helium gas pressure, P_o (MPa), and temperature T_o (°C), are measured immediately before the impact and then at a predetermined time interval after the impact.
- 5.1.1. The time interval, Δt , starts when the vehicle comes to rest after the impact and continues for at least 60 minutes.
- 5.1.2. The time interval, Δt , shall be increased, if necessary, in order to accommodate measurement accuracy for a storage system with a large volume operating up to 70 MPa; in that case, Δt can be calculated from the following equation:

$$\Delta t = V_{\text{CHSS}} \times \text{NWP} / 1\,000 \times ((-0,028 \times \text{NWP} + 5,5) \times R_s - 0,3) - 2,6 \times R_s$$

where $R_s = P_s / \text{NWP}$, P_s is the pressure range of the pressure sensor (MPa), NWP is the Nominal Working Pressure (MPa), V_{CHSS} is the volume of the compressed hydrogen storage system (L), and Δt is the time interval (min).

- 5.1.3. If the value of Δt is less than 60 minutes, Δt is set to 60 minutes.
- 5.2. The initial mass of helium in the storage system is calculated as follows:

$$P_o' = P_o \times 288 / (273 + T_o)$$

$$\rho_o' = -0,0043 \times (P_o')^2 + 1,53 \times P_o' + 1,49$$

$$M_o = \rho_o' \times V_{\text{CHSS}}$$

- 5.3. The final mass of helium in the storage system at the end of the time interval, Δt , is calculated as follows:

$$P_f' = P_f \times 288 / (273 + T_f)$$

$$\rho_f' = -0,0043 \times (P_f')^2 + 1,53 \times P_f' + 1,49$$

$$M_f = \rho_f' \times V_{\text{CHSS}}$$

where P_f is the measured final pressure (MPa) at the end of the time interval, and T_f is the measured final temperature (°C).

- 5.4. The average helium flow rate over the time interval is therefore:

$$V_{\text{He}} = (M_f - M_o) / \Delta t \times 22,41 / 4,003 \times (P_{\text{target}} / P_o)$$

where V_{He} is the average volumetric flow rate (NL/min) over the time interval and the term (P_{target}/P_o) is used to compensate for differences between the measured initial pressure (P_o) and the targeted fill pressure (P_{target}).

- 5.5. Conversion of the average volumetric flow of helium to the average hydrogen flow is calculated with the following formula:

$$V_{H_2} = V_{\text{He}} / 0,75$$

where V_{H_2} is the corresponding average volumetric flow of hydrogen.

6. Post-crash concentration measurement for enclosed spaces
 - 6.1. Post-crash data collection in enclosed spaces commences when the vehicle comes to a rest. Data from the sensors installed in accordance with paragraph 3.2 of this annex are collected at least every 5 seconds and continue for a period of 60 minutes after the test. A first-order lag (time constant) up to a maximum of 5 seconds may be applied to the measurements to provide 'smoothing' and filter the effects of spurious data points.
-

ANNEX 5

Test procedures for the vehicles equipped with electric power train

This annex describes test procedures to demonstrate compliance to the electrical safety requirements of paragraph 5.2.2 of this Regulation.

1. Test setup and equipment

If a high voltage disconnect function is used, measurements are to be taken from both sides of the device performing the disconnect function. However, if the high voltage disconnect is integral to the REESS or the energy conversion system and the high-voltage bus of the REESS or the energy conversion system is protected according to protection degree IPXXB following the impact test, measurements may only be taken between the device performing the disconnect function and the electrical loads.

The voltmeter used in this test shall measure DC values and have an internal resistance of at least 10 MΩ.

2. The following instructions may be used if voltage is measured.

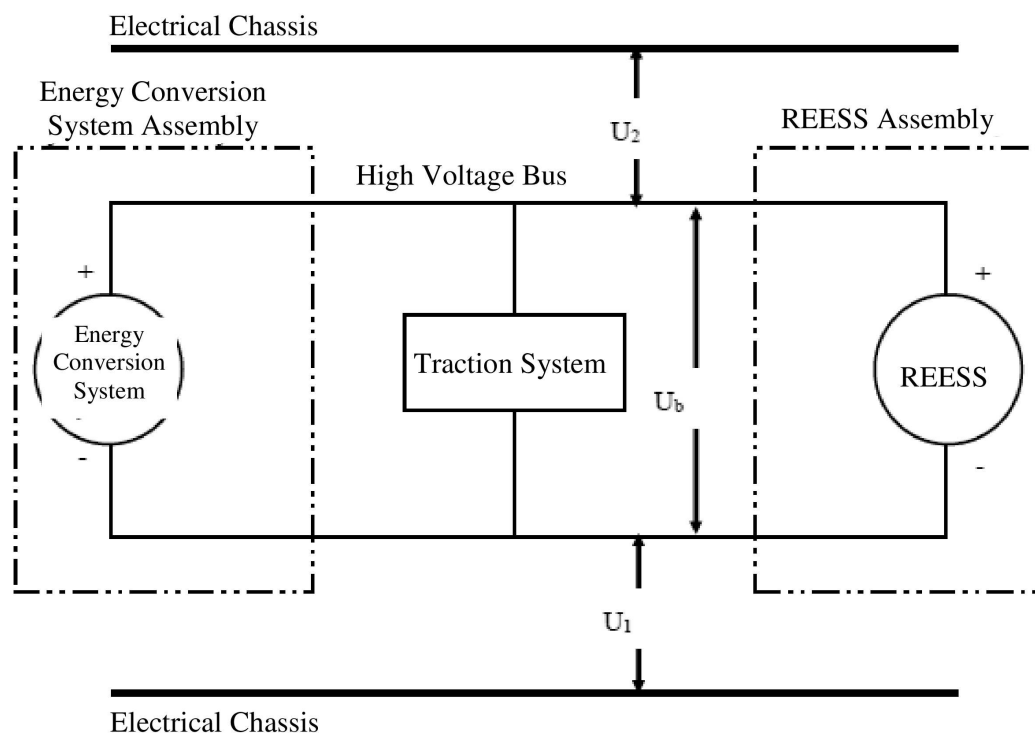
After the impact test, determine the high voltage bus voltages (U_b , U_1 , U_2) (see Figure 1 below).

The voltage measurement shall be made not earlier than 10 seconds, but, not later than 60 seconds after the impact.

This procedure is not applicable if the test is performed under the condition where the electric power train is not energized.

Figure 1

Measurement of U_b , U_1 , U_2



3. Assessment procedure for low electrical energy

Prior to the impact a switch S1 and a known discharge resistor Re is connected in parallel to the relevant capacitance (ref. Figure 2 below).

- (a) Not earlier than 10 seconds and not later than 60 seconds after the impact the switch S1 shall be closed while the voltage U_b and the current I_e are measured and recorded. The product of the voltage U_b and the current I_e shall be integrated over the period of time, starting from the moment when the switch S1 is closed (t_c) until the voltage U_b falls below the high voltage threshold of 60 V DC (t_h). The resulting integration equals the Total Energy (TE) in joules.

$$TE = \int_{t_c}^{t_h} U_b \times I_e dt$$

- (b) When U_b is measured at a point in time between 10 seconds and 60 seconds after the impact and the capacitance of the X-capacitors (C_x) is specified by the manufacturer, Total Energy (TE) shall be calculated according to the following formula:

$$TE = 0,5 \times C_x \times U_b^2$$

- (c) When U_1 and U_2 (see Figure 1 above) are measured at a point in time between 10 seconds and 60 seconds after the impact and the capacitances of the Y-capacitors (C_{y1} , C_{y2}) are specified by the manufacturer, Total Energy (TE_{y1} , TE_{y2}) shall be calculated according to the following formulas:

$$TE_{y1} = 0,5 \times C_{y1} \times U_1^2$$

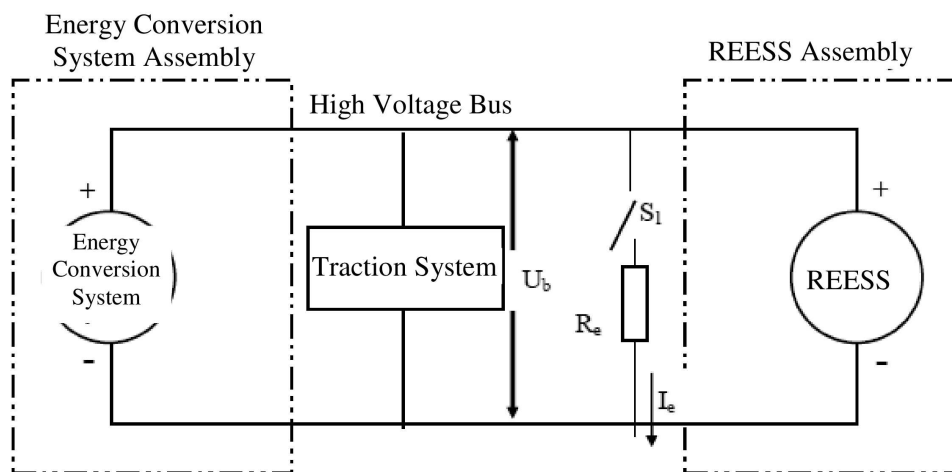
$$TE_{y2} = 0,5 \times C_{y2} \times U_2^2$$

This procedure is not applicable if the test is performed under the condition where the electric power train is not energized.

Figure 2

e.g. measurement of high voltage bus energy stored in X-capacitors

Electrical Chassis



Electrical Chassis

4. Physical protection

Following the vehicle impact test any parts surrounding the high voltage components shall be, without the use of tools, opened, disassembled or removed. All remaining surrounding parts shall be considered part of the physical protection.

The jointed test finger described in Figure 3 shall be inserted into any gaps or openings of the physical protection with a test force of $10\text{ N} \pm 10\text{ per cent}$ for electrical safety assessment. If partial or full penetration into the physical protection by the jointed test finger occurs, the jointed test finger shall be placed in every position as specified below.

Starting from the straight position, both joints of the test finger shall be rotated progressively through an angle of up to 90° with respect to the axis of the adjoining section of the finger and shall be placed in every possible position.

Internal electrical protection barriers are considered part of the enclosure.

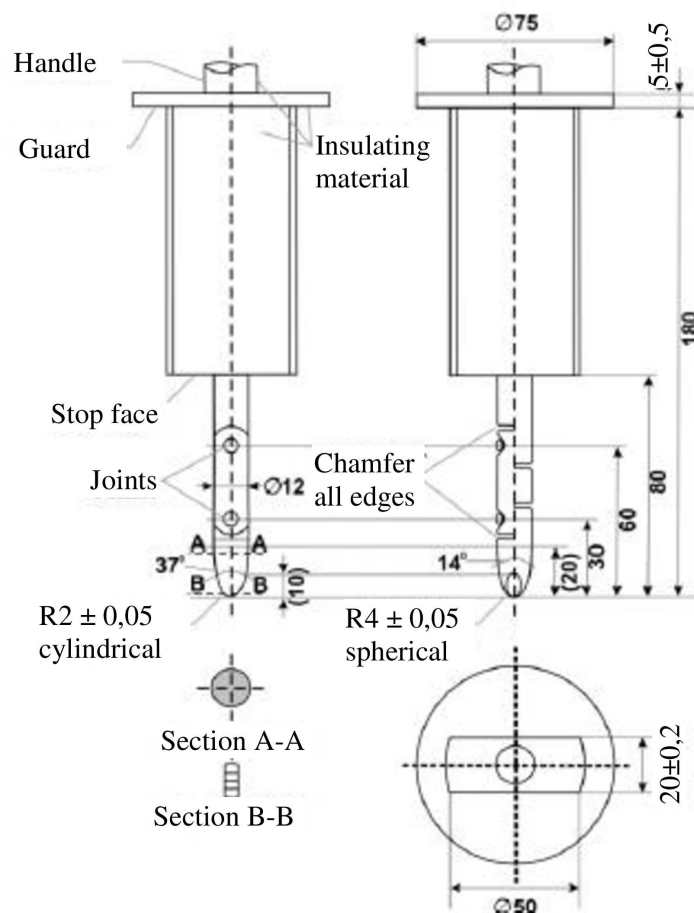
If appropriate a low-voltage supply (of not less than 40 V and not more than 50 V) in series with a suitable lamp should be connected, between the jointed test finger and high voltage live parts inside the electrical protection barrier or enclosure.

Figure 3

Joint Test Finger

IPXXB

Jointed test finger



Material: metal, except where otherwise specified

Linear dimensions in mm.

Tolerances on dimensions without specific tolerance:

(a) On angles: $+ 0^{\circ}0'0''/- 0^{\circ}0'10''$;

(b) On linear dimensions:

(i) ≤ 25 mm: $+ 0/- 0,05$ mm;

(ii) > 25 mm: $\pm 0,2$ mm

Both joints shall permit movement in the same plane and the same direction through an angle of 90° with a 0 to $+ 10^{\circ}$ tolerance.

The requirements of paragraph 5.2.2.1.3 of this Regulation are met if the jointed test finger described in Figure 3, is unable to contact high voltage live parts.

If necessary, a mirror or a fiberscope may be used to inspect whether the jointed test finger touches the high voltage buses.

If this requirement is verified by a signal circuit between the jointed test finger and high voltage live parts, the lamp shall not light.

4.1. Test method for measuring electric resistance:

(a) Test method using a resistance tester.

The resistance tester is connected to the measuring points (typically, the electrical chassis and electro conductive enclosure/electrical protection barrier) and the resistance is measured using a resistance tester that meets the specification that follows:

(i) Resistance tester: Measurement current at least $0,2$ A;

(ii) Resolution: $0,01 \Omega$ or less;

(iii) The resistance R shall be less than $0,1 \Omega$.

(b) Test method using DC power supply, voltmeter and ammeter.

The DC power supply, voltmeter and ammeter are connected to the measuring points (Typically, electrical chassis and electro conductive enclosure/electrical protection barrier).

The voltage of the DC power supply is adjusted so that the current flow becomes at least $0,2$ A.

The current 'I' and the voltage 'U' are measured.

The resistance 'R' is calculated according to the following formula:

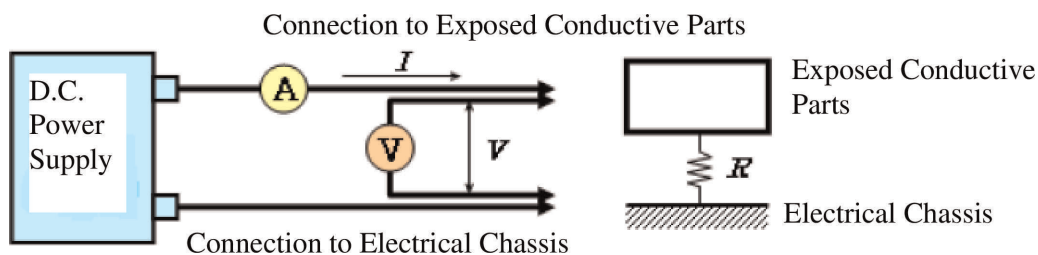
$$R = U / I$$

The resistance R shall be less than $0,1 \Omega$.

Note: If lead wires are used for voltage and current measurement, each lead wire shall be independently connected to the electrical protection barrier/enclosure/electrical chassis. Terminal can be common for voltage measurement and current measurement.

Example of the test method using DC power supply, voltmeter and ammeter is shown below.

Figure 4

Example of test method using DC power supply

5. Isolation resistance

5.1. General

The isolation resistance for each high voltage bus of the vehicle is measured or shall be determined by calculating the measurement values of each part or component unit of a high voltage bus.

All measurements for calculating voltage(s) and electrical isolation are made after a minimum of 10 s after the impact.

5.2. Measurement method.

The isolation resistance measurement is conducted by selecting an appropriate measurement method from among those listed in paragraphs 5.2.1 to 5.2.2 of this annex, depending on the electrical charge of the live parts or the isolation resistance.

The range of the electrical circuit to be measured is clarified in advance, using electrical circuit diagrams. If the high voltage buses are conductively isolated from each other, isolation resistance shall be measured for each electrical circuit.

Moreover, modifications necessary for measuring the isolation resistance may be carried out, such as removal of the cover in order to reach the live parts, drawing of measurement lines and change in software.

In cases where the measured values are not stable due to the operation of the on-board isolation resistance monitoring system, necessary modifications for conducting the measurement may be carried out by stopping the operation of the device concerned or by removing it. Furthermore, when the device is removed, a set of drawings will be used to prove that the isolation resistance between the live parts and the electrical chassis remains unchanged.

These modifications shall not influence the test results.

Utmost care shall be exercised to avoid short circuit and electric shock since this confirmation might require direct operations of the high-voltage circuit.

5.2.1. Measurement method using DC voltage from external sources.

5.2.1.1. Measurement instrument.

An isolation resistance test instrument capable of applying a DC voltage higher than the working voltage of the high voltage bus shall be used.

5.2.1.2. Measurement method.

An isolation resistance test instrument is connected between the live parts and the electrical chassis. The isolation resistance is subsequently measured by applying a DC voltage at least half of the working voltage of the high voltage bus.

If the system has several voltage ranges (e.g. because of boost converter) in conductively connected circuit and some of the components cannot withstand the working voltage of the entire circuit, the isolation resistance between those components and the electrical chassis can be measured separately by applying at least half of their own working voltage with those components disconnected.

5.2.2. Measurement method using the vehicle's own REESS as DC voltage source.

5.2.2.1. Test vehicle conditions.

The high voltage-bus is energized by the vehicle's own REESS and/or energy conversion system and the voltage level of the REESS and/or energy conversion system throughout the test shall be at least the nominal operating voltage as specified by the vehicle manufacturer.

5.2.2.2. Measurement method.

5.2.2.2.1. First step.

The voltage is measured as shown in Figure 1 and the high voltage bus voltage (U_b) is recorded.

5.2.2.2.2. Second step.

The voltage (U_1) between the negative side of the high voltage bus and the electrical chassis is measured and recorded (see Figure 1).

5.2.2.2.3. Third step.

The voltage (U_2) between the positive side of the high voltage bus and the electrical chassis is measured and recorded (see Figure 1).

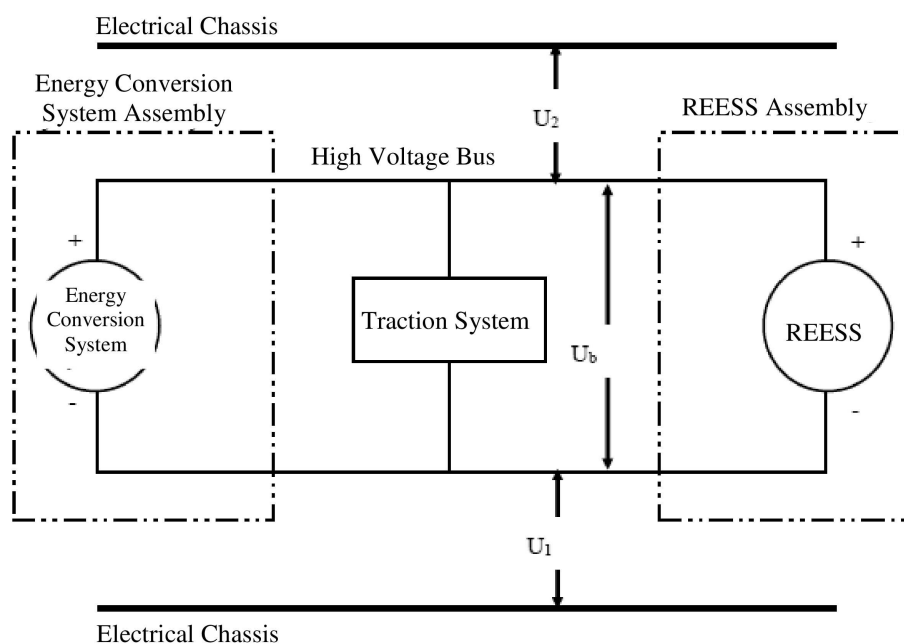
5.2.2.2.4. Fourth step.

If U_1 is greater than or equal to U_2 , a standard known resistance (R_0) is inserted between the negative side of the high voltage bus and the electrical chassis. With R_0 installed, the voltage (U_1') between the negative side of the high voltage bus and the electrical chassis is measured (see Figure 5).

The electrical isolation (R_i) is calculated according to the following formula:

$$R_i = R_0 * U_b * (1/U_1' - 1/U_1)$$

Figure 5

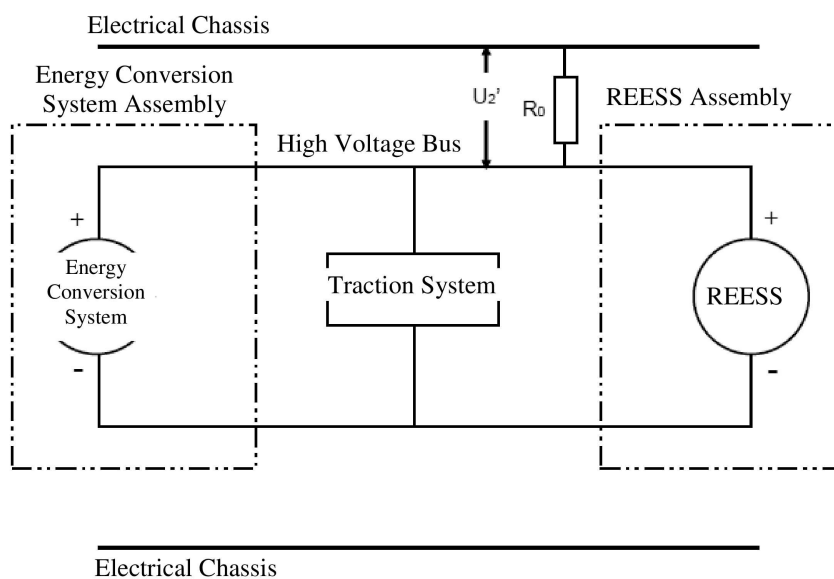
Measurement of U_1' 

If U_2 is greater than U_1 , insert a standard known resistance (R_0) between the positive side of the high voltage bus and the electrical chassis. With R_0 installed, measure the voltage (U_2') between the positive side of the high voltage bus and the electrical chassis (see Figure 6).

The electrical isolation (R_i) is calculated according to the following formula:

$$R_i = R_0 \cdot U_b \cdot (1/U_2' - 1/U_2)$$

Figure 6

Measurement of U_2' 

5.2.2.2.5. Fifth step.

The electrical isolation value R_i (in Ω) divided by the working voltage of the high voltage bus (in V) results in the isolation resistance (in Ω/V).

Note: The standard known resistance R_0 (in Ω) should be the value of the minimum required isolation resistance (Ω/V) multiplied by the working voltage (V) of the vehicle plus/minus 20 per cent. R_0 is not required to be precisely this value since the equations are valid for any R_0 ; however, a R_0 value in this range should provide a good resolution for the voltage measurements.

6. Electrolyte leakage

An appropriate coating, if necessary, may be applied to the physical protection (casing) in order to confirm if there is any electrolyte leakage from the REESS after the impact test.

7. REESS retention

Compliance shall be determined by visual inspection.

Only the original UN/ECE texts have legal effect under international public law. The status and date of entry into force of this Regulation should be checked in the latest version of the UN/ECE status document

TRANS/WP.29/343, available at:

<http://www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29docstts.html>

UN Regulation No 155 – Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system [2021/387]

Date of entry into force: 22 January 2021

This document is meant purely as documentation tool. The authentic and legally binding texts are:

- ECE/TRANS/WP.29/2020/79
- ECE/TRANS/WP.29/2020/94 and
- ECE/TRANS/WP.29/2020/97

CONTENTS

REGULATION

1. Scope
2. Definitions
3. Application for approval
4. Markings
5. Approval
6. Certificate of Compliance for Cybersecurity Management System
7. Specifications
8. Modification of vehicle type and extension of type approval
9. Conformity of production
10. Penalties for non-conformity of production
11. Production definitively discontinued
12. Names and addresses of Technical Services responsible for conducting approval test, and of Type Approval Authorities

ANNEXES

- 1 Information document
- 2 Communication
- 3 Arrangement of approval mark
- 4 Model of Certificate of Compliance for CSMS
- 5 List of threats and corresponding mitigations

1. SCOPE

- 1.1. This Regulation applies to vehicles, with regard to cybersecurity, 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 L₆ and L₇ 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 cybersecurity.
- 2.2. 'Cybersecurity' means the condition in which road vehicles and their functions are protected from cyber threats to electrical or electronic components.
- 2.3. 'Cybersecurity 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 cyberattacks.
- 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 cybersecurity 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 cybersecurity, 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 cybersecurity measures in the design of the vehicle type;
 - (d) Detect and respond to possible cybersecurity attacks;
 - (e) Log data to support the detection of cyberattacks and provide data forensic capability to enable analysis of attempted or successful cyberattacks.
- 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 cybersecurity 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 cybersecurity 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 cybersecurity where the Approval Authority or Technical Service has not received sufficient information from the vehicle manufacturer to assess the cybersecurity 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 cybersecurity aspects as covered by this Regulation.
- 5.3.1. The Approval Authority and its Technical Services shall ensure, in addition to the criteria laid down in Schedule 2 of the 1958 Agreement that they have:
- (a) Competent personnel with appropriate cybersecurity skills and specific automotive risk assessments knowledge ⁽¹⁾;
 - (b) Implemented procedures for the uniform evaluation according to this Regulation.

⁽¹⁾ E.g. ISO 26262-2018, ISO/PAS 21448, ISO/SAE 21434.

- 5.3.2. Each Contracting Party applying this Regulation shall notify and inform by its Approval Authority other Approval Authorities of the Contracting Parties applying this UN Regulation about the method and criteria taken as a basis by the notifying Authority to assess the appropriateness of the measures taken in accordance with this regulation and in particular with paragraphs 5.1, 7.2 and 7.3.

This information shall be shared (a) only before granting an approval according to this Regulation for the first time; and (b) each time the method or criteria for assessment is updated.

This information is intended to be shared for the purposes of collection and analysis of the best practices and in view of ensuring the convergent application of this Regulation by all Approval Authorities applying this Regulation.

- 5.3.3. The information referred to in paragraph 5.3.2 shall be uploaded in English language to the secure internet database 'DETA' ⁽²⁾, established by the United Nations Economic Commission for Europe, in due time and no later than 14 days before an approval is granted for the first time under the methods and criteria of assessment concerned. The information shall be sufficient to understand what minimum performance levels the Approval Authority adopted for each specific requirement referred to in paragraph 5.3.2 as well as the processes and measures it applies to verify that these minimum performance levels are met ⁽³⁾.
- 5.3.4. Approval Authorities receiving the information referred to in paragraph 5.3.2 may submit comments to the notifying Approval Authority by uploading them to DETA within 14 days after the day of notification.
- 5.3.5. If it is not possible for the granting Approval Authority to take into account the comments received in accordance with paragraph 5.3.4, the Approval Authorities having sent comments and the granting Approval Authority shall seek further clarification in accordance with Schedule 6 to the 1958 Agreement. The relevant subsidiary Working Party ⁽⁴⁾ of the World Forum for Harmonization of Vehicle Regulations (WP.29) for this Regulation shall agree on a common interpretation of methods and criteria of assessment ⁽⁵⁾. That common interpretation shall be implemented and all Approval Authorities shall issue type approvals under this Regulation accordingly.
- 5.3.6. Each Approval Authority granting a type approval pursuant to this Regulation shall notify other Approval Authorities of the approval granted. The type approval together with the supplementing documentation shall be uploaded in English language by the Approval Authority within 14 days after the day of granting the approval to DETA ⁽⁶⁾.
- 5.3.7. The Contracting Parties may study the approvals granted based on the information uploaded according to paragraph 5.3.6. In case of any diverging views between Contracting Parties this shall be settled in accordance with Article 10 and Schedule 6 of the 1958 Agreement. The Contracting Parties shall also inform the relevant subsidiary Working Party of the World Forum for Harmonization of Vehicle Regulations (WP.29) of the diverging interpretations within the meaning of Schedule 6 to the 1958 Agreement. The relevant Working Party shall support the settlement of the diverging views and may consult with WP.29 on this if needed.
- 5.4. For the purpose of paragraph 7.2 of this Regulation, the manufacturer shall ensure that the cybersecurity aspects covered by this Regulation are implemented.

⁽²⁾ <https://www.unece.org/trans/main/wp29/datasharing.html>

⁽³⁾ Guidance for the detailed information (e.g. method, criteria, performance level) to be uploaded and the format shall be given in the interpretation document which is under preparation by the Task Force on Cybersecurity and Over-the-Air issues for the seventh session of GRVA.

⁽⁴⁾ The Working Party on Automated/Autonomous and Connected Vehicles (GRVA).

⁽⁵⁾ This interpretation shall be reflected in the interpretation document referred to in the footnote to paragraph 5.3.3.

⁽⁶⁾ Further information on the minimum requirements for the documentation package will be developed by GRVA during its seventh session.

6. CERTIFICATE OF COMPLIANCE FOR CYBERSECURITY 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 Cybersecurity 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 Cybersecurity 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 cybersecurity 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. In due time, permitting the Approval Authority to complete its assessment before the end of the period of validity of the Certificate of Compliance for CSMS, the manufacturer shall apply for a new or for the extension of the existing Certificate of Compliance for CSMS. The Approval Authority shall, subject to 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 verify that the CSMS continue to comply with the requirements of this Regulation. 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, which may include the withdrawal of the approval if the conditions for granting the approval are not met anymore.

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 Cybersecurity Management System

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

7.2.2. The Cybersecurity 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 Cybersecurity 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 Cybersecurity 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 cybersecurity;
- (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 cybersecurity 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 cyberattacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cybersecurity 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 cyberattacks.

7.2.2.3. The vehicle manufacturer shall demonstrate that the processes used within their Cybersecurity 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 Cybersecurity 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 cyberattacks 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 Cybersecurity 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 Cybersecurity 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 cybersecurity 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 cyberattacks against vehicles of the vehicle type;
- (b) Support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyberattacks relevant to the vehicle type;
- (c) Provide data forensic capability to enable analysis of attempted or successful cyberattacks.

- 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 cyberattacks. The vehicle manufacturer shall also report and confirm to the Approval Authority or the Technical Service that the cybersecurity 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 OF VEHICLE TYPE AND EXTENSION OF TYPE APPROVAL

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. Proceed to necessary complementary assessment pursuant to paragraph 5, and require, where relevant, 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 DEFINITELY 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. Cybersecurity
 - 9.1. General construction characteristics of the vehicle type, including:
 - (a) The vehicle systems which are relevant to the cybersecurity of the vehicle type;
 - (b) The components of those systems that are relevant to cybersecurity;
 - (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 cybersecurity 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 cybersecurity:
-

Appendix 1 to Annex 1

Model of Manufacturer's Declaration of Compliance for CSMS

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

Manufacturer Name:

Manufacturer Address:

..... (*Manufacturer Name*) attests that the necessary processes to comply with the requirements for the Cybersecurity Management System laid down in paragraph 7.2 of UN Regulation 155 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 × 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 155

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 cybersecurity 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).

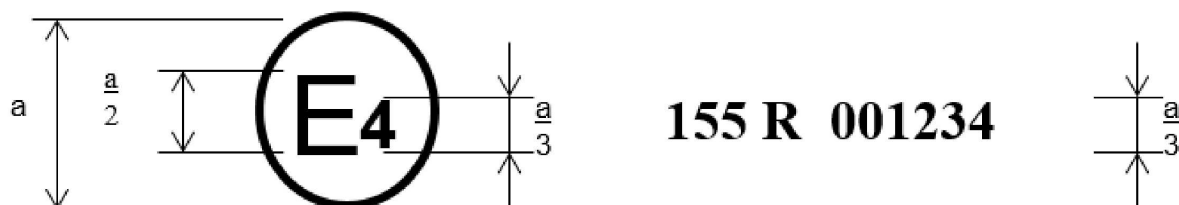
(²) Strike out what does not apply.

ANNEX 3

Arrangement of approval mark

MODEL A

(See paragraph 4.2 of this Regulation)

 $a = 8 \text{ mm min.}$

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 155, 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 Cybersecurity Management System

with UN Regulation No 155

Certificate Number [*Reference number*][..... *Approval Authority*]

Certifies that

Manufacturer:

Address of the manufacturer:

complies with the provisions of paragraph 7.2 of Regulation No 155

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 Cybersecurity 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 back-ends.
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

High-level and sub-level descriptions of vulnerability/ threat			Example of vulnerability or attack method	
4.3.2. Threats to vehicles regarding their communication channels	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	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 vulnerable to session hijacking/replay attacks	6.1	Accepting information from an unreliable or untrusted source
			6.2	Man in the middle attack/ session hijacking
			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

High-level and sub-level descriptions of vulnerability/ threat			Example of vulnerability or attack method	
	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

High-level and sub-level descriptions of vulnerability/ threat			Example of vulnerability or attack method	
			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 cyberattack	15	Legitimate actors are able to take actions that would unwittingly facilitate a cyberattack	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
4.3.5. Threats to vehicles regarding their external connectivity and connections	16	Manipulation of the connectivity of vehicle functions enables a cyberattack, 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)
	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

High-level and sub-level descriptions of vulnerability/ threat			Example of vulnerability or attack method	
	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
	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

High-level and sub-level descriptions of vulnerability/ threat			Example of vulnerability or attack method	
	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

Table A1 reference	Threats to 'Vehicle communication channels'	Ref	Mitigation
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
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		

Table A1 reference	Threats to 'Update process'	Ref	Mitigation
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 cyberattack'

Mitigations to the threats which are related to 'Unintended human actions facilitating a cyberattack' are listed in Table B3.

Table B3

Mitigations to the threats which are related to 'Unintended human actions facilitating a cyberattack'

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)		

Table A1 reference	Threats to 'External connectivity and connections'	Ref	Mitigation
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.

Table A1 reference	Threats to 'Potential targets of, or motivations for, an attack'	Ref	Mitigation
20.4	Data manipulation to falsify vehicle's driving data (e.g. mileage, driving speed, driving directions, etc.)		Data manipulation attacks on sensors or transmitted data could be mitigated by correlating the data from different sources of information
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

Table A1 reference	Threats to 'Potential vulnerabilities that could be exploited if not sufficiently protected or hardened'	Ref	Mitigation
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'

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)		

Only the original UN/ECE texts have legal effect under international public law. The status and date of entry into force of this Regulation should be checked in the latest version of the UN/ECE status document

TRANS/WP.29/343, available at:

<http://www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29docstts.html>

UN Regulation No 156 – Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system [2021/388]

Date of entry into force: 22 January 2021

This document is meant purely as documentation tool. The authentic and legally binding text is: ECE/TRANS/WP.29/2020/80.

CONTENTS

REGULATION

1. Scope
2. Definitions
3. Application for approval
4. Markings
5. Approval
6. Certificate of compliance for Software Update Management System
7. General specifications
8. Modification of vehicle type and extension of type approval
9. Conformity of production
10. Penalties for non-conformity of production
11. Production definitively discontinued
12. Names and addresses of Technical Services responsible for conducting approval tests and of Type Approval Authorities

ANNEXES

- 1 Information document
 - Appendix 1 – Model of declaration of compliance for Software Update Management System
- 2 Communication
- 3 Arrangement of approval mark
- 4 Model of Certificate of Compliance for Software Update Management System

1. SCOPE

- 1.1. This Regulation applies to vehicles of Categories ⁽¹⁾ 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.

⁽¹⁾ As defined in the Consolidated Resolution on the Construction of Vehicles (R.E.3.), document ECE/TRANS/WP.29/78/Rev.6, para. 2 - www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29resolutions.html

- 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 No 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.
- 5.1.1. The Approval Authority or the Technical Service shall verify by testing a vehicle of the vehicle type that the vehicle manufacturer has implemented the measures they have documented. Tests shall be performed by approval authority or the technical service itself or in collaboration with the vehicle manufacturer by sampling.
- 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.

^(*) The distinguishing numbers of the Contracting Parties to the 1958 Agreement are reproduced in Annex 3 to the Consolidated Resolution on the Construction of Vehicles (R.E.3), document ECE/TRANS/WP.29/78/Rev.6.

- 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 confirm the compatibility of a software update with the target vehicle(s) configuration before it is issued. This shall include an assessment of the last known software/hardware configuration of the target vehicle(s) for compatibility with the update before it is issued;
 - 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 the Technical Services. This may be for the purpose of type approval, conformity of production, market surveillance, recalls and Periodic Technical Inspection (PTI).
- 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 confirmation of the compatibility of the 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:
 - (a) 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;
 - (b) Any changes implemented by the update on vehicle functions;
 - (c) The expected time to complete execution of the update;
 - (d) Any vehicle functionalities which may not be available during the execution of the update;
 - (e) 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:
 - (a) Ensure the vehicle cannot be driven during the execution of the update;
 - (b) 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:

- (a) The vehicle user is able to be informed of the success (or failure) of the update;
- (b) 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. The vehicle shall ensure that preconditions have to be met before the software update is executed.

8. MODIFICATION OF VEHICLE TYPE AND EXTENSION OF TYPE APPROVAL

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 DEFINITELY 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.

*Appendix 1 to Annex 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 No 156 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 × 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 156

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 marking provisions (footnote) in this Regulation).

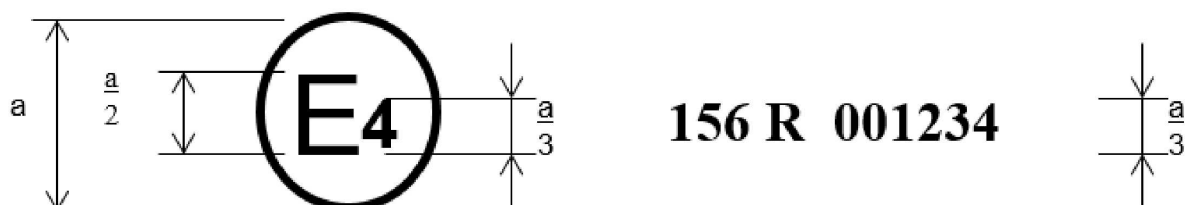
(²) Strike out what does not apply.

ANNEX 3

Arrangement of approval mark

MODEL A

(See paragraph 4.2 of this Regulation)

 $a = 8 \text{ mm min.}$

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 156, 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 156

Certificate Number [*Reference number*][..... *Approval Authority*]

Certifies that

Manufacturer:

Address of the manufacturer:

Complies with the provisions of Regulation No 156

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*]

Only the original UN/ECE texts have legal effect under international public law. The status and date of entry into force of this Regulation should be checked in the latest version of the UN/ECE status document

TRANS/WP.29/343, available at:

<http://www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29docstts.html>

UN Regulation No 157 – Uniform provisions concerning the approval of vehicles with regards to Automated Lane Keeping Systems [2021/389]

Date of entry into force: 22 January 2021

This document is meant purely as documentation tool. The authentic and legally binding text is: ECE/TRANS/WP.29/2020/81.

CONTENTS

REGULATION

Introduction

1. Scope and purpose
2. Definitions
3. Application for approval
4. Approval
5. System Safety and Fail-safe Response
6. Human-Machine Interface/Operator Information
7. Object and Event Detection and Response
8. Data Storage System for Automated Driving
9. Cybersecurity and Software Updates
10. Modification of vehicle type and extension of type approval
11. Conformity of production
12. Penalties for non-conformity of production
13. Production definitively discontinued
14. Names and addresses of Technical Services responsible for conducting approval tests and of Type Approval Authorities

ANNEXES

- 1 Communication
- 2 Arrangements of approval marks
- 3 (Reserved)
- 4 Special requirements to be applied to the safety aspects of electronic control systems and Audit
- 5 Test Specifications for ALKS

INTRODUCTION

The intention of the Regulation is to establish uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems (ALKS).

ALKS controls the lateral and longitudinal movement of the vehicle for extended periods without further driver command. ALKS is a system whereby the activated system is in primary control of the vehicle.

This Regulation is the first regulatory step for an automated driving system (as defined in ECE/TRANS/WP.29/1140) in traffic and it therefore provides innovative provisions aimed at addressing the complexity related to the evaluation of the system safety. It contains administrative provisions suitable for type approval, technical requirements, audit and reporting provisions and testing provisions.

ALKS can be activated under certain conditions on roads where pedestrians and cyclists are prohibited and which, by design, are equipped with a physical separation that divides the traffic moving in opposite directions and prevent traffic from cutting across the path of the vehicle. In a first step, the original text of this Regulation limits the operational speed to 60 km/h maximum and passenger cars (M₁ vehicles).

This Regulation includes general requirements regarding the system safety and the failsafe response. When the ALKS is activated, it shall perform the driving task instead of the driver, i.e. manage all situations including failures, and shall not endanger the safety of the vehicle occupants or any other road users. There is however always the possibility for the driver to override the system, at any time.

The Regulation also lays down requirements on how the driving task shall be safely handed over from the ALKS to the driver including the capability for the system to come to a stop in case the driver does not reply appropriately.

Finally, the Regulation includes requirements on the Human-Machine Interface (HMI) to prevent misunderstanding or misuse by the driver. The Regulation for instance requires that on-board displays used by the driver for other activities than driving when the ALKS is activated, shall be automatically suspended as soon as the system issues a transition demand. These measures are without prejudice to driver behaviour rules on how to use these systems in the Contracting Parties as currently being discussed by the Global Forum for Road Traffic Safety (WP.1) at the time of drafting this document (See e.g. Informal Document 4 Revision 1 of the seventy-eighth session of WP.1).

1. SCOPE AND PURPOSE

- 1.1. This Regulation applies to the type approval of vehicles of Category M₁ ⁽¹⁾ with regards to their Automated Lane Keeping System.

2. DEFINITIONS

For the purposes of this Regulation:

- 2.1. 'Automated Lane Keeping System (ALKS)' for low speed application is a system which is activated by the driver and which keeps the vehicle within its lane for travelling speed of 60 km/h or less by controlling the lateral and longitudinal movements of the vehicle for extended periods without the need for further driver input.

Within this Regulation, ALKS is also referred to as '*the system*'.

- 2.1.1. 'Vehicle Type with regard to Automated Lane Keeping System (ALKS)' means a category of vehicles which do not differ in such essential aspects as:

- (a) Vehicle features which significantly influence the performances of ALKS;
- (b) The system characteristics and design of ALKS.

- 2.2. 'Transition demand' is a logical and intuitive procedure to transfer the Dynamic Driving Task (DDT) from the system (automated control) to the human driver (manual control). This request is given from the system to the human driver.

⁽¹⁾ As defined in the Consolidated Resolution on the Construction of Vehicles (R.E.3.), document ECE/TRANS/WP.29/78/Rev.6, para. 2 – www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29resolutions.html

- 2.3. 'Transition phase' means the duration of the transition demand.
- 2.4. 'Planned event' is a situation which is known in advance, e.g. at the time of activation such as a journey point (e.g. exit of a highway) etc. and which requires a transition demand.
- 2.5. 'Unplanned event' is a situation which is unknown in advance, but assumed as very likely in happening, e.g. road construction, inclement weather, approaching emergency vehicle, missing lane marking, load falling from truck (collision) and which requires a transition demand.
- 2.6. 'Imminent collision risk' describes a situation or an event which leads to a collision of the vehicle with another road user or an obstacle which cannot be avoided by a braking demand with lower than 5 m/s².
- 2.7. 'Minimum Risk Manoeuvre (MRM)' means a procedure aimed at minimising risks in traffic, which is automatically performed by the system after a transition demand without driver response or in the case of a severe ALKS or vehicle failure.
- 2.8. 'Emergency Manoeuvre (EM)' is a manoeuvre performed by the system in case of an event in which the vehicle is at imminent collision risk and has the purpose of avoiding or mitigating a collision.
- 2.9. Speed
- 2.9.1. 'Specified maximum speed' is the speed declared by the manufacturer up to which the system operates under optimum conditions.
- 2.9.2. 'Maximum operational speed' is the speed selected by the system up to which the system operates under current environmental and sensor conditions. It is the maximum vehicle speed at which the system may be active and shall be determined by the capability of the sensing system as well as the environmental conditions.
- 2.9.3. 'Present speed' or 'speed' is the current speed selected by the system due to traffic.
- 2.10. 'Detection range' of the sensing system is the distance at which the system can reliably recognise a target, taking account of the deterioration of components of the sensing system due to time and usage throughout the lifetime of the vehicle and generate a control signal.
- 2.11. Failures
- 2.11.1. An 'ALKS failure' is any single failure specific to the operation of the ALKS (e.g. single sensor failure, loss of necessary calculation data for the driving path of the vehicle).
- 2.11.2. 'Failure mode' is the operation status of the system in which the system operates with an ALKS failure.
- 2.11.3. A 'severe ALKS failure' is a failure specific to the operation of the ALKS that affects the safe operation of the system when in failure mode with a very low probability of occurrence such as generally used for essential components as e.g. an electronic control unit. Single sensor failures are only considered as such when accompanied by another influence affecting the safe operation of the system.
- 2.11.4. A 'severe vehicle failure' is any failure of the vehicle (e.g. electrical, mechanical) that affects the ability of the ALKS to perform the DDT and would also affect the manual operation of the vehicle (e.g. loss of power supply, failure of the braking system, sudden loss of tyre pressure).

- 2.12. 'Self-check' means an integrated function which checks for any system failure and for the detection range of the sensing system on a continuous basis.
- 2.13. A 'system override' by the driver means a situation when the driver provides an input to a control which has priority over the longitudinal or lateral control of the system, while the system is still active.
- 2.14. 'Dynamic Driving Task (DDT)' is the control and execution of all longitudinal and lateral movements of the vehicle.
- 2.15. 'Data Storage System for Automated Driving (DSSAD)' enables the determination of interactions between the ALKS and the human driver.
- 2.16. 'Lifetime of the system' is the period of time during which the ALKS system is available, as a function, on the vehicle.
- 2.17. 'Occurrences' means, in the context of DSSAD provisions in paragraph 8, an action or instance of an arising event or incident, which requires storage within the data storage system.
- 2.18. 'R157 Software Identification Number (R₁₅₇ SWIN)' 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 UN Regulation No 157 type approval relevant characteristics of the vehicle.
- 2.19. 'Electronic control system' means a combination of units, designed to co-operate in the production of the stated automated lane keeping function by electronic data processing. Such systems, commonly controlled by software, are built from discrete functional components such as sensors, electronic control units and actuators and connected by transmission links. They may include mechanical, electro-pneumatic or electro-hydraulic elements.
- 2.20. 'Software' means the part of an Electronic Control System that consists of digital data and instructions.
3. APPLICATION FOR APPROVAL
- 3.1. The application for approval of a vehicle type with regard to the ALKS shall be submitted by the vehicle manufacturer or by the manufacturer's authorized representative.
- 3.2. It shall be accompanied by the documents mentioned below in triplicate:
- 3.2.1. A description of the vehicle type with regard to the items mentioned in paragraph 2.1.1, together with a documentation package as required in Annex 4 which gives access to the basic design of the ALKS and the means by which it is linked to other vehicle systems or by which it directly controls output variables. The numbers and/or symbols identifying the vehicle type shall be specified.
- 3.3. A vehicle representative of the vehicle type to be approved shall be submitted to the Technical Service conducting the approval tests.
4. APPROVAL
- 4.1. If the vehicle type submitted for approval pursuant to this Regulation meets the requirements of paragraph 5 to 9 below, approval of that vehicle shall be granted.

- 4.2. An approval number shall be assigned to each type approved; its first two digits (at present 00 corresponding to the 00 series of amendments, its original version) shall indicate the series of amendments incorporating the most recent major technical amendments made to the Regulation at the time of issue of the approval. The same Contracting Party shall not assign the same number to another vehicle type.
- 4.3. Notice of approval or of refusal or withdrawal of approval pursuant to this Regulation shall be communicated to the Parties to the Agreement which apply this Regulation by means of a form conforming to the model in Annex 1 and documentation supplied by the applicant being in a format not exceeding A4 (210 × 297 mm), or folded to that format, and on an appropriate scale or electronic format.
- 4.4. 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 conforming to the model described in Annex 2, consisting of:
- 4.4.1. A circle surrounding the letter 'E' followed by the distinguishing number of the country which has granted approval ⁽²⁾;
- 4.4.2. The number of this Regulation, followed by the letter 'R', a dash and the approval number to the right of the circle prescribed in paragraph 4.4.1 above.
- 4.5. 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 4.4.1 above need not be repeated; in such a case, the Regulation and approval numbers and the additional symbols shall be placed in vertical columns to the right of the symbol prescribed in paragraph 4.4.1 above.
- 4.6. The approval mark shall be clearly legible and be indelible.
- 4.7. The approval mark shall be placed close to or on the vehicle data plate.
5. SYSTEM SAFETY AND FAIL-SAFE RESPONSE
- 5.1. General Requirements
- The fulfilment of the provisions of this paragraph shall be demonstrated by the manufacturer to the technical service during the inspection of the safety approach as part of the assessment to Annex 4 (in particular for conditions not tested under Annex 5) and according to the relevant tests in Annex 5.
- 5.1.1. The activated system shall perform the DDT shall manage all situations including failures, and shall be free of unreasonable risks for the vehicle occupants or any other road users.
- The activated system shall not cause any collisions that are reasonably foreseeable and preventable. If a collision can be safely avoided without causing another one, it shall be avoided. When the vehicle is involved in a detectable collision, the vehicle shall be brought to a standstill.
- 5.1.2. The activated system shall comply with traffic rules relating to the DDT in the country of operation.
- 5.1.3. The activated system shall exercise control over systems required to support the driver in resuming manual control at any time (e.g. demist, windscreen wipers and lights).

⁽²⁾ The distinguishing numbers of the Contracting Parties to the 1958 Agreement are reproduced in Annex 3 to the Consolidated Resolution on the Construction of Vehicles (R.E.3), document ECE/TRANS/WP.29/78/Rev. 6 – www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29resolutions.html

- 5.1.4. A transition demand shall not endanger the safety of the vehicle occupants or other road users.
- 5.1.5. If the driver fails to resume control of the DDT during the transition phase, the system shall perform a minimum risk manoeuvre. During a minimum risk manoeuvre, the system shall minimise risks to safety of the vehicle occupants and other road users.
- 5.1.6. The system shall perform self-checks to detect the occurrence of failures and to confirm system performance at all times (e.g. after vehicle start the system has at least once detected an object at the same or a higher distance than that declared as detection range according to paragraph 7.1).
- 5.1.7. The effectiveness of the system shall not be adversely affected by magnetic or electrical fields. This shall be demonstrated by compliance with the 05 or later series of amendments to UN Regulation No 10.
- 5.1.8. The manufacturer shall take measures to guard against reasonably foreseeable misuse by the driver and tampering of the system.
- 5.1.9. When the system can no longer meet the requirements of this Regulation, it shall not be possible to activate the system.
- The manufacturer shall declare and implement a process to manage the safety and continued compliance of the ALKS system over lifetime.

5.2. Dynamic Driving Task

The fulfilment of the provisions of this paragraph shall be demonstrated by the manufacturer to the technical service during the inspection of the safety approach as part of the assessment to Annex 4 (in particular for conditions not tested under Annex 5) and according to the relevant tests in Annex 5.

- 5.2.1. The activated system shall keep the vehicle inside its lane of travel and ensure that the vehicle does not cross any lane marking (outer edge of the front tyre to outer edge of the lane marking). The system shall aim to keep the vehicle in a stable lateral position inside the lane of travel to avoid confusing other road users.
- 5.2.2. The activated system shall detect a vehicle driving beside as defined in paragraph 7.1.2 and, if necessary, adjust the speed and/or the lateral position of the vehicle within its lane as appropriate.
- 5.2.3. The activated system shall control the speed of the vehicle.
- 5.2.3.1. The maximum speed up to which the system is permitted to operate is 60 km/h.
- 5.2.3.2. The activated system shall adapt the vehicle speed to infrastructural and environmental conditions (e.g. narrow curve radii, inclement weather).
- 5.2.3.3. The activated system shall detect the distance to the next vehicle in front as defined in paragraph 7.1.1 and shall adapt the vehicle speed in order to avoid collision.

While the ALKS vehicle is not at standstill, the system shall adapt the speed to adjust the distance to a vehicle in front in the same lane to be equal or greater than the minimum following distance.

In case the minimum time gap cannot be respected temporarily because of other road users (e.g. vehicle is cutting in, decelerating lead vehicle, etc.), the vehicle shall readjust the minimum following distance at the next available opportunity without any harsh braking unless an emergency manoeuvre would become necessary.

The minimum following distance shall be calculated using the formula:

$$d_{\min} = v_{\text{ALKS}} * t_{\text{front}}$$

Where:

$d_{\min}$ = the minimum following distance

v_{ALKS} = the present speed of the ALKS vehicle in m/s

t_{front} = minimum time gap in seconds between the ALKS vehicle and a leading vehicle in front as per the table below:

<i>Present speed of the ALKS vehicle</i>		<i>Minimum time gap</i>	<i>Minimum following distance</i>
(km/h)	(m/s)	(s)	(m)
7,2	2,0	1,0	2,0
10	2,78	1,1	3,1
20	5,56	1,2	6,7
30	8,33	1,3	10,8
40	11,11	1,4	15,6
50	13,89	1,5	20,8
60	16,67	1,6	26,7

For speed values not mentioned in the table, linear interpolation shall be applied.

Notwithstanding the result of the formula above for present speeds below 2 m/s the minimum following distance shall never be less than 2 m.

- 5.2.4. The activated system shall be able to bring the vehicle to a complete stop behind a stationary vehicle, a stationary road user or a blocked lane of travel to avoid a collision. This shall be ensured up to the maximum operational speed of the system.
- 5.2.5. The activated system shall detect the risk of collision in particular with another road user ahead or beside the vehicle, due to a decelerating lead vehicle, a cutting in vehicle or a suddenly appearing obstacle and shall automatically perform appropriate manoeuvres to minimize risks to safety of the vehicle occupants and other road users.

For conditions not specified in paragraphs 5.2.4, 5.2.5 or its subparagraphs, this shall be ensured at least to the level at which a competent and careful human driver could minimize the risks. This shall be demonstrated in the assessment carried out under Annex 4 and by taking guidance from Appendix 3 to Annex 4.

- 5.2.5.1. The activated system shall avoid a collision with a leading vehicle which decelerates up to its full braking performance provided that there was no undercut of the minimum following distance the ALKS vehicle would adjust to a leading vehicle at the present speed due to a cut in manoeuvre of this lead vehicle.
- 5.2.5.2. The activated system shall avoid a collision with a cutting in vehicle:
- (a) Provided the cutting in vehicle maintains its longitudinal speed which is lower than the longitudinal speed of the ALKS vehicle; and
 - (b) Provided that the lateral movement of the cutting in vehicle has been visible for a time of at least 0,72 seconds before the reference point for $TTC_{\text{LaneIntrusion}}$ is reached;

- (c) When the distance between the vehicle's front and the cutting in vehicle's rear corresponds to a TTC calculated by the following equation:

$$TTC_{\text{LaneIntrusion}} > \frac{V_{\text{rel}}}{\left(2 \cdot \frac{6\text{m}}{\text{s}^2}\right)} + 0,35 \text{ s}$$

Where:

V_{rel} = relative velocity between both vehicles, positive for vehicle being faster than the cutting in vehicle

$TTC_{\text{LaneIntrusion}}$ = The TTC value, when the outside of the tyre of the intruding vehicle's front wheel closest to the lane markings crosses a line 0,3 m beyond the outside edge of the visible lane marking to which the intruding vehicle is being drifted.

- 5.2.5.3. The activated system shall avoid a collision with an unobstructed crossing pedestrian in front of the vehicle.

In a scenario with an unobstructed pedestrian crossing with a lateral speed component of not more than 5 km/h where the anticipated impact point is displaced by not more than 0,2 m compared to the vehicle longitudinal plane, the activated ALKS shall avoid a collision up to the maximum operational speed of the system.

- 5.2.5.4. It is recognised that the fulfilment of the requirement in paragraph 5.2.5 may not be fully achieved in other conditions than those described above. However, the system shall not deactivate or unreasonably switch the control strategy in these other conditions. This shall be demonstrated in accordance with Annex 4 of this Regulation.

5.3. Emergency Manoeuvre (EM)

The fulfilment of the provisions of this paragraph shall be demonstrated by the manufacturer to the technical service during the inspection of the safety approach as part of the assessment to Annex 4 and according to the relevant tests in Annex 5.

- 5.3.1. An Emergency Manoeuvre shall be carried out in case of an imminent collision risk.

- 5.3.1.1. Any longitudinal deceleration demand of more than 5,0 m/s² of the system shall be considered to be an EM.

- 5.3.2. This manoeuvre shall decelerate the vehicle up to its full braking performance if necessary and/or may perform an automatic evasive manoeuvre, when appropriate.

If failures are affecting the braking or steering performance of the system, the manoeuvre shall be carried out with consideration for the remaining performance.

During the evasive manoeuvre the ALKS vehicle shall not cross the lane marking (outer edge of the front tyre to outer edge of the lane marking).

After the evasive manoeuvre the vehicle shall aim at resuming a stable position.

- 5.3.3. An emergency manoeuvre shall not be terminated, unless the imminent collision risk disappeared, or the driver deactivated the system.

- 5.3.3.1. After an emergency manoeuvre is terminated the system shall continue to operate.

- 5.3.3.2. If the emergency manoeuvre results in the vehicle being at standstill, the signal to activate the hazard warning lights shall be generated. If the vehicle automatically drives off again, the signal to deactivate the hazard warning lights shall be generated automatically.

- 5.3.4. The vehicle shall implement a logic signal indicating emergency braking as specified in UN Regulation No 13-H.

5.4. Transition demand and system operation during transition phase

The fulfilment of the provisions of this paragraph shall be demonstrated by the manufacturer to the technical service during the inspection of the safety approach as part of the assessment to Annex 4 (in particular for conditions not tested under Annex 5) and according to the relevant tests in Annex 5.

5.4.1. The activated system shall recognise all situations in which it needs to transition the control back to the driver.

Types of situations in which the vehicle will generate a transition demand to the driver shall be declared by the vehicle manufacturer and included in the documentation package required in Annex 4.

5.4.2. The initiation of the transition demand shall be such that sufficient time is provided for a safe transition to manual driving.

5.4.2.1. In case of a planned event that would prevent the ALKS from continuing the operation, a transition demand shall be given early enough to ensure the minimal risk maneuver, in case the driver would not resume control, would bring the vehicle to standstill before the planned event occurs.

5.4.2.2. In case of an unplanned event, a transition demand shall be given upon detection.

5.4.2.3. In case of any failure affecting the operation of the system, the system shall immediately initiate a transition demand upon detection.

5.4.3. During the transition phase the system shall continue to operate. The system may reduce the speed of the vehicle to ensure its safe operation but shall not bring it to standstill unless required by the situation (e.g. due to vehicles or obstacles obstructing the path of the vehicle) or when caused by a haptic warning according to paragraph 6.4.1 started at speeds below 20 km/h.

5.4.3.1. Once in standstill the vehicle may remain in this condition and shall generate the signal to activate the hazard warning lights within 5 s.

5.4.3.2. During the transition phase, the transition demand shall be escalated latest after 4 s after the start of the transition demand.

5.4.4. A transition demand shall only be terminated once the system is deactivated or a minimum risk manoeuvre has started.

5.4.4.1. In case the driver is not responding to a transition demand by deactivating the system (either as described in paragraph 6.2.4 or 6.2.5), a minimum risk manoeuvre shall be started, earliest 10 s after the start of the transition demand.

5.4.4.1.1. Notwithstanding paragraph 5.4.4.1 a minimum risk manoeuvre may be initiated immediately in case of a severe ALKS or severe vehicle failure.

In case of a severe ALKS or vehicle failure the ALKS may no longer be capable of fulfilling the requirements of this Regulation, but it shall aim at enabling a safe transition of control back to the driver.

5.4.4.1.2. The manufacturer shall declare the types of severe vehicle failures and severe ALKS failures that will lead the ALKS to initiate a MRM immediately.

5.5. Minimum Risk Manoeuvre (MRM)

The fulfilment of the provisions of this paragraph shall be demonstrated by the manufacturer to the technical service during the inspection of the safety approach as part of the assessment to Annex 4 (in particular for conditions not tested under Annex 5) and according to the relevant tests in Annex 5.

- 5.5.1. During the minimum risk manoeuvre the vehicle shall be slowed down inside the lane or, in case the lane markings are not visible, remain on an appropriate trajectory taking into account surrounding traffic and road infrastructure, with an aim of achieving a deceleration demand not greater than 4,0 m/s².

Higher deceleration demand values are permissible for very short durations, e.g. as haptic warning to stimulate the driver's attention, or in case of a severe ALKS or severe vehicle failure.

Additionally, the signal to activate the hazard warning lights shall be generated with the start of the minimum risk manoeuvre.

- 5.5.2. The minimum risk manoeuvre shall bring the vehicle to standstill unless the system is deactivated by the driver during the manoeuvre.

- 5.5.3. A minimum risk manoeuvre shall only be terminated once the system is deactivated or the system has brought the vehicle to a standstill.

- 5.5.4. The system shall be deactivated at the end of any minimum risk manoeuvre.

The hazard warning lights shall remain activated unless deactivated manually and the vehicle shall not move away after standstill without manual input.

- 5.5.5. Reactivation of the system after the end of any minimum risk manoeuvre shall only be possible after each new engine start/run cycle.

6. HUMAN-MACHINE INTERFACE/OPERATOR INFORMATION

6.1. Driver Availability Recognition System

The fulfilment of the provisions of this paragraph shall be demonstrated by the manufacturer to the technical service during the inspection of the safety approach as part of the assessment to Annex 4 and according to the relevant tests in Annex 5.

- 6.1.1. The system shall comprise a driver availability recognition system.

The driver availability recognition system shall detect if the driver is present in a driving position, if the safety belt of the driver is fastened and if the driver is available to take over the driving task.

6.1.2. Driver presence

A transition demand shall be initiated according to paragraph 5.4 if any of the following conditions is met:

- (a) When the driver is detected not to be in the seat for a period of more than one second; or
- (b) When the driver's safety belt is unbuckled.

The second level warning of the safety-belt reminder according to UN-R16 may be used instead of an acoustic warning of the Transition Demand.

6.1.3. Driver availability

The system shall detect if the driver is available and in an appropriate driving position to respond to a transition demand by monitoring the driver.

The manufacturer shall demonstrate to the satisfaction of the technical service the vehicle's capability to detect that the driver is available to take over the driving task.

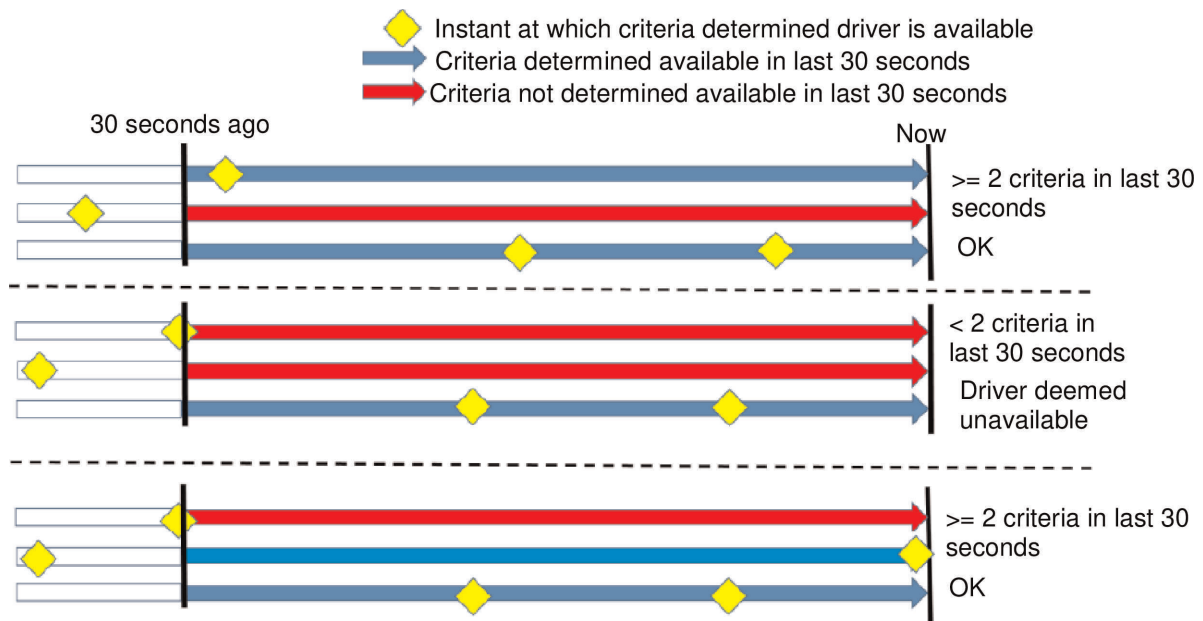
6.1.3.1. Criteria for deeming driver availability

The driver shall be deemed to be unavailable unless at least two availability criteria (e.g. input to driver-exclusive vehicle control, eye blinking, eye closure, conscious head or body movement) have individually determined that the driver is available in the last 30 seconds.

At any time, the system may deem the driver unavailable.

As soon as the driver is deemed to be unavailable, or fewer than two availability criteria can be monitored, the system shall immediately provide a distinctive warning until appropriate actions of the driver are detected or until a transition demand is initiated. At the latest, a transition demand shall be initiated according to paragraph 5.4 if this warning continues for 15s.

Justification for the number and combination of availability criteria, in particular with regard to the corresponding time interval, shall be provided by the manufacturer by documented evidence. However, the time interval required for any availability criteria shall not exceed 30 seconds. This shall be demonstrated by the manufacturer and assessed by the technical service according to Annex 4.



6.1.4. 'Other activities than driving' through on-board displays available upon activation of the ALKS shall be automatically suspended (i) as soon as the system issues a Transition Demand; or (ii) as soon as the system is deactivated, whichever comes first.

6.2. Activation, Deactivation and Driver Input

The fulfilment of the provisions of this paragraph shall be demonstrated by the manufacturer to the technical service during the inspection of the safety approach as part of the assessment to Annex 4 and according to the relevant tests in Annex 5.

6.2.1. The vehicle shall be equipped with dedicated means for the driver to activate (active mode) and deactivate (off mode) the system. When the ALKS is activated, the means to deactivate ALKS shall be permanently visible to the driver.

6.2.2. The default status of the system shall be the off mode at the initiation of each new engine start/run cycle.

This requirement does not apply when a new engine start/run cycle is performed automatically, e.g. by the operation of a stop/start system.

6.2.3. The system shall become active only upon a deliberate action by the driver and if all the following conditions are met:

- (a) The driver is in the driver seat and the driver's safety belt is fastened according to paragraphs 6.1.1 and 6.1.2;
- (b) The driver is available to take over control of the DDT according to paragraph 6.1.3;
- (c) No failure affecting the safe operation or the functionality of the ALKS is present;
- (d) DSSAD is operational;

- (e) The environmental and infrastructural conditions allow the operation;
- (f) Positive confirmation of system self-check; and
- (g) The vehicle is on roads where pedestrians and cyclists are prohibited and which, by design, are equipped with a physical separation that divides the traffic moving in opposite directions.

If any of the above conditions is no longer fulfilled, the system shall immediately initiate a transition demand unless specified differently in this Regulation.

- 6.2.4 It shall be possible to manually deactivate (off-mode) the system by an intentional action of the driver using the same means as to activate the system, as mentioned in paragraph 6.2.1.

The means of deactivating shall provide protection against unintentional manual deactivation for example by requiring a single input exceeding a certain threshold of time or a double press, or two separate but simultaneous inputs.

Additionally, it shall be ensured the driver is in lateral control of the vehicle at the time of the deactivation, by e. g. placing the deactivation means on the steering control or confirming the driver is holding the steering control.

- 6.2.5. In addition to paragraph 6.2.4, the system shall not be deactivated by any driver input other than those described below in paragraphs 6.2.5.1 to 6.2.5.4.

- 6.2.5.1. Deactivation by input to driving controls

The system shall be deactivated when at least one of the following conditions is met:

- (a) The driver overrides the system by steering while holding the steering control and this override is not suppressed, as specified in paragraph 6.3; or
- (b) The driver is holding the steering control and overrides the system by braking or accelerating, as specified in paragraph 6.3.1 below.

- 6.2.5.2. Deactivation during an ongoing transition demand or an ongoing minimum risk manoeuvre

In case a transition demand or a minimum risk manoeuvre is on-going, the system shall only be deactivated:

- (a) As defined in paragraph 6.2.5.1; or
- (b) Upon detection that the driver has taken hold of the steering control as a response to the transition demand or the minimum risk manoeuvre and provided the system confirms the driver is attentive as defined in paragraph 6.3.1.1.

- 6.2.5.3. Deactivation during an ongoing emergency manoeuvre

In case of an ongoing emergency manoeuvre, the deactivation of the system may be delayed until the imminent collision risk disappeared.

- 6.2.5.4. Deactivation in case of a severe vehicle failure or a severe ALKS failure

In case of a severe vehicle failure or a severe ALKS failure the ALKS may employ different strategies with regard to deactivation.

These different strategies shall be declared by the manufacturer and their effectiveness shall be assessed by the Technical Service with regard to ensuring a safe transition of control from the system to the human driver according to Annex 4.

- 6.2.6. On deactivation of the system, there shall not be an automatic transition to any function, which provides continuous longitudinal and/or lateral movement of the vehicle (e.g. ACSF of Category B1 function).

After deactivation, Corrective Steering Function (CSF) may be active with the aim at accustoming the driver to execute the lateral control task by gradually reducing lateral support.

Notwithstanding both paragraphs above, any other safety system delivering longitudinal or lateral support in imminent collision situations (e.g. Advanced Emergency Braking System (AEBS), Electronic Stability Control (ESC), Brake Assist System (BAS) or Emergency Steering Function (ESF)) shall not be deactivated in case of deactivation of ALKS.

6.2.7. Any deactivation shall be indicated to the driver as defined in paragraph 6.4.2.3.

6.3. System override

6.3.1. A driver input to the steering control shall override the lateral control function of the system when the input exceeds a reasonable threshold designed to prevent unintentional override.

This threshold shall include a specified force and duration and shall vary depending on parameters that include criteria used for driver attentiveness to be checked during the drivers input as defined in paragraph 6.3.1.1.

These thresholds and the rationale for any variation shall be demonstrated to the Technical Service during the assessment according to Annex 4.

6.3.1.1. Driver attentiveness

The system shall detect if the driver is attentive. The driver is deemed to be attentive when at least one of the following criteria is met:

- (a) Driver gaze direction is confirmed as primarily looking at the road ahead;
- (b) Driver gaze direction is being confirmed as looking at the rear-view mirrors; or,
- (c) Driver head movement is confirmed as primarily directed towards the driving task.

The specification for confirming these or equally safe criteria must be declared by the manufacturer and supported by documented evidence. This shall be assessed by the technical service according to Annex 4.

6.3.2. A driver input to the braking control resulting in a higher deceleration than that induced by the system or maintaining the vehicle in standstill by any braking system, shall override the longitudinal control function of the system.

6.3.3. A driver input to the accelerator control may override the longitudinal control function of the system. However, such an input shall not cause the system to no longer meet the requirements of this Regulation.

6.3.4. Any driver input to the accelerator or brake control shall immediately initiate a transition demand as specified in paragraph 5.4, when the input exceeds a reasonable threshold designed to prevent unintentional input.

6.3.5. Notwithstanding the provisions laid down in paragraphs 6.3.1 to 6.3.3, the effect of the driver input on any control may be reduced or suppressed by the system in case the system has detected an imminent collision risk due to this driver input.

6.3.6. In case of a severe vehicle failure or a severe ALKS failure the ALKS may employ different strategies with regard to system override. These different strategies shall be declared by the manufacturer and their effectiveness shall be assessed by the Technical Service with regard to ensuring a safe transition of control from the system to the human driver.

6.3.7. The fulfilment of the provisions in paragraph 6.3 and its subparagraphs shall be demonstrated by the manufacturer to the technical service during the inspection of the safety approach as part of the assessment to Annex 4.

6.4. Information to the driver

6.4.1. The following information shall be indicated to the driver:

- (a) The system status as defined in paragraph 6.4.2;
- (b) Any failure affecting the operation of the system with at least an optical signal unless the system is deactivated (off mode);
- (c) Transition demand by at least an optical and in addition an acoustic and/or haptic warning signal.
At the latest 4 s after the initiation of the transition demand, the transition demand shall:
 - (i) Contain a constant or intermittent haptic warning unless the vehicle is at standstill; and
 - (ii) Be escalated and remain escalated until the transition demand ends;
- (d) Minimum risk manoeuvre by at least an optical signal and in addition an acoustic and/or a haptic warning signal; and
- (e) Emergency manoeuvre by an optical signal.

The optical signals above shall be adequate in size and contrast. The acoustic signals above shall be loud and clear.

6.4.2. System status

6.4.2.1. System unavailability indication

In case activation of the system following the deliberate action of the driver is denied by the system due to system unavailability, this shall be at least visually displayed to the driver.

6.4.2.2. System status display when activated

Upon activation the system status (active mode) shall be displayed by a dedicated optical signal to the driver.

The optical signal shall contain an unambiguous indication including:

- (a) A steering control or a vehicle, with an additional 'A' or 'AUTO,' or the standardized symbols in accordance with UN Regulation No 121; and additionally
- (b) An easily perceptible indication in the peripheral field of vision and located near the direct line of driver's sight to the outside in front of the vehicle, e.g. prominent indication in the instrument cluster or on the steering control covering part of the outer rim perimeter facing towards the driver.

The optical signal shall indicate the active system state until the system is deactivated (off mode).

The optical signal shall be constant while the system is in regular operation and with the initiation of a transition demand at least the indication according to (b) shall change its characteristics, e.g. to an intermittent signal or a different colour.

When an intermittent signal is used, a low frequency shall be used in order to not unreasonably alert the driver.

During the transition phase and minimum risk manoeuvre, the indication according to (a) may be replaced by the instruction to take over manual control according to paragraph 6.4.3.

6.4.2.3. System status display when deactivated

Upon deactivation when the system status changes from active mode to off mode this shall be indicated to the driver by at least an optical warning signal. This optical signal shall be realized by non-displaying the optical signal used to indicate the active mode or non-displaying the instruction to take over manual control.

Additionally, an acoustic warning signal shall be provided unless the system is deactivated following a transition demand which contained an acoustic signal.

6.4.3. Transition Phase and Minimum Risk Manoeuvre

During the transition phase and the Minimum Risk Manoeuvre, the system shall instruct the driver in an intuitive and unambiguous way to take over manual control of the vehicle. The instruction shall include a pictorial information showing hands and the steering control and may be accompanied by additional explanatory text or warning symbols, as shown in the example below.



Example 1

Example 2

6.4.3.2. With the start of the minimum risk manoeuvre, the given signal shall change its characteristics to emphasize the urgency of an action by the driver. e.g. by red flashing of the steering control and moving hands of the pictorial information.

6.4.4. Where examples are given above, an adequate and equally perceptible interface design for the optical signals may be used instead. This shall be demonstrated by the manufacturer and shall be supported by documented evidence. This shall be assessed by the Technical Service according to Annex 4.

6.4.5. Prioritization of ALKS warnings

The warnings of an ALKS during a transition phase, a Minimal Risk Manoeuvre or an Emergency Manoeuvre may be prioritized over other warnings in the vehicle.

The prioritization of different acoustic and optical warnings during the ALKS operation shall be declared by the manufacturer to the Technical Service during Type Approval.

7. OBJECT AND EVENT DETECTION AND RESPONSE (OEDR)

7.1. Sensing requirements

The fulfilment of the provisions of this paragraph shall be demonstrated by the manufacturer to the technical service during the inspection of the safety approach as part of the assessment to Annex 4 and according to the relevant tests in Annex 5.

The ALKS vehicle shall be equipped with a sensing system such that, it can at least determine the driving environment (e.g. road geometry ahead, lane markings) and the traffic dynamics:

- (a) Across the full width of its own traffic lane, the full width of the traffic lanes immediately to its left and to its right, up to the limit of the forward detection range;
- (b) Along the full length of the vehicle and up to the limit of the lateral detection range.

The requirements of this paragraph are without prejudice to other requirements in this Regulation, most notably paragraph 5.1.1.

7.1.1. Forward detection range

The manufacturer shall declare the forward detection range measured from the forward most point of the vehicle. This declared value shall be at least 46 metres.

The Technical Service shall verify that the distance at which the vehicle sensing system detects a road user during the relevant test in Annex 5 is equal or greater than the declared value.

7.1.2. Lateral detection range

The manufacturer shall declare the lateral detection range. The declared range shall be sufficient to cover the full width of the lane immediately to the left and of the lane immediately to the right of the vehicle.

The Technical Service shall verify that the vehicle sensing system detects vehicles during the relevant test in Annex 5. This range shall be equal or greater than the declared range.

7.1.3. The ALKS shall implement strategies to detect and compensate for environmental conditions that reduce the detection range, e.g. prevent enabling the system, disabling the system and transferring the control back to the driver, reducing the speed when visibility is too low. These strategies shall be described by the manufacturer and assessed according to Annex 4.

7.1.4. The vehicle manufacturer shall provide evidence that the effects of wear and ageing do not reduce the performance of the sensing system below the minimum required value specified in paragraph 7.1 over the lifetime of the system/vehicle.

7.1.5. The fulfilment of the provisions of paragraph 7.1 and its subparagraphs shall be demonstrated to the technical service and tested according to the relevant tests in Annex 5.

7.1.6. A single perception malfunction without failure should not induce hazardous event. The design strategies put in place shall be described by the vehicle manufacturer and their safety shall be demonstrated to the satisfaction of the technical service in accordance with Annex 4.

8. DATA STORAGE SYSTEM FOR AUTOMATED DRIVING

8.1. Each vehicle equipped with ALKS (the system) shall be fitted with a DSSAD that meets the requirements specified below. The fulfilment of the provisions of paragraph 8 shall be demonstrated by the manufacturer to the technical service during the inspection of the safety approach as part of the assessment to Annex 4.

This Regulation is without prejudice to national and regional laws governing access to data, privacy and data protection.

8.2. Recorded occurrences

8.2.1. Each vehicle equipped with a DSSAD shall at least record an entry for each of the following occurrences upon activation of the system:

- (a) Activation of the system.
- (b) Deactivation of the system, due to:
 - (i) Use of dedicated means for the driver to deactivate the system;
 - (ii) Override on steering control;
 - (iii) Override by accelerator control while holding steering control;
 - (iv) Override by braking control while holding steering control.
- (c) Transition Demand by the system, due to:
 - (i) Planned event;
 - (ii) Unplanned event;
 - (iii) Driver unavailability (as per para. 6.1.3);
 - (iv) Driver not present or unbuckled (as per para. 6.1.2);
 - (v) System failure;
 - (vi) System override by braking input;
 - (vii) System override by accelerator input.

- (d) Reduction or suppression of driver input;
- (e) Start of Emergency Manoeuvre;
- (f) End of Emergency Manoeuvre;
- (g) Event Data Recorder (EDR) trigger input;
- (h) Involved in a detected collision;
- (i) Minimum Risk Manoeuvre engagement by the system;
- (j) Severe ALKS failure;
- (k) Severe vehicle failure.

8.3. Data elements

8.3.1. For each event listed in paragraph 8.2, the DSSAD shall at least record the following data elements in a clearly identifiable way:

- (a) The occurrence flag, as listed in paragraph 8.2;
- (b) Reason for the occurrence, as appropriate, and listed in paragraph 8.2;
- (c) Date (Resolution: yyyy/mm/dd);
- (d) Timestamp:
 - (i) Resolution: hh/mm/ss timezone e.g. 12:59:59 UTC;
 - (ii) Accuracy: +/- 1,0 s.

8.3.2. For each event listed in paragraph 8.2, the R₁₅₇SWIN for ALKS, or the software versions relevant to ALKS, indicating the software that was present at the time when the event occurred, shall be clearly identifiable.

8.3.3. A single timestamp may be allowed for multiple elements recorded simultaneously within the timing resolution of the specific data elements. If more than one element is recorded with the same timestamp, the information from the individual elements shall indicate the chronological order.

8.4. Data availability

8.4.1. DSSAD data shall be available subject to requirements of national and regional law ⁽³⁾.

8.4.2. Once the storage limits of the DSSAD are achieved, existing data shall only be overwritten following a first in first out procedure with the principle of respecting the relevant requirements for data availability.

Documented evidence regarding the storage capacity shall be provided by the vehicle manufacturer.

8.4.3. The data shall be retrievable even after an impact of a severity level set by UN Regulations Nos 94, 95 or 137. If the main on-board vehicle power supply is not available, it shall still be possible to retrieve all data recorded on the DSSAD, as required by national and regional law.

8.4.4. Data stored in the DSSAD shall be easily readable in a standardized way via the use of an electronic communication interface, at least through the standard interface (OBD port).

8.4.5. Instructions from the manufacturer shall be provided on how to access the data.

⁽³⁾ Note: based on a recent quantitative study of a Contracting Party, GRVA is considering that the text specifies several timestamps specifications of 2 500 timestamps to correspond with a period of 6 months of use.

8.5. Protection against manipulation.

8.5.1. It shall be ensured that there is adequate protection against manipulation (e.g. data erasure) of stored data such as anti-tampering design.

8.6. Availability of DSSAD operation

8.6.1. DSSAD shall be able to communicate with the system to inform that the DSSAD is operational.

9. CYBERSECURITY AND SOFTWARE UPDATES

9.1. The effectiveness of the system shall not be adversely affected by cyber-attacks, cyber threats and vulnerabilities. The effectiveness of the security measures shall be demonstrated by compliance with UN Regulation No 155.

9.2. If the system permits software updates, the effectiveness of the software update procedures and processes shall be demonstrated by compliance with UN Regulation No 156.

9.3. Requirements for software identification

9.3.1. For the purpose of ensuring the software of the System can be identified, an R₁₅₇SWIN may be implemented by the vehicle manufacturer. If R₁₅₇SWIN is not implemented, an alternative software identification system (i.e. software version) shall be implemented.

9.3.2. If the manufacturer implements an R₁₅₇WIN the following shall apply:

9.3.2.1. The vehicle manufacturer shall have a valid approval according to UN Regulation No 156 (Software Update Regulation).

9.3.2.2. The vehicle manufacturer shall provide the following information in the communication form of this Regulation:

(a) The R₁₅₇SWIN;

(b) How to read the R₁₅₇SWIN or software version(s) in case the R₁₅₇SWIN is not held on the vehicle.

9.3.2.3. The vehicle manufacturer may provide in the communication form of this Regulation a list of the relevant parameters that will allow the identification of those vehicles that can be updated with the software represented by the R₁₅₇SWIN. The information provided shall be declared by the vehicle manufacturer and may not be verified by an Approval Authority.

9.3.3. The vehicle manufacturer may obtain a new vehicle approval for the purpose of differentiating software versions intended to be used on vehicles already registered in the market from the software versions that are used on new vehicles. This may cover the situations where type approval regulations are updated or hardware changes are made to vehicles in series production. In agreement with the testing agency, duplication of tests shall be avoided where possible.

10. MODIFICATION OF VEHICLE TYPE AND EXTENSION OF TYPE APPROVAL

10.1. Every modification to an existing vehicle type shall be notified to the Type Approval Authority which approved the vehicle type.

The Authority shall then either:

(a) Decide, in consultation with the manufacturer, that a new type-approval is to be granted; or

- (b) Apply the procedure contained in paragraph 10.1.1 (Revision) and, if applicable, the procedure contained in paragraph 10.1.2 (Extension).

10.1.1. Revision

When particulars recorded in the information documents have changed and the Type Approval Authority considers that the modifications made are unlikely to have appreciable adverse effects and that in any case the foot controls still meet the requirements, the modification shall be designated a 'revision'.

In such a case, the Type Approval Authority shall issue the revised pages of the information documents as necessary, marking each revised page to show clearly the nature of the modification and the date of re-issue.

A consolidated, updated version of the information documents, accompanied by a detailed description of the modification, shall be deemed to meet this requirement.

10.1.2. Extension

The modification shall be designated an 'extension' if, in addition to the change of the particulars recorded in the information documents,

- (a) Further inspections or tests are required; or
- (b) Any information on the communication document (with the exception of its attachments) has changed; or
- (c) Approval to a later series of amendments is requested after its entry into force.

- 10.2. Confirmation or refusal of approval, specifying the alteration, shall be communicated by the procedure specified in paragraph 4.3 above to the Contracting Parties to the Agreement applying this Regulation. In addition, the index to the information documents and to the test reports, attached to the communication document of Annex 1, shall be amended accordingly to show the date of the most recent revision or extension.

- 10.3. The competent authority issuing the extension of approval shall assign a serial number to each communication form drawn up for such an extension.

11. CONFORMITY OF PRODUCTION

- 11.1. Procedures concerning conformity of production shall comply with those set out in the 1958 Agreement, Schedule 1 (E/ECE/TRANS/505/Rev.3) and meet the following requirements:

- 11.2. A vehicle approved pursuant to this Regulation shall be so manufactured as to conform to the type approved by meeting the requirements of this regulation;

- 11.3. The Type Approval Authority which has granted approval may at any time verify the conformity of control methods applicable to each production unit. The normal frequency of such inspections shall be once every two years.

12. PENALTIES FOR NON-CONFORMITY OF PRODUCTION

- 12.1. The approval granted in respect of a vehicle type pursuant to this Regulation may be withdrawn if the requirements laid down in paragraph 8, above are not complied with.

- 12.2. If a Contracting Party withdraws an approval it had previously granted, it shall forthwith so notify the other Contracting Parties applying this Regulation by sending them a communication form conforming to the model in Annex 1 to this Regulation.

13. PRODUCTION DEFINITELY DISCONTINUED

13.1. 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 Type Approval Authority which granted the approval, which in turn shall forthwith inform the other Contracting Parties to the Agreement applying this Regulation by means of a communication form conforming to the model in Annex 1 to this Regulation.

13.2. The production is not considered definitely discontinued if the vehicle manufacturer intends to obtain further approvals for software updates for vehicles already registered in the market.

14. NAMES AND ADDRESSES OF TECHNICAL SERVICES RESPONSIBLE FOR CONDUCTING APPROVAL TESTS AND OF TYPE APPROVAL AUTHORITIES

The Contracting Parties to the Agreement applying this Regulation shall communicate to the United Nations Secretariat ⁽⁴⁾ 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 are to be sent.

—

⁽⁴⁾ Through the online platform ('/343 Application') provided by UNECE and dedicated to the exchange of such information: <https://www.unece.org/trans/main/wp29/datasharing.html>

ANNEX 1

Communication

(Maximum format: A4 (210 × 297 mm))



issued by:

Name of administration:

.....

.....

.....

Concerning (²): Approval granted
 Approval extended
 Approval refused
 Approval withdrawn
 Production definitively discontinued

of a vehicle type with regard to Automated Lane Keeping System pursuant to UN Regulation No 157

Approval No

Reason for extension or revision:

1. Trade name or mark of vehicle

2. Vehicle type

3. Manufacturer's name and address

4. If applicable, name and address of manufacturer's representative

5. General construction characteristics of the vehicle:

5.1. Photographs and/or drawings of a representative vehicle:

6. Description and/or drawing of the ALKS including:

6.1. Specified maximum speed of the ALKS declared by the manufacturer:

6.2. Sensing system (incl. components):

6.3. Installation of the ALKS sensing system:

6.4. Software Identification of the ALKS (if applicable):

7. Written description and/or drawing of the ALKS Human-Machine Interface including:

7.1. Methods to detect driver availability

7.2. Means to activate, deactivate and override the system

7.3. Methods to determine driver attentiveness

7.4. Any system limitations due to environmental or road conditions

8. Written description and/or drawing of the information given to the driver including:
 - 8.1. System status:
 - 8.2. Transition demand:
 - 8.3. Minimum Risk Manoeuvre:
 - 8.4. Emergency Manoeuvre:
9. Data Storage System for Automated Driving (DSSAD):
 - 9.1. DSSAD performance verified after the tests performed according to Annex 5:yes/no
 - 9.2. DSSAD documentation concerning data retrievability, data integrity self-check and protection against manipulation of stored data verified: yes/no
10. Cyber Security and Software updates
 - 10.1. Cyber Security Type Approval Number (if applicable):
 - 10.2. Software Update Type approval number (if applicable):
11. Special requirements to be applied to the safety aspects of electronic control systems (Annex 4)
 - 11.1. Manufacturers document reference for Annex 4 (including version number):
 - 11.2. Information document form (Appendix 2 of Annex 4)
12. Technical Service responsible for conducting approval tests.....
 - 12.1. Date of report issued by that service.....
 - 12.2. (Reference) Number of the report issued by that service.....
13. Approval granted/extended/revised/refused/withdrawn²
14. Position of approval mark on vehicle.....
15. Place.....
16. Date
17. Signature
18. Annexed to this communication is a list of documents in the approval file deposited at the administration services having delivered the approval and which can be obtained upon request.

Additional information

19. R₁₅₇SWIN:
- 19.1. Information on how to read the R₁₅₇SWIN or software version(s) in case the R₁₅₇SWIN is not held on the vehicle:

19.2. If applicable, list the relevant parameters that will allow the identification of those vehicles that can be updated with the software represented by the R₁₅₇SWIN under item 19.1:

(¹) Distinguishing number of the country which has granted/extended/refused/withdrawn approval (see approval provisions in UN Regulation No 157).

(²) Strike out what does not apply.

*Appendix***Addendum to Type approval Communication No ... concerning the type approval of a vehicle type with regard to ALKS pursuant to Regulation No 157****Additional information**

Contracting Party regions where the vehicle manufacturer has declared that the ALKS had been assessed to comply with local traffic rules:

Country	Assessed	Comments on any restrictions
E 1 Germany	Yes/No	
E 2 France		
E 3 Italy		
E 4 Netherlands		
E 5 Sweden		
E 6 Belgium		
E 7 Hungary		
E 8 Czech Republic		
E 9 Spain		
E 10 Serbia		
E 11 United Kingdom		
E 12 Austria		
E 13 Luxembourg		
E 14 Switzerland		
E 16 Norway		
E 17 Finland		
E 18 Denmark		
E 19 Romania		
E 20 Poland		
E 21 Portugal		
E 22 Russian Federation		
E 23 Greece		
E 24 Ireland		
E 25 Croatia		
E 26 Slovenia		
E 27 Slovakia		
E 28 Belarus		
E 29 Estonia		
E 30 Republic of Moldova		
E 31 Bosnia and Herzegovina		
E 32 Latvia		
E 34 Bulgaria		
E 35 Kazakhstan		
E 36 Lithuania		

Country	Assessed	Comments on any restrictions
E 37 Turkey		
E 39 Azerbaijan		
E 40 North Macedonia		
E 43 Japan		
E 45 Australia		
E 46 Ukraine		
E 47 South Africa		
E 48 New Zealand		
E 49 Cyprus		
E 50 Malta		
E 51 Republic of Korea		
E 52 Malaysia		
E 53 Thailand		
E 54 Albania		
E 55 Armenia		
E 56 Montenegro		
E 57 San Marino		
E 58 Tunisia		
E 60 Georgia		
E 62 Egypt		
E 63 Nigeria		
[E 64 Pakistan]		

*

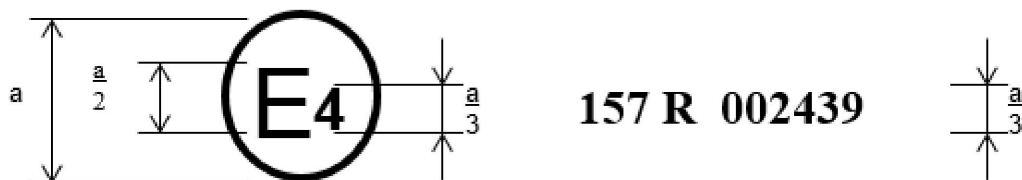
* The list of Contracting Parties applying UN Regulation No 157 is available online: [https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XI-B-16-15\[X\]&chapter=11&clang=_en](https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XI-B-16-15[X]&chapter=11&clang=_en)

ANNEX 2

Arrangements of approval marks

MODEL A

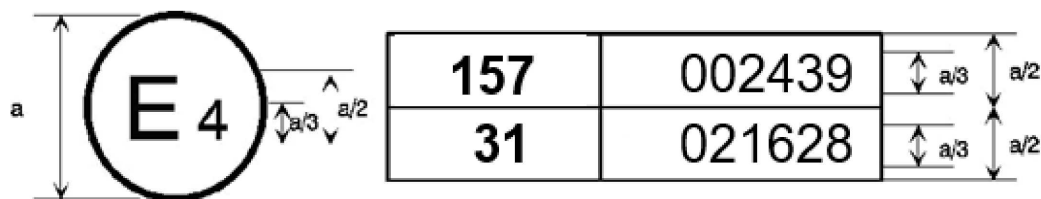
(See paragraph 4.4 of this Regulation)

 $a = 8 \text{ mm min}$

The above approval mark affixed to a vehicle shows that the vehicle type concerned has, with regard to ALKS, been approved in the Netherlands (E 4) pursuant to UN Regulation No 157 under approval No 002439. The approval number indicates that the approval was granted in accordance with the requirements of UN Regulation No 157 in its original version.

MODEL B

(See paragraph 4.5 of this Regulation)

 $a = 8 \text{ mm min}$

The above approval mark affixed to a vehicle shows that the vehicle type concerned has been approved in the Netherlands (E 4) pursuant to Regulations Nos 157 and 31. ⁽¹⁾ The approval numbers indicate that, at the dates when the respective approvals were given, UN Regulation No 157 was in its original version and UN Regulation No 31 included the 02 series of amendments.

⁽¹⁾ The second number is given merely as an example.

ANNEX 3

(Reserved)

ANNEX 4

Special requirements to be applied to the functional and operational safety aspects of Automated Lane Keeping Systems (ALKS)

1. GENERAL

This annex is intended to ensure that an acceptable thorough consideration of functional and operational safety for the automated system that provides the function(s) regulated by the ALKS Regulation has been performed by the manufacturer during the design and development processes and will continue to be done throughout the vehicle type lifecycle (design, development, production, field operation, decommissioning).

It covers the documentation which must be disclosed by the manufacturer to the type-approval authority or the technical Service acting on its behalf (hereafter referred as type-approval authority), for type approval purposes.

This documentation shall demonstrate that automated lane keeping system meets the performance requirements specified in this UN Regulation, that it is designed and developed to operate in such a way that it is free of unreasonable safety risks to the driver, passengers and other road users.

The type approval authority granting the approval shall verify through targeted spot checks and tests that the argumentation provided by the documentation is strong enough and that the design and processes described in documentation are actually implemented by the manufacturer.

While based on the provided documentation, evidence and process audits/product assessments carried out to the satisfaction of the type approval authority concerning this Regulation, the residual level of risk of the assessed automated lane keeping system is deemed to be acceptable for the entry into service of the vehicle type, the overall vehicle safety during the automated lane keeping system lifetime in accordance with the requirements of this regulation remains the responsibility of the manufacturer requesting the type-approval.

2. DEFINITIONS

For the purposes of this annex,

- 2.1. 'The system' means a 'Higher-Level Electronic Control' system and its electronic control system(s) that provide the automated driving function. This also includes any transmission links to or from other systems that are outside the scope of this Regulation that acts on the automated lane keeping function.
- 2.2. 'Safety Concept' is a description of the measures designed into the system, for example within the electronic units, so that the vehicle operates in such a way that it is free of unreasonable safety risks to the driver, passengers and other road users under faults and non-fault conditions. The possibility of a fallback to partial operation or even to a back-up system for vital vehicle functions shall be a part of the safety concept.
- 2.3. 'Electronic control system' means a combination of units, designed to co-operate in the production of the stated automated lane keeping function by electronic data processing. Such systems, commonly controlled by software, are built from discrete functional components such as sensors, electronic control units and actuators and connected by transmission links. They may include mechanical, electro-pneumatic or electro-hydraulic elements.
- 2.4. 'Higher-Level Electronic Control' systems are those which employ processing and/or sensing provisions to realize the dynamic driving task.
- 2.5. 'Units' are the smallest divisions of system components which will be considered in this annex, since these combinations of components will be treated as single entities for purposes of identification, analysis or replacement.
- 2.6. 'Transmission links' are the means used for inter-connecting distributed units for the purpose of conveying signals, operating data or an energy supply. This equipment is generally electrical but may, in some part, be mechanical, pneumatic or hydraulic.

- 2.7. 'Range of control' refers to an output variable and defines the range over which the system is likely to exercise control.
- 2.8. 'Boundary of functional operation' defines the boundaries of the external physical limits within which the system is able to perform the dynamic driving tasks (i.e. including the transition demands and minimum risk manoeuvres).
- 2.9. 'Operational Design Domain (ODD)' of the automated lane keeping system defines the specific operating conditions (e.g. environmental, geographic, time-of-day, traffic, infrastructure, speed range, weather and other conditions) within the boundaries fixed by this regulation under which the automated lane keeping system is designed to operate without any intervention by the driver.
- 2.10. 'Automated Driving Function' means a function of 'The System' that is capable of performing the dynamic driving task of the vehicle.
- 2.11. 'Control strategy' means a strategy to ensure robust and safe operation of the function(s) of 'The System' in response to a specific set of ambient and/or operating conditions (such as road surface condition, traffic intensity and other road users, adverse weather conditions, etc.). This may include the automatic deactivation of a function or temporary performance restrictions (e.g. a reduction in the maximum operating speed, etc.).
- 2.12. 'Functional safety': absence of unreasonable risks under the occurrence of hazards caused by a malfunctioning behaviour of electric/electronic systems (safety hazards resulting from system faults).
- 2.13. 'Fault': abnormal condition that can cause an element (system, component, software) or an item (system or combination of systems that implement a function of a vehicles) to fail.
- 2.14. 'Failure' means the termination of an intended behaviour of an element or an item.
- 2.15. 'Operational safety' means the absence of unreasonable risk under the occurrence of hazards resulting from functional insufficiencies of the intended functionality (e.g. false/missed detection), operational disturbances (e.g. environmental conditions like fog, rain, shadows, sunlight, infrastructure) or by reasonably foreseeable misuse/errors by the driver, passengers and other road users (safety hazards – without system faults).
- 2.16. 'Unreasonable risk' means the overall level of risk for the driver, vehicle occupants and other road users which is increased compared to a competently and carefully driven manual vehicle.

3. DOCUMENTATION

3.1. Requirements

The manufacturer shall provide a documentation package which gives access to the basic design of 'The System' and the means by which it is linked to other vehicle systems or by which it directly controls output variables.

The function(s) of 'The System', including the control strategies, and the safety concept, as laid down by the manufacturer, shall be explained.

Documentation shall be brief, yet provide evidence that the design and development has had the benefit of expertise from all the system fields which are involved.

For periodic technical inspections, the documentation shall describe how the current operational status of 'The System' can be checked.

Information about how the software version(s) and the failure warning signal status can be readable in a standardized way via the use of an electronic communication interface, at least be the standard interface (OBD port).

The Type-approval authority shall assess the documentation package to show that 'The System':

- (a) Is designed and was developed to operate in such a way that it is free from unreasonable risks for the driver, passengers and other road users within the declared ODD and boundaries;
- (b) Respects, under the performance requirements specified elsewhere in this UN Regulation;
- (c) Was developed according to the development process/method declared by the manufacturer and that this includes at least the steps listed in paragraph 3.4.4.

3.1.1. Documentation shall be made available in three parts:

- (a) Application for type approval: The information document which is submitted to the type approval authority at the time of type approval application shall contain brief information on the items listed in Appendix 2. It will become part of the approval.
- (b) The formal documentation package for the approval, containing the material listed in this paragraph 3 (with the exception of that of paragraph 3.4.4) which shall be supplied to the Type Approval Authority for the purpose of conducting the product assessment / process audit. This documentation package shall be used by the Type Approval Authority as the basic reference for the verification process set out in paragraph 4 of this annex. The Type Approval Authority shall ensure that this documentation package remains available for a period determined of at least 10 years counted from the time when production of the vehicle type is definitely discontinued.
- (c) Additional confidential material and analysis data (intellectual property) of paragraph 3.4.4 which shall be retained by the manufacturer, but made open for inspection (e.g. on-site in the engineering facilities of the manufacturer) at the time of the product assessment / process audit. The manufacturer shall ensure that this material and analysis data remains available for a period of 10 years counted from the time when production of the vehicle type is definitely discontinued.

3.2. Description of the functions of 'The System' including control strategies

A description shall be provided which gives a simple explanation of all the functions including control strategies of 'The System' and the methods employed to perform the dynamic driving tasks within the ODD and the boundaries under which the automated lane keeping system is designed to operate, including a statement of the mechanism(s) by which control is exercised. The manufacturer shall describe the interactions expected between the system and the driver, vehicle occupants and other road users as well as Human-Machine Interface (HMI).

Any enabled or disabled automated driving functions for which the hardware and software are present in the vehicle at the time of production, shall be declared and are subject to the requirements of this annex, prior to their use in the vehicle. The manufacturer shall also document the data processing in case of continuous learning algorithms are implemented.

- 3.2.1. A list of all input and sensed variables shall be provided and the working range of these defined, along with a description of how each variable affects system behaviour.
- 3.2.2. A list of all output variables which are controlled by 'The System' shall be provided and an explanation given, in each case, of whether the control is direct or via another vehicle system. The range of control (paragraph 2.7) exercised on each such variable shall be defined.
- 3.2.3. Limits defining the boundaries of functional operation including ODD-limits shall be stated where appropriate to automated lane keeping system performance.
- 3.2.4. Interaction concept with the driver when ODD limits are reached shall be explained including the list of types of situations in which the system will generate a transition demand to the driver.

- 3.2.5. Information shall be provided about the means to activate, override or deactivate the system including the strategy how the system is protected against unintentional deactivation. This shall also include information about how the system detects that the driver is available to take over driving control along with specification and documented evidence of the used parameter to identify driver attentiveness as well as the influence on the steering thresholds.

3.3. System layout and schematics

3.3.1. Inventory of components.

A list shall be provided, collating all the units of 'The System' and mentioning the other vehicle systems which are needed to achieve the control function in question.

An outline schematic showing these units in combination, shall be provided with both the equipment distribution and the interconnections made clear.

This outline shall include:

- (a) Perception and objects detection including mapping and positioning;
- (b) Characterization of Decision-making;
- (c) Remote supervision and remote monitoring by a remote supervision centre (if applicable);
- (d) The data storage system (DSSAD).

3.3.2. Functions of the units

The function of each unit of 'The System' shall be outlined and the signals linking it with other units or with other vehicle systems shall be shown. This may be provided by a labelled block diagram or other schematic, or by a description aided by such a diagram.

- 3.3.3. Interconnections within 'The System' shall be shown by a circuit diagram for the electric transmission links, by a piping diagram for pneumatic or hydraulic transmission equipment and by a simplified diagrammatic layout for mechanical linkages. The transmission links both to and from other systems shall also be shown.

- 3.3.4. There shall be a clear correspondence between transmission links and the signals carried between Units. Priorities of signals on multiplexed data paths shall be stated wherever priority may be an issue affecting performance or safety.

3.3.5. Identification of units

Each unit shall be clearly and unambiguously identifiable (e.g. by marking for hardware, and by marking or software output for software content) to provide corresponding hardware and documentation association. Where software version can be changed without requiring replacement of the marking or component, the software identification must be by software output only.

Where functions are combined within a single unit or indeed within a single computer, but shown in multiple blocks in the block diagram for clarity and ease of explanation, only a single hardware identification marking shall be used. The manufacturer shall, by the use of this identification, affirm that the equipment supplied conforms to the corresponding document.

- 3.3.5.1. The identification defines the hardware and software version and, where the latter changes such as to alter the function of the unit as far as this Regulation is concerned, this identification shall also be changed.

3.3.6. Installation of sensing system components

The manufacturer shall provide information regarding the installation options that will be employed for the individual components that comprise the sensing system. These options shall include, but are not limited to, the location of the component in/on the vehicle, the material(s) surrounding the component, the dimensioning and geometry of the material surrounding the component, and the surface finish of the materials surrounding the component, once installed in the vehicle. The information shall also include installation specifications that are critical to the system's performance, e.g. tolerances on installation angle.

Changes to the individual components of the sensing system, or the installation options, shall be notified to the Type Approval Authority and be subject to further assessment.

3.4. Safety concept of the manufacturer

3.4.1. The manufacturer shall provide a statement which affirms that the 'The System' is free from unreasonable risks for the driver, passengers and other road users.

3.4.2. In respect of software employed in 'The System', the outline architecture shall be explained and the design methods and tools used shall be identified (see 3.5.1). The manufacturer shall show evidence of the means by which they determined the realization of the system logic, during the design and development process.

3.4.3. The manufacturer shall provide the Type Approval Authority with an explanation of the design provisions built into 'The System' so as to ensure functional and operational safety. Possible design provisions in 'The System' are for example:

- (a) Fall-back to operation using a partial system.
- (b) Redundancy with a separate system.
- (c) Removal of the automated driving function(s).

3.4.3.1. If the chosen provision selects a partial performance mode of operation under certain fault conditions (e.g. in case of severe failures), then these conditions shall be stated (e.g. type of severe failure) and the resulting limits of effectiveness defined (e.g. initiation of a minimum risk manoeuvre immediately) as well as the warning strategy to the driver.

3.4.3.2. If the chosen provision selects a second (back-up) means to realise the performance of the dynamic driving task, the principles of the change-over mechanism, the logic and level of redundancy and any built in back-up checking features shall be explained and the resulting limits of back-up effectiveness defined.

3.4.3.3. If the chosen provision selects the removal of the automated driving function, this shall be done in compliance with the relevant provisions of this regulation. All the corresponding output control signals associated with this function shall be inhibited.

3.4.4. The documentation shall be supported, by an analysis which shows, in overall terms, how the system will behave to mitigate or avoid hazards which can have a bearing on the safety of the driver, passengers and other road users.

The chosen analytical approach(es) shall be established and maintained by the manufacturer and shall be made open for inspection by the Type Approval Authority at the time of the type approval.

The Type Approval Authority shall perform an assessment of the application of the analytical approach(es):

- (a) Inspection of the safety approach at the concept (vehicle) level.

This approach shall be based on a Hazard / Risk analysis appropriate to system safety.

- (b) Inspection of the safety approach at the system level including a top down (from possible hazard to design) and bottom up approach (from design to possible hazards). The safety approach may be based on a Failure Mode and Effect Analysis (FMEA), a Fault Tree Analysis (FTA) and a System-Theoretic Process Analysis (STPA) or any similar process appropriate to system functional and operational safety.

- (c) Inspection of the validation/verification plans and results including appropriate acceptance criteria. This shall include validation testing appropriate for validation, for example, Hardware in the Loop (HIL) testing, vehicle on-road operational testing, testing with real end users, or any other testing appropriate for validation/verification. Results of validation and verification may be assessed by analysing coverage of the different tests and setting coverage minimal thresholds for various metrics.

The inspection shall confirm that at least each of the following items is covered where applicable under (a)-(c):

- (i) Issues linked to interactions with other vehicle systems (e.g. braking, steering);
- (ii) Failures of the automated lane keeping system and system risk mitigation reactions;
- (iii) Situations within the ODD when a system may create unreasonable safety risks for the driver, passengers and other road users due to operational disturbances (e.g. lack of or wrong comprehension of the vehicle environment, lack of understanding of the reaction from the driver, passenger or other road users, inadequate control, challenging scenarios);
- (iv) Identification of the relevant scenarios within the boundary conditions and management method used to select scenarios and validation tool chosen;
- (v) Decision making process resulting in the performance of the dynamic driving tasks (e.g. emergency manoeuvres), for the interaction with other road users and in compliance with traffic rules;
- (vi) Reasonably foreseeable misuse by the driver (e.g. driver availability recognition system and an explanation on how the availability criteria were established), mistakes or misunderstanding by the driver (e.g. unintentional override) and intentional tampering of the system;
- (vii) Cyberattacks having an impact on the safety of the vehicle (can be done through the analysis done under the UN Regulation No 155 on Cyber Security and Cyber Security Management System).

The assessment by the approval authority shall consist of spot checks of selected hazards (or cyber threats) to establish that argumentation supporting the safety concept is understandable and logical and implemented in the different functions of the systems. The assessment shall also check that validation plans are robust enough to demonstrate safety (e.g. reasonable coverage of chosen scenarios testing by the validation tool chosen) and have been completed.

It shall demonstrate that the vehicle is free from unreasonable risks for the driver; vehicle occupants and other road users in the operational design domain, i.e. through:

- (a) an overall validation target (i.e., validation acceptance criteria) supported by validation results, demonstrating that the entry into service of the automated lane keeping system will overall not increase the level of risk for the driver, vehicle occupants, and other road users compared to a manually driven vehicles; and
- (b) A scenario specific approach showing that the system will overall not increase the level of risk for the driver, passengers and other road users compared to a manually driven vehicles for each of the safety relevant scenarios; and

The Type Approval Authority shall perform or shall require performing tests as specified in paragraph 4 to verify the safety concept.

3.4.4.1. This documentation shall itemize the parameters being monitored and shall set out, for each failure condition of the type defined in paragraph 3.4.4 of this annex, the warning signal to be given to the driver/vehicle occupants/other road users and/or to service/technical inspection personnel.

3.4.4.2. This documentation shall also describe the measures in place to ensure the 'The System' is free from unreasonable risks for the driver, vehicle occupants, and other road users when the performance of 'The System' is affected by environmental conditions e.g. climatic, temperature, dust ingress, water ingress, ice packing.

3.5. Safety management system (Process Audit)

3.5.1. In respect of software and hardware employed in 'The System', the manufacturer shall demonstrate to the type approval authority in terms of a safety management system that effective processes, methodologies and tools are in place, up to date and being followed within the organization to manage the safety and continued compliance throughout the product lifecycle (design, development, production, operation including respect of traffic rules, and decommissioning).

- 3.5.2. The design and development process shall be established including safety management system, requirements management, requirements' implementation, testing, failure tracking, remedy and release
- 3.5.3. The manufacturer shall institute and maintain effective communication channels between manufacturer departments responsible for functional/operational safety, cybersecurity and any other relevant disciplines related to the achievement of vehicle safety.
- 3.5.4. The manufacturer shall have processes to monitor safety-relevant incidents/ crashes/collisions caused by the engaged automated lane keeping system and a process to manage potential safety-relevant gaps post-registration (closed loop of field monitoring) and to update the vehicles. They shall report critical incidents (e.g. collision with another road users and potential safety-relevant gaps) to the type-approval authorities when critical incidents.
- 3.5.5. The manufacturer shall demonstrate that periodic independent internal process audits are carried out to ensure that the processes established in accordance with paragraphs 3.5.1 to 3.5.4 are implemented consistently.
- 3.5.6. Manufacturers shall put in place suitable arrangements (e.g. contractual arrangements, clear interfaces, quality management system) with suppliers to ensure that the supplier safety management system comply with the requirements of paragraphs 3.5.1 (except for vehicle related aspects like 'operation' and 'decommissioning'), 3.5.2, 3.5.3 and 3.5.5.

4. VERIFICATION AND TESTS

- 4.1. The functional operation of 'The System', as laid out in the documents required in paragraph 3, shall be tested as follows:

- 4.1.1. Verification of the function of 'The System'

The Type approval authority shall verify 'The System' under non-failure conditions by testing on a track a number of selected functions from those described by the manufacturer in paragraph 3.2 above, and by checking the overall behaviour of the system in real driving conditions including the compliance with traffic rules.

These tests shall include scenarios whereby the system is overridden by the driver.

Tests according to this Annex shall take into account tests already conducted in Annex 5 of this Regulation.

- 4.1.1.1. The verification results shall correspond with the description, including the control strategies, provided by the manufacturer in paragraph 3.2 and shall comply with the requirements of this regulation.

- 4.1.2. Verification of the safety concept of paragraph 3.4.

The reaction of 'The System' shall be checked under the influence of a faults in any individual unit by applying corresponding output signals to electrical units or mechanical elements in order to simulate the effects of internal failure within the unit. The Type approval authority shall conduct this check for at least one individual unit, but shall not check the reaction of 'The System' to multiple simultaneous failures of individual units.

The Type Approval Authority shall verify that these tests include aspects that may have an impact on vehicle controllability and user information (HMI aspects e.g. transition scenarios).

- 4.1.2.1. The Type Approval Authorities shall also check a number of scenarios that are critical for the Object and Event Detection and Response (OEDR) and characterization of the decision-making and HMI functions of the system (e.g. object difficult to detect, when the system reaches the ODD boundaries, traffic disturbance scenarios) as defined in the regulation.

- 4.1.2.2. The verification results shall correspond with the documented summary of the hazard analysis, to a level of overall effect such that the safety concept and execution are confirmed as being adequate and in compliance with the requirements of this regulation.
- 4.2. Simulation tool and mathematical models for verification of the safety concept may be used in accordance with Schedule 8 of Revision 3 of the 1958 Agreement, in particular for scenarios that are difficult on a test track or in real driving conditions. Manufacturers shall demonstrate the scope of the simulation tool, its validity for the scenario concerned as well as the validation performed for the simulation tool chain (correlation of the outcome with physical tests).
5. REPORTING
- Reporting of the assessment shall be performed in such a manner that allows traceability, e.g. versions of documents inspected are coded and listed in the records of the Technical Service.
- An example of a possible layout for the assessment form from the Technical Service to the Type Approval Authority is given in Appendix 1 to this Annex. The listed items in this Appendix are outlined as minimum set of items which need to be covered.
6. COMMUNICATION TO OTHER TYPE APPROVAL AUTHORITIES (Appendix 2) containing:
- (a) Description of the ODD and the high-level functional architecture focusing on the functions available to the driver, vehicle occupants and other road users.
 - (b) Test results during the verification process by the type approval authorities.
7. COMPETENCE OF THE AUDITORS/ASSESSORS
- The assessments under this Annex shall only be conducted by auditors/assessors with the technical and administrative knowledge necessary for such purposes. They shall in particular be competent as auditor/assessor for ISO 26262-2018 (Functional Safety – Road Vehicles), and ISO/PAS 21448 (Safety of the Intended Functionality of road vehicles); and shall be able to make the necessary link with cybersecurity aspects in accordance with UN Regulation No 155 and ISO/SAE 21434). This competence should be demonstrated by appropriate qualifications or other equivalent training records.
-

Appendix 1

Model assessment form for Automated Lane Keeping System

Test report No:

1. Identification

1.1. Make:

1.2. Vehicle Type:

1.3. Means of system identification on the vehicle:

1.4. Location of that marking:

1.5. Manufacturer's name and address:

1.6. If applicable, name and address of manufacturer's representative:

1.7. Manufacturer's formal documentation package:

Documentation reference No:

Date of original issue:

Date of latest update:

2. Test vehicle(s)/system(s) description

2.1. General description:

2.2. Description of all the control functions of 'The System', and methods of operation:

2.3. Description of the components and diagrams of the interconnections within 'The System':

3. Manufacturer's safety concept

3.1. Description of signal flow and operating data and their priorities:

3.2. Manufacturer's declaration:

The manufacturer(s) affirm(s) that the 'The System' is free from unreasonable risks for the driver, vehicle occupants and other road users.

3.3. Software outline architecture and the design methods and tools used:

3.4. Explanation of the safety concept of 'The System':

3.5. Documented analyses of the behaviour of 'The System' under individual hazard or fault conditions:

3.6. Description of the measures in place for environmental conditions:

3.7. Provisions for the periodic technical inspection of 'The System':

3.8. Results of 'The System' verification test, as per para. 4.1.1 of Annex 4 to UN Regulation No 157:

3.9. Results of safety concept verification test, as per para. 4.1.2 of Annex 4 to UN Regulation No 157:

3.10. Date of test(s):

3.11. This test(s) has been carried out and the results reported in accordance with to UN Regulation No 157 as last amended by the series of amendments.

Technical Service carrying out the test

Signed: Date:

3.12. Comments:

Appendix 2

Information document form for automated lane keeping systems to be provided by the manufacturer for the approval

1. SYSTEM DESCRIPTION AUTOMATED LANE KEEPING SYSTEM
 - 1.1. Operational Design Domain (Speed, road type, country, Environment, Road conditions, etc.)/ Boundary conditions/ Main conditions for Minimum risk manoeuvres and transition demands
 - 1.2. Basic Performance (e.g. Object and Event Detection and Response (OEDR) ...)
 - 1.3. The means to activate, override or deactivate the system.
2. DESCRIPTION OF THE FUNCTIONS OF 'THE SYSTEM' INCLUDING CONTROL STRATEGIES
 - 2.1. Main automated Driving Functions (functional architecture, environmental perception).
 - 2.1.1. Vehicle-internal
 - 2.1.2. Vehicle-external (e.g. back-end)
3. OVERVIEW MAJOR COMPONENTS (UNITS) OF 'THE SYSTEM'
 - 3.1. Control Units
 - 3.2. Sensors
 - 3.3. Maps/Positioning
4. SYSTEM LAYOUT AND SCHEMATICS
 - 4.1. Schematic system layout including sensors for the environmental perception (e.g. block diagram)
 - 4.2. List and schematic overview of interconnections (e.g. block diagram)
5. SPECIFICATIONS
 - 5.1. Means to check the correct operational status of the system
 - 5.2. Means implemented to protect against simple unauthorized activation/operation and interventions into the system
6. SAFETY CONCEPT
 - 6.1. Safe Operation – Vehicle Manufacturer Statement
 - 6.2. Outline software architecture (e.g. block diagram)
 - 6.3. Means by which the realization of the system logic is determined
 - 6.4. General explanation of the main design provisions built into 'The System' so as to generate safe operation and interaction with other road users under fault conditions, under operational disturbances and the occurrence of planned/unplanned conditions that would exceed the ODD.

6.5.	General description of failure handling main principles, fall-back level strategy including risk mitigation strategy (minimum risk manoeuvre)
6.6.	Driver, vehicle occupants and other road users interaction including warning signals and transition demands to be given to driver.
6.7.	Validation by the manufacturer for the performance requirements specified elsewhere in the regulation including the OEDR, the HMI, the respect of traffic rules and the conclusion that the system is designed in such a way that it is free from unreasonable risks for the driver, vehicle occupants and other road users.
7.	VERIFICATION AND TEST BY THE AUTHORITIES
7.1.	Verification of the basic function of 'The System'
7.2.	Examples for checking the system reaction under the influence of a failure or an operational disturbance, emergency conditions and boundary conditions.....
8.	DATA STORAGE SYSTEM
8.1.	Type of Data stored
8.2.	Storage location.....
8.3.	Recorded occurrences and data elements means to ensure data security and data protection.....
8.4.	Means to access the data
9.	CYBERSECURITY (CROSS REFERENCE TO THE CYBER REGULATION IS POSSIBLE)
9.1.	General description of the cybersecurity and software update management scheme
9.2.	General description of the different risks and measures put in place to mitigate these risks.
9.3.	General description of the update procedure.
10.	INFORMATION PROVISIONS TO USERS
10.1.	Model of the information provided to users (including expected driver's tasks within the ODD and when going out of the ODD)
10.2.	Extract of the relevant part of the owner's manual.....

*Appendix 3***Guidance on Traffic disturbance critical scenarios for ALKS**

1. GENERAL
 - 1.1 This document clarifies derivation process to define conditions under which Automated Lane Keeping Systems (ALKS) shall avoid a collision. Conditions under which ALKS shall avoid a collision are determined by a general simulation program with following attentive human driver performance model and related parameters in the traffic critical disturbance scenarios.
2. TRAFFIC CRITICAL SCENARIOS
 - 2.1. Traffic disturbance critical scenarios are those which have conditions under which ALKS may not be able to avoid a collision.
 - 2.2. Following three are traffic critical scenarios:
 - (a) Cut-in: the 'other vehicle' suddenly merges in front of the 'ego vehicle';
 - (b) Cut-out: the 'other vehicle' suddenly exits the lane of the 'ego vehicle';
 - (c) Deceleration: the 'other vehicle' suddenly decelerates in front of the 'ego vehicle';
 - 2.3. Each of these traffic critical scenarios can be created using the following parameters/elements:
 - (a) Road geometry;
 - (b) Other vehicles' behaviour/ manoeuvre.
3. PERFORMANCE MODEL OF ALKS
 - 3.1. Traffic critical scenarios of ALKS are divided into preventable and unpreventable scenarios. The threshold for preventable/unpreventable is based on the simulated performance of a skilled and attentive human driver. It is expected that some of the 'unpreventable' scenarios by human standards may actually be preventable by the ALKS system.
 - 3.2. In a low-speed ALKS scenario, the avoidance capability of the driver model is assumed to be only by braking. The driver model is separated into the following three segments: 'Perception'; 'Decision'; and, 'Reaction'. The following diagram is a visual representation of these segments:
 - 3.3. To determine conditions under which Automated Lane Keeping Systems (ALKS) shall avoid a collision, performance model factors for these three segments in the following table should be used as the performance model of ALKS considering attentive human drivers' behaviour with ADAS.

Figure 1

Skilled human performance model

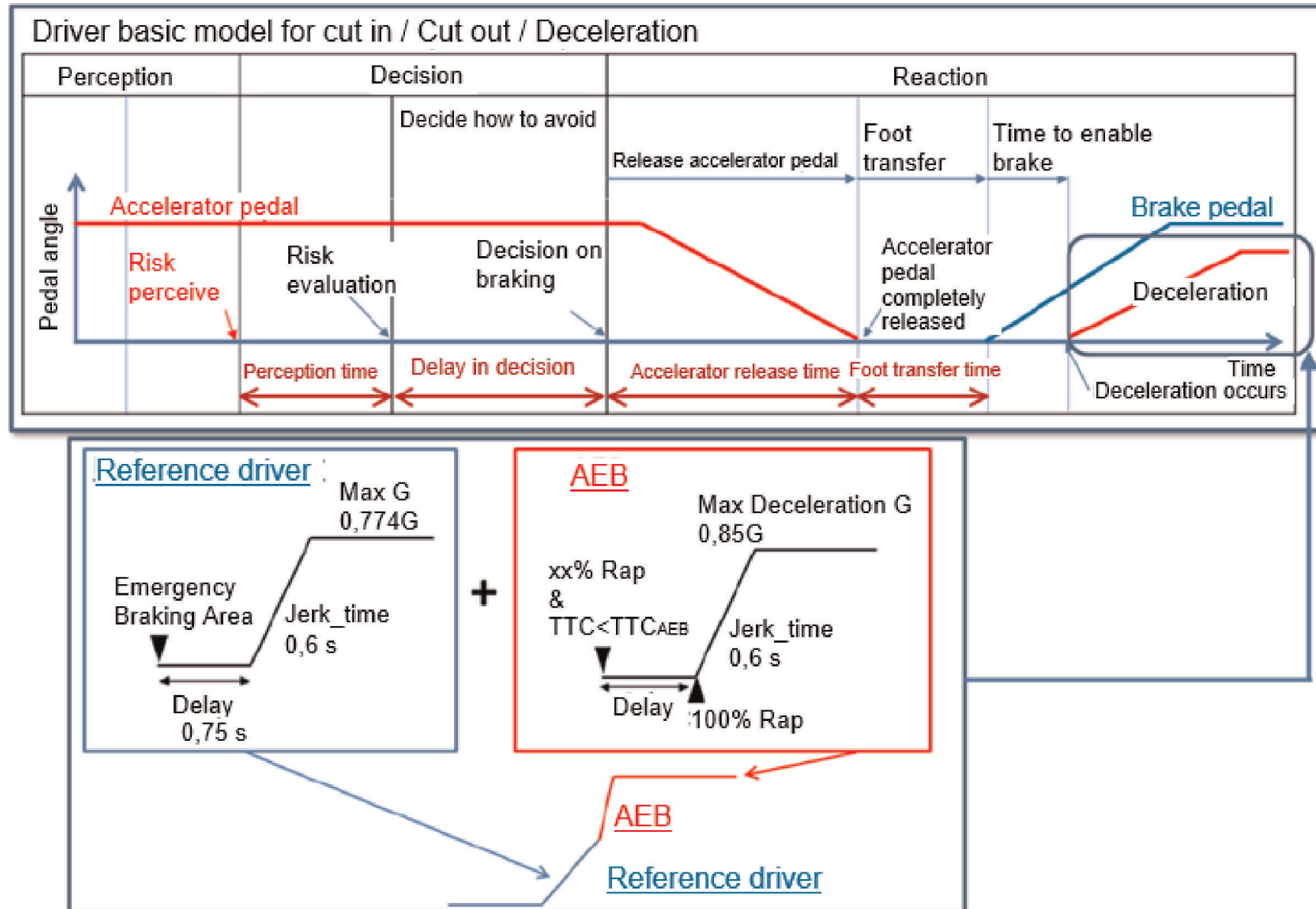


Table 1

Performance model factors for vehicles

		Factors
Risk perception point	Lane change (cutting in, cutting out)	Deviation of the centre of a vehicle over 0,375m from the centre of the driving lane (derived from research by Japan)
	Deceleration	Deceleration ratio of preceding vehicle and following distance of ego vehicle
Risk evaluation time		0,4 seconds (from research by Japan)
Time duration from having finished perception until starting deceleration		0,75 seconds (common data in Japan)
Jerking time to full deceleration (road friction 1,0)		0,6 seconds to 0,774G (from experiments by NHTSA and Japan)
Jerking time to full deceleration (after full wrap of ego vehicle and cut-in vehicle, road friction 1,0)		0,6 seconds to 0,85G (derived from UN Regulation No 152 on AEBS)

3.4. Driver model for the three ALKS scenarios:

3.4.1. For Cut in scenario:

The lateral wandering distance the vehicle will normally wander within the lane is 0,375 m.

The perceived boundary for cut-in occurs when the vehicle exceeds the normal lateral wandering distance (possibly prior to actual lane change)

The distance a. is the perception distance based on the perception time [a]. It defines the lateral distance required to perceive that a vehicle is executing a cut-in manoeuvre a. is obtained from the following formula;

$a = \text{lateral movement speed} \times \text{Risk perception time [a]} (0,4\text{sec})$

The risk perception time begins when the leading vehicle exceeds the cut-in boundary threshold.

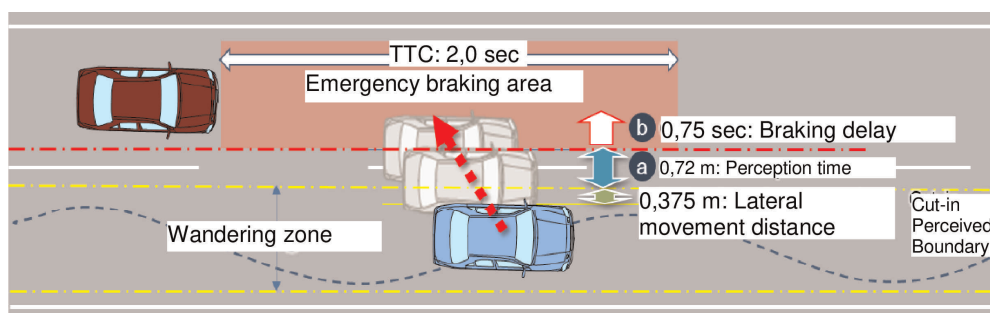
Max lateral movement speed is real world data in Japan.

Risk perception time [a] is driving simulator data in Japan.

2sec* is specified as the maximum Time To Collision (TTC) below which it was concluded that there is a danger of collision in the longitudinal direction.

Note: TTC = 2,0 seconds is chosen based on the UN Regulation guidelines on warning signals.

Figure 2

Driver model for the cut-in scenario

3.4.2. For Cut-out scenario:

The lateral wandering distance the vehicle will normally wander within the lane is 0,375 m.

The perceived boundary for cut-out occurs when the vehicle exceeds the normal lateral wandering distance (possibly prior to actual lane change)

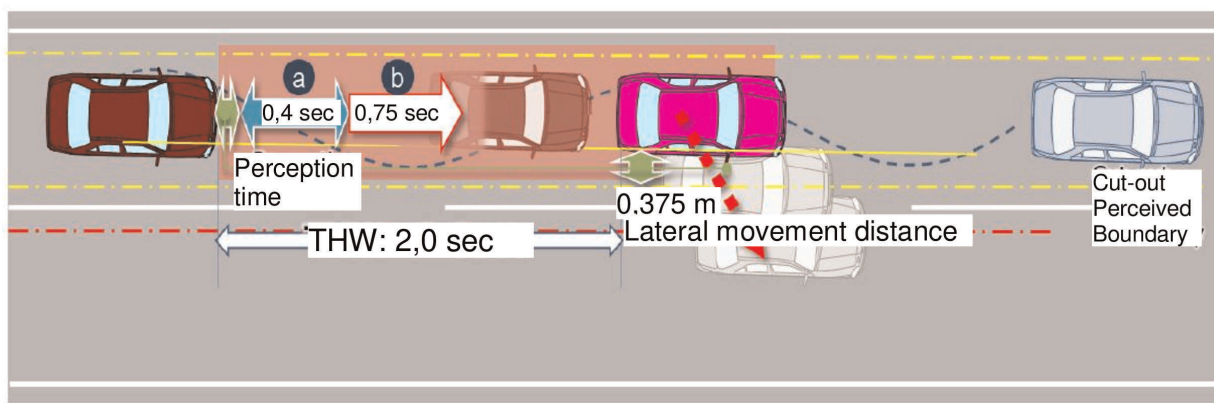
The risk perception time [a] is 0,4 seconds and begins when the leading vehicle exceeds the cut-out boundary threshold.

The time 2 seconds is specified as the maximum Time Head Way (THW) for which it was concluded that there is a danger in longitudinal direction.

Note: THW = 2,0 seconds is chosen according to other countries' regulations and guidelines.

Figure 3

Cut in scenario

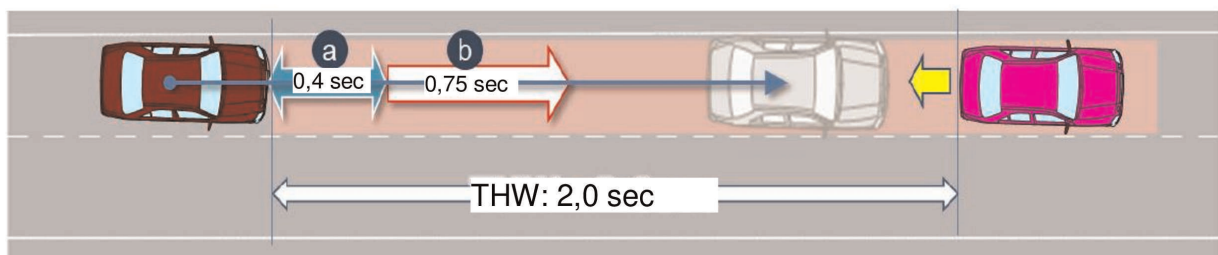


3.4.3. For Deceleration scenario:

The risk perception time [a] is 0,4 seconds. The risk perception time [a] begins when the leading vehicle exceeds a deceleration threshold 5m/s^2 .

Figure 4

Deceleration scenario



4. PARAMETERS

4.1. Parameters below are essential when describing the pattern of the traffic critical scenarios in section 2.1.

4.2. Additional parameters could be added according to the operating environment (e.g. friction rate of the road, road curvature, lighting conditions).

Table 2

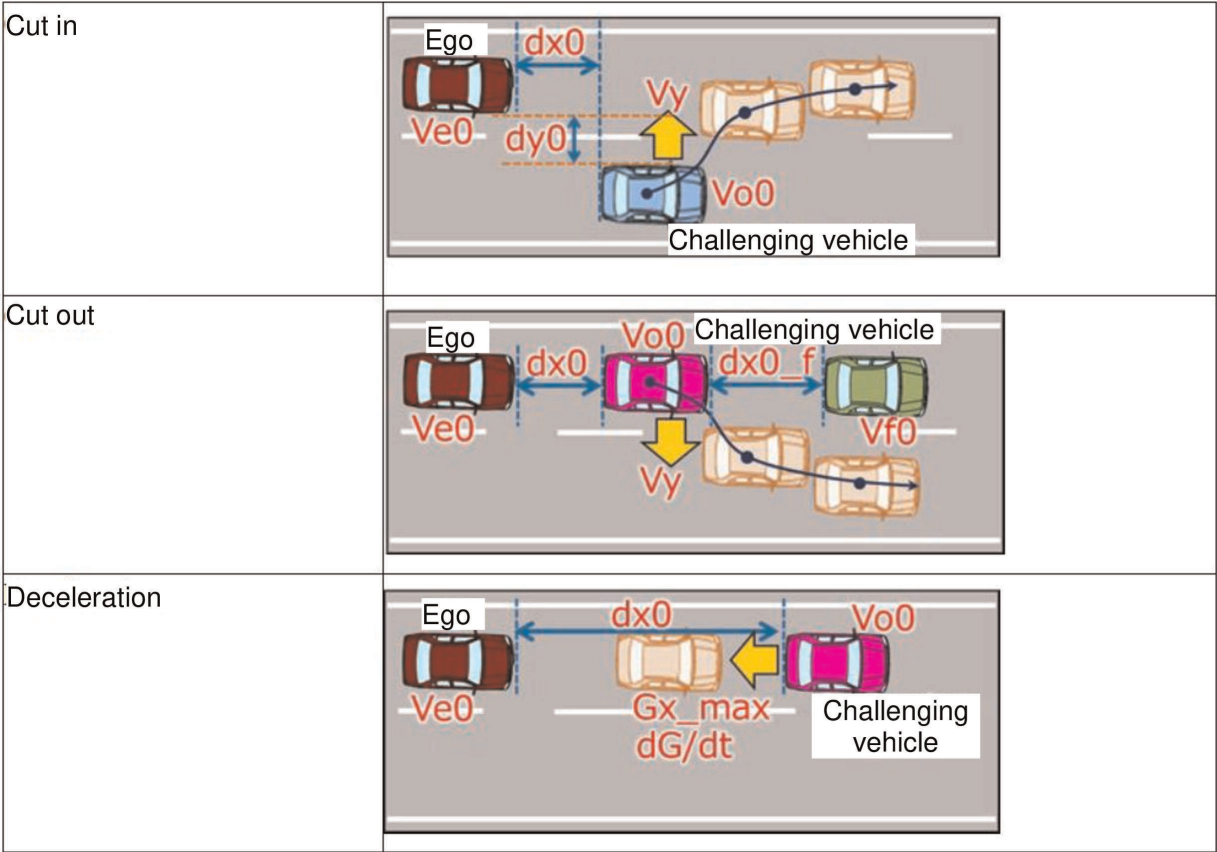
Additional parameters

Operating conditions	Roadway	Number of lanes = The number of parallel and adjacent lanes in the same direction of travel Lane Width = The width of each lane Roadway grade = The grade of the roadway in the area of test Roadway condition = the condition of the roadway (dry, wet, icy, snow, new, worn) including coefficient of friction Lane markings = the type, colour, width, visibility of lane markings
	Environmental conditions	Lighting conditions = The amount of light and direction (i.e., day, night, sunny, cloudy) Weather conditions = The amount, type and intensity of wind, rain, snow etc.
Initial condition	Initial velocity	Ve0 = Ego vehicle
		Vo0 = Leading vehicle in lane or in adjacent lane
		Vf0 = Vehicle in front of leading vehicle in lane
	Initial distance	dx0 = Distance in Longitudinal direction between the front end of the ego vehicle and the rear end of the leading vehicle in ego vehicle's lane or in adjacent lane
		dy0 = Inside Lateral distance between outside edge line of ego vehicle in parallel to the vehicle's median longitudinal plane within lanes and outside edge line of leading vehicle in parallel to the vehicle's median longitudinal plane in adjacent lines.
		dy0_f = Inside Lateral distance between outside edge line of leading vehicle in parallel to the vehicle's median longitudinal plane within lanes and outside edge line of vehicle in front of the leading vehicle in parallel to the vehicle's median longitudinal plane in adjacent lines.
		dx0_f = Distance in longitudinal direction between front end of leading vehicle and rear end of vehicle in front of leading vehicle
		dfy = Width of vehicle in front of leading vehicle
		doy = Width of leading vehicle
		dox = Length of the leading vehicle
Vehicle motion	Lateral motion	Vy = Leading vehicle lateral velocity
	Deceleration	Gx_max = Maximum deceleration of the leading vehicle in G
		dG/dt = Deceleration rate (Jerk) of the leading vehicle

4.3. Following are visual representations of parameters for the three types of scenarios

Figure 5

Visualisation



5. REFERENCE

Following data sheets are pictorial examples of simulations which determines conditions under which ALKS shall avoid a collision, taking into account the combination of every parameter, at and below the maximum permitted ALKS vehicle speed.

5.1. Cut in

Figure 6

Parameters

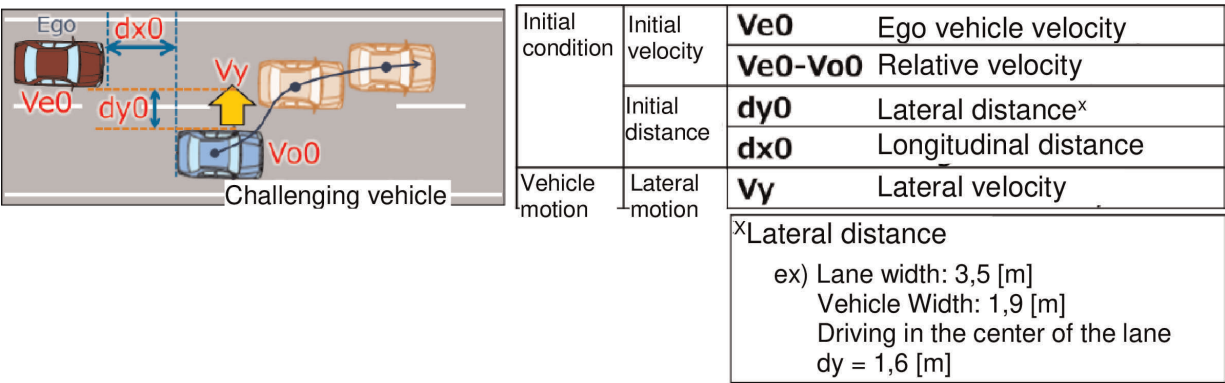


Figure 7
Overview

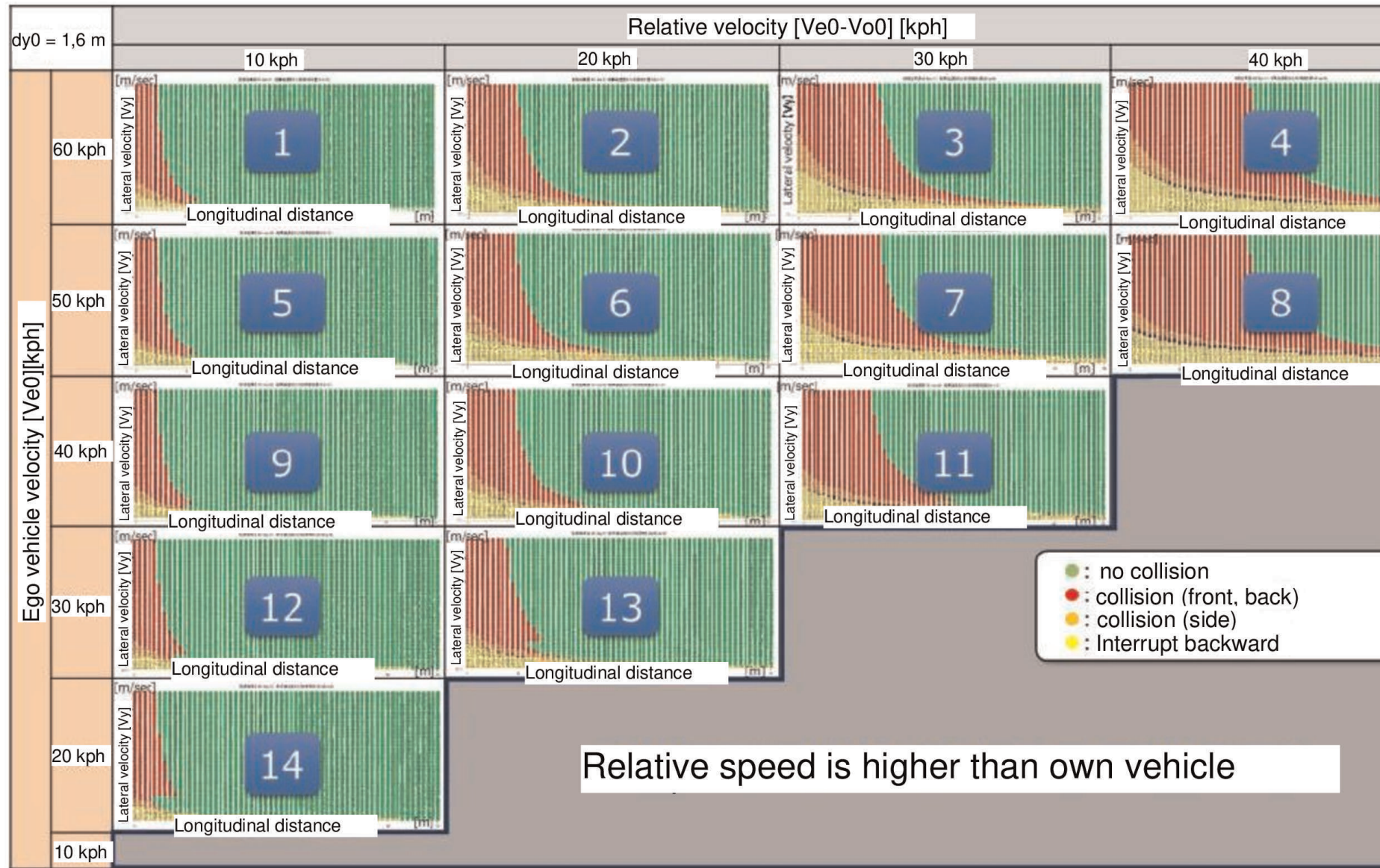
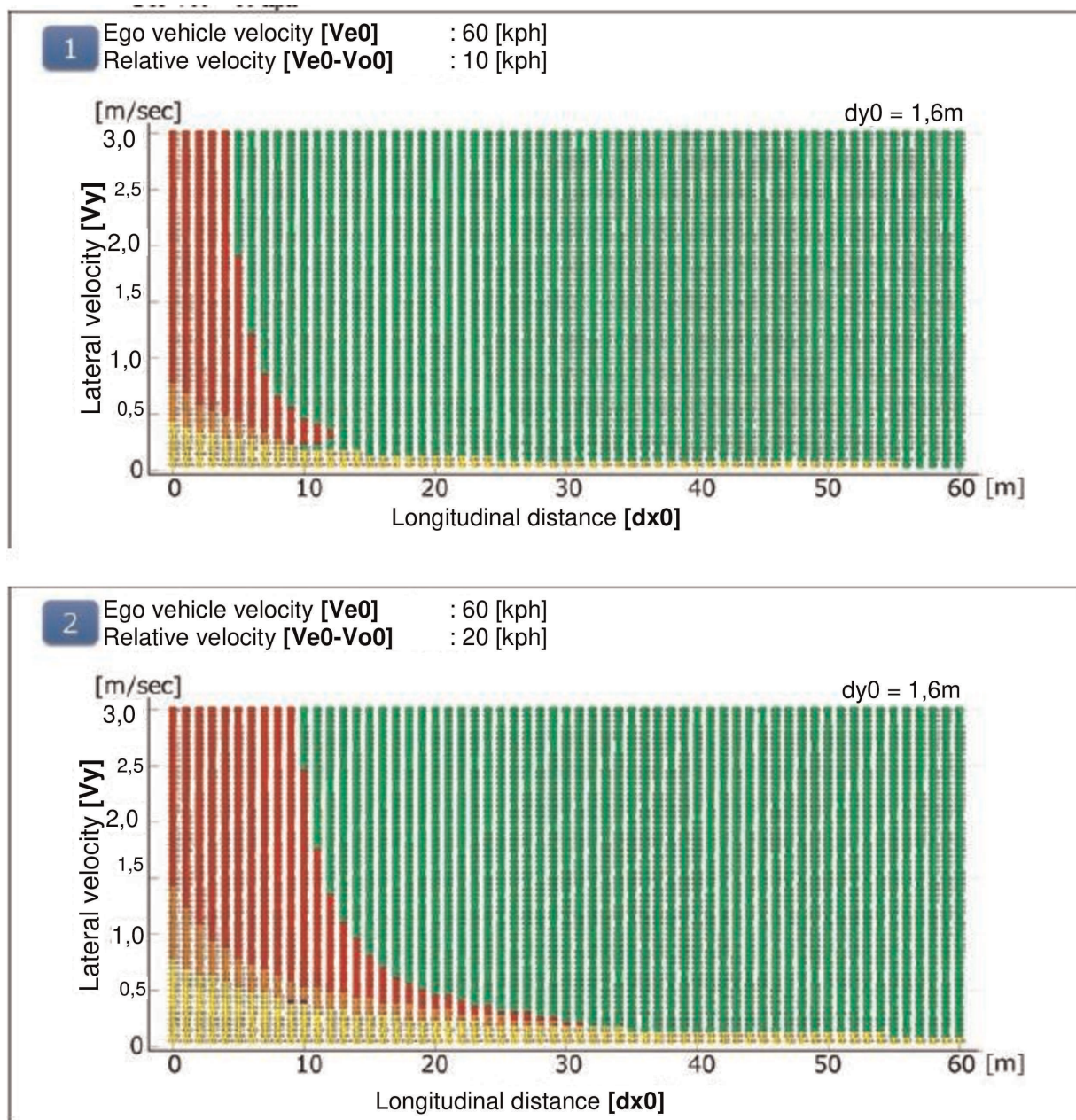


Figure 8

For $V_{e0} = 60$ kph

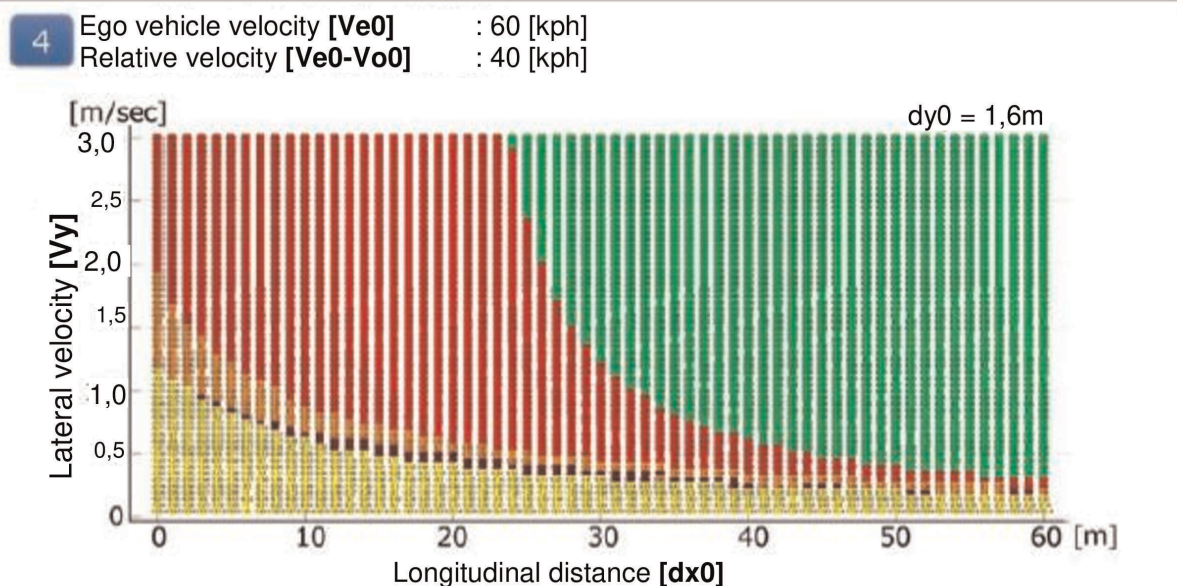
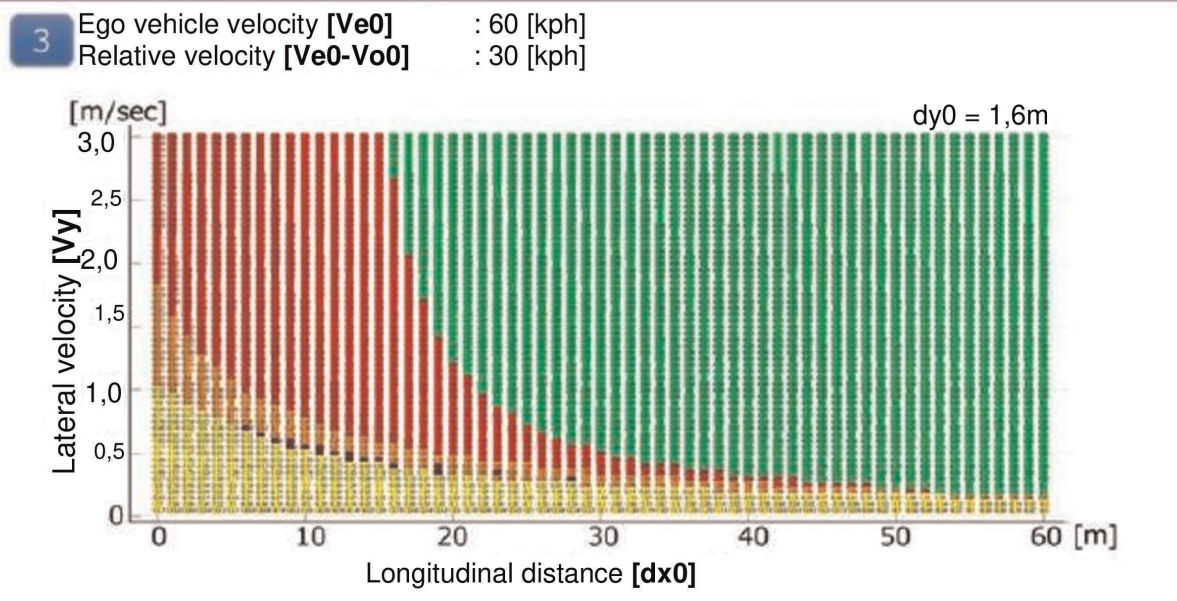
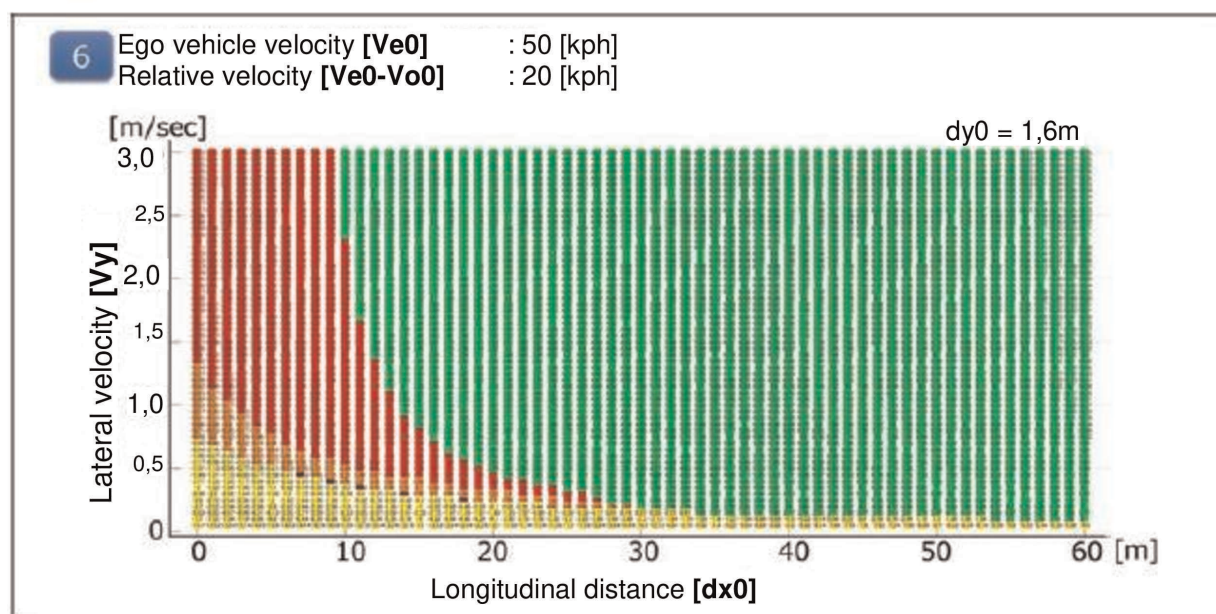
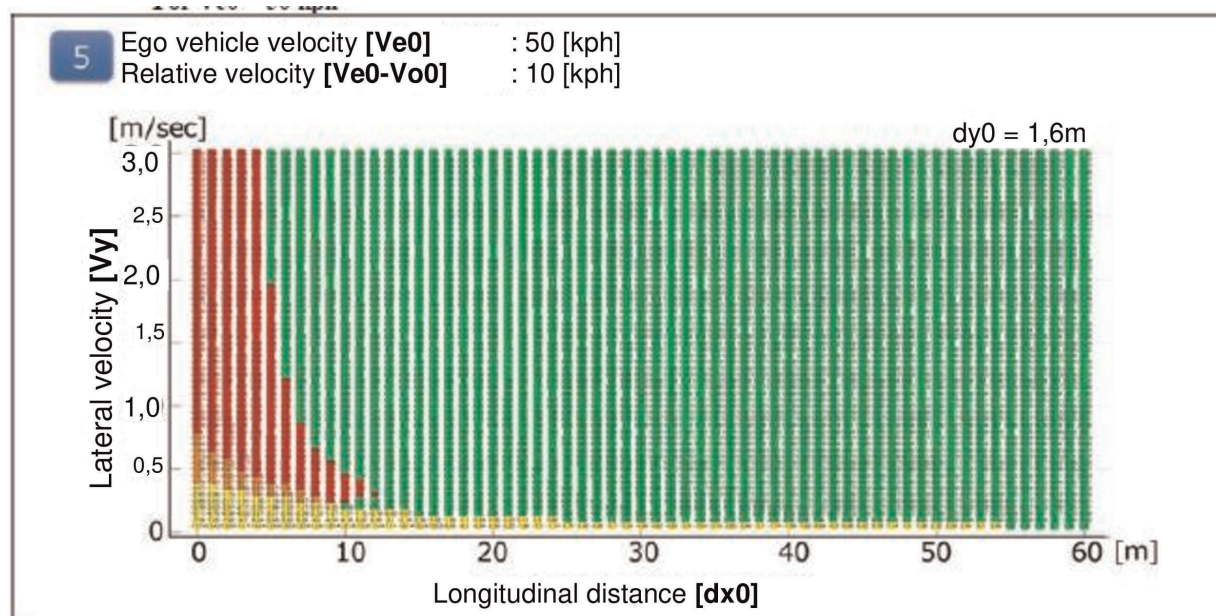


Figure 9

For $V_{e0} = 50$ kph

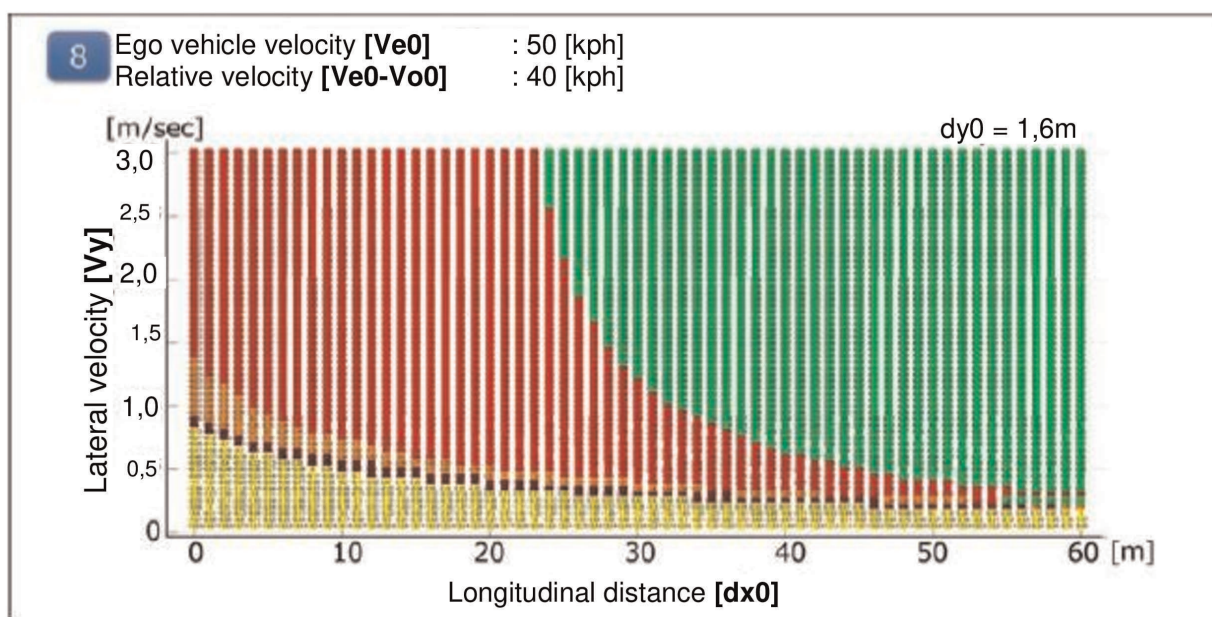
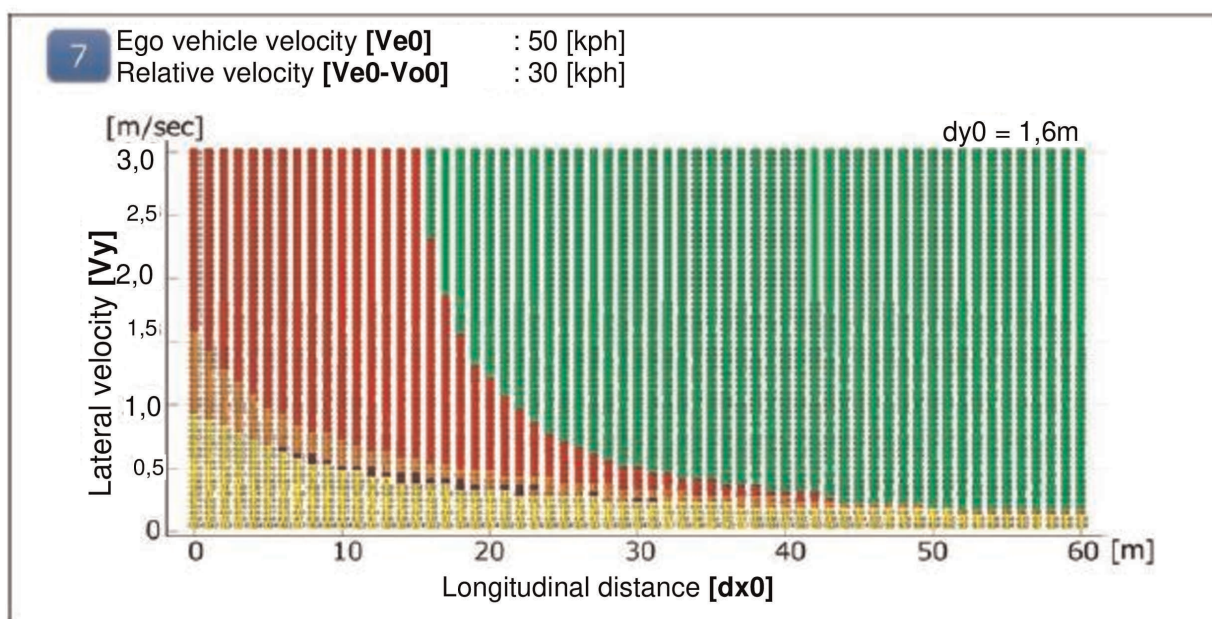
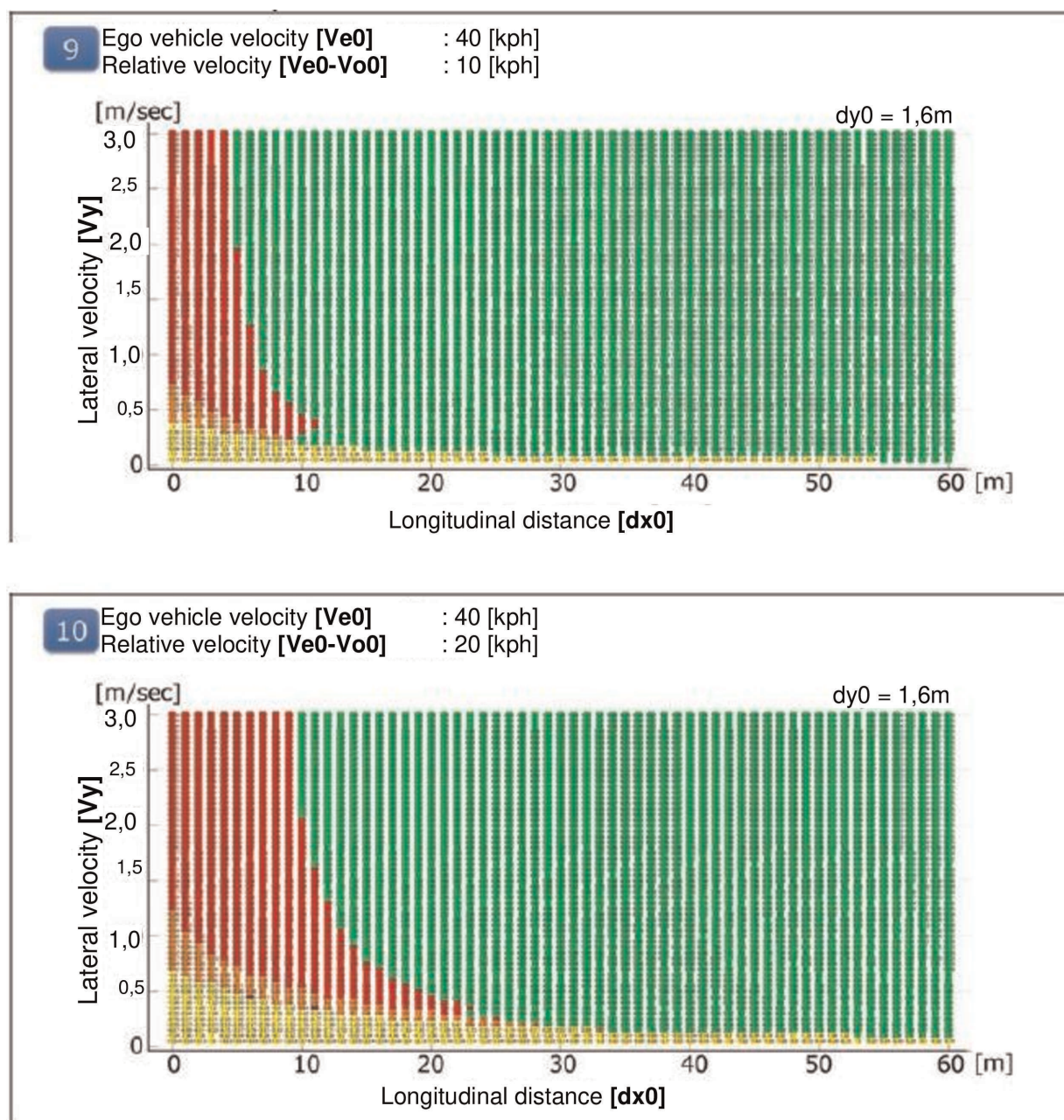


Figure 10

For $V_{e0} = 40$ kph

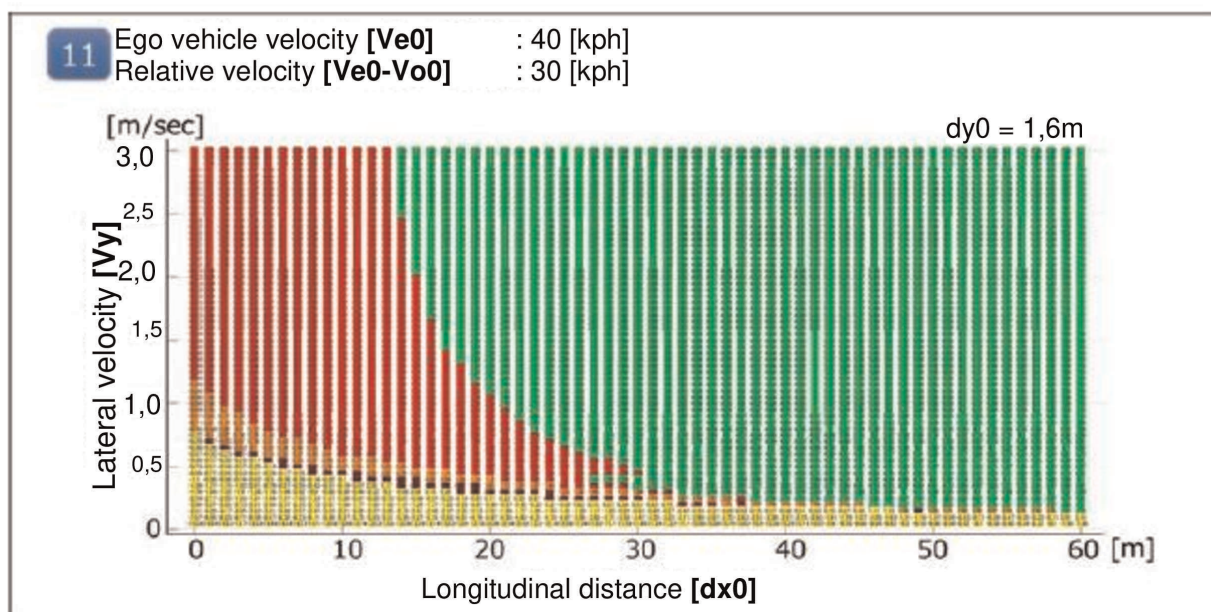
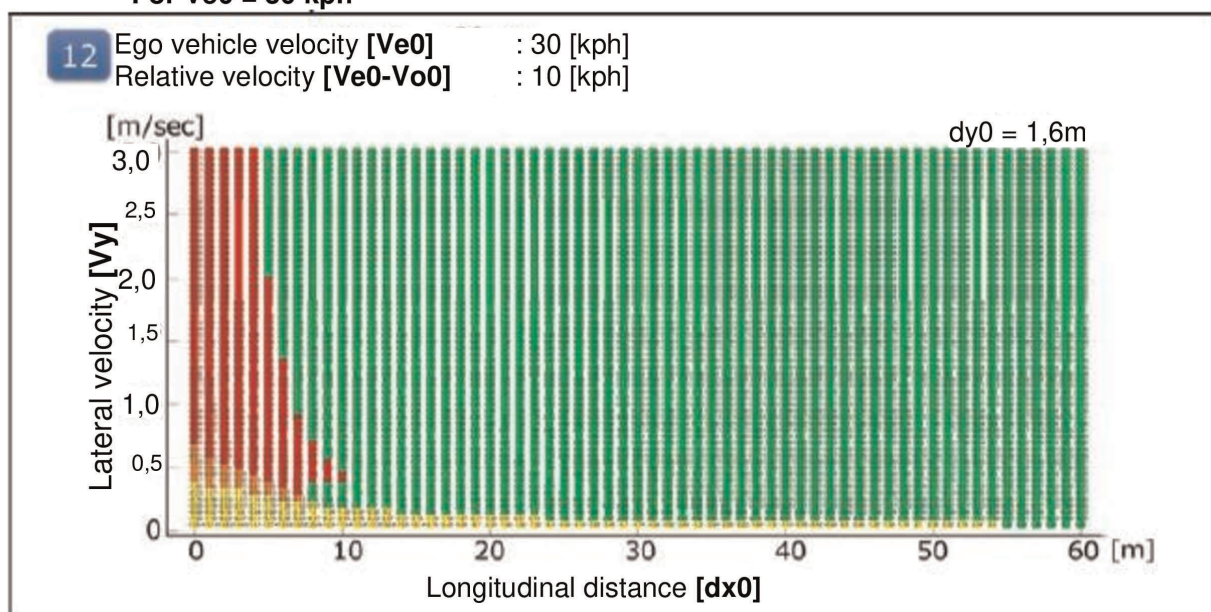


Figure 11

For **Ve0** = 30 kph

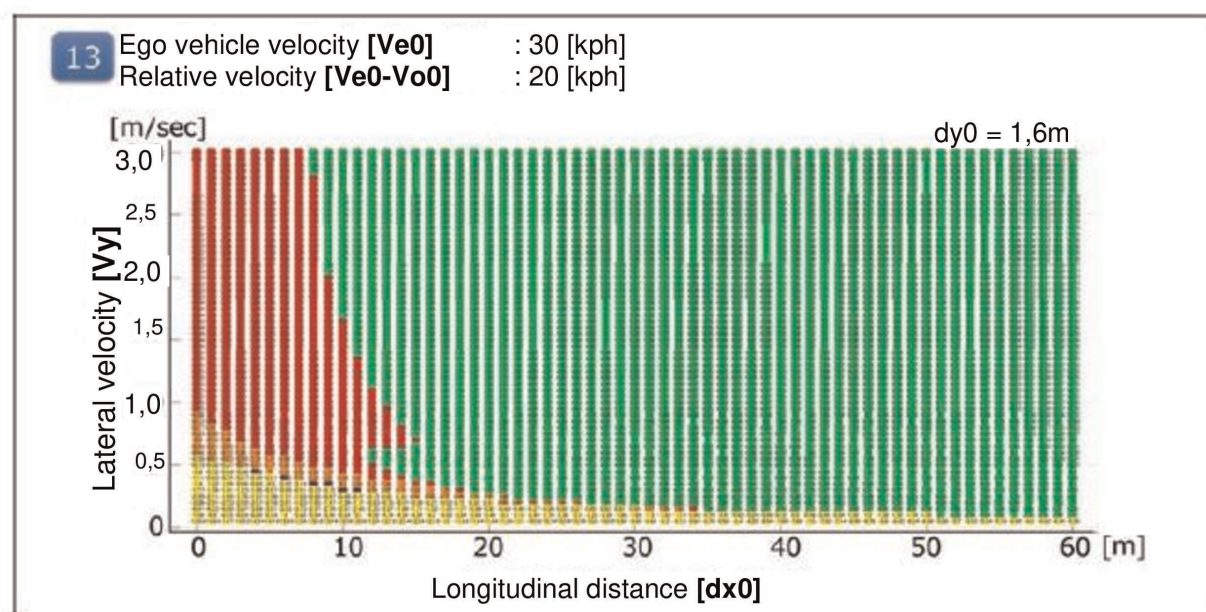
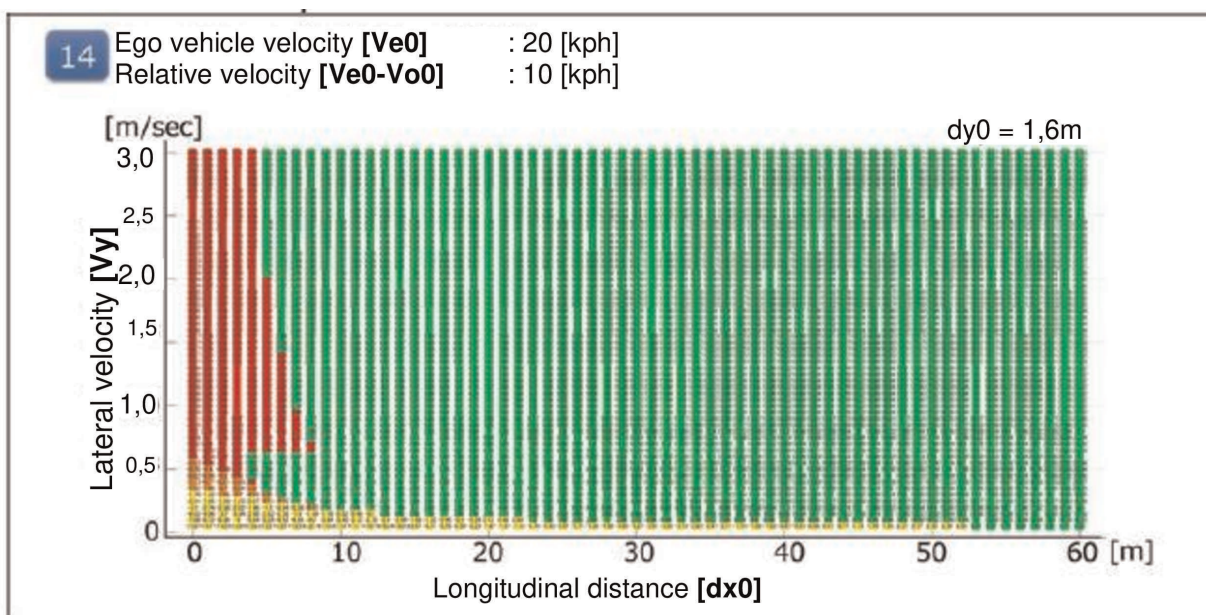


Figure 12

For Ve0 = 20 kph



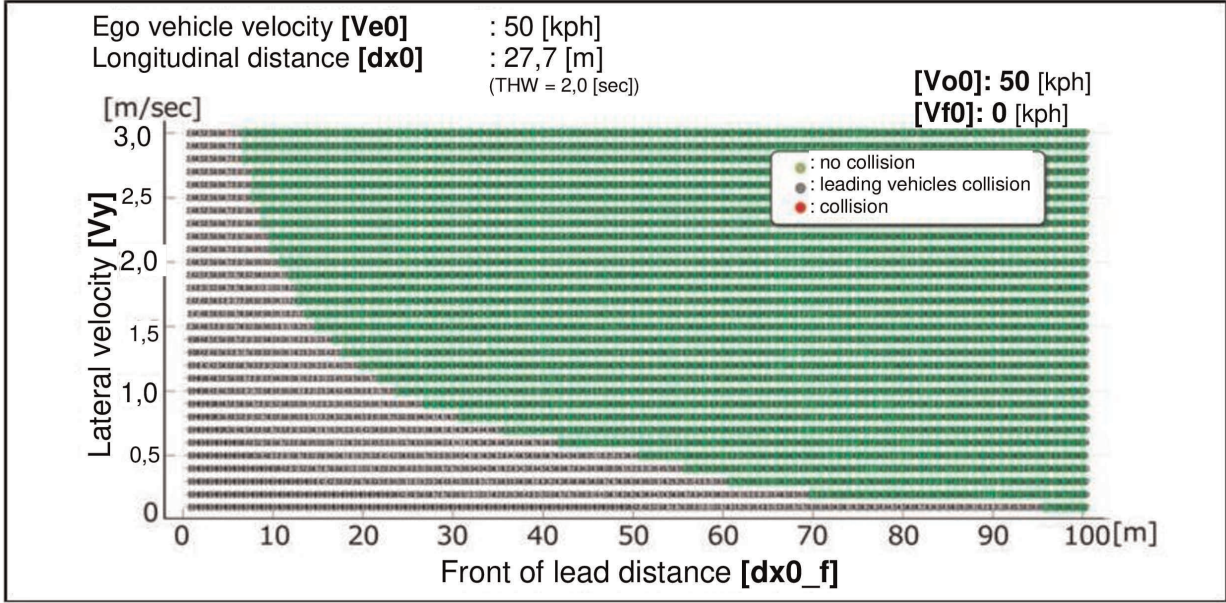
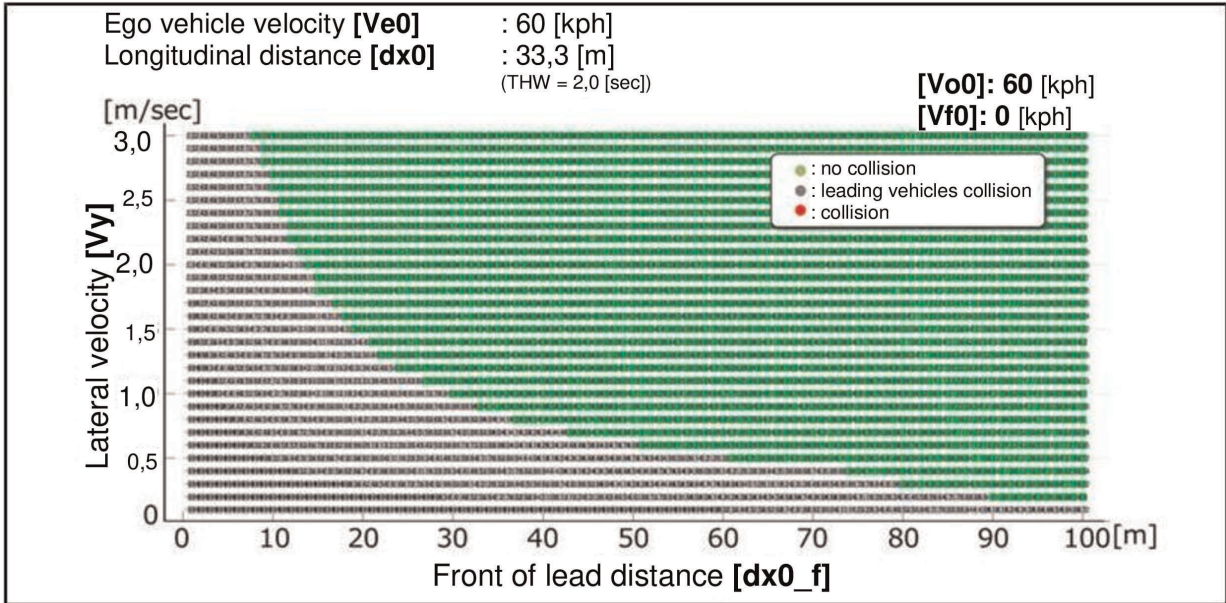
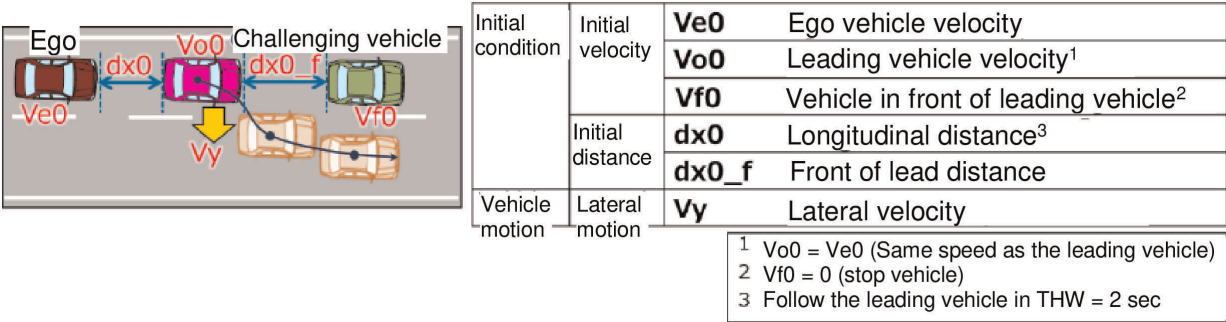
5.2. Cut-out

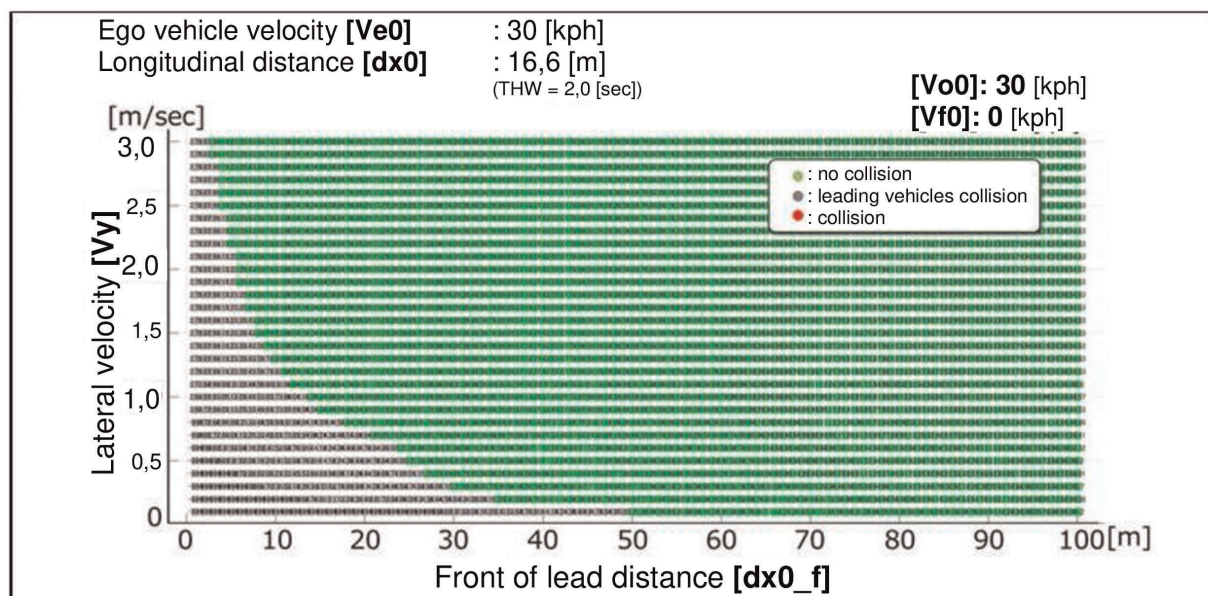
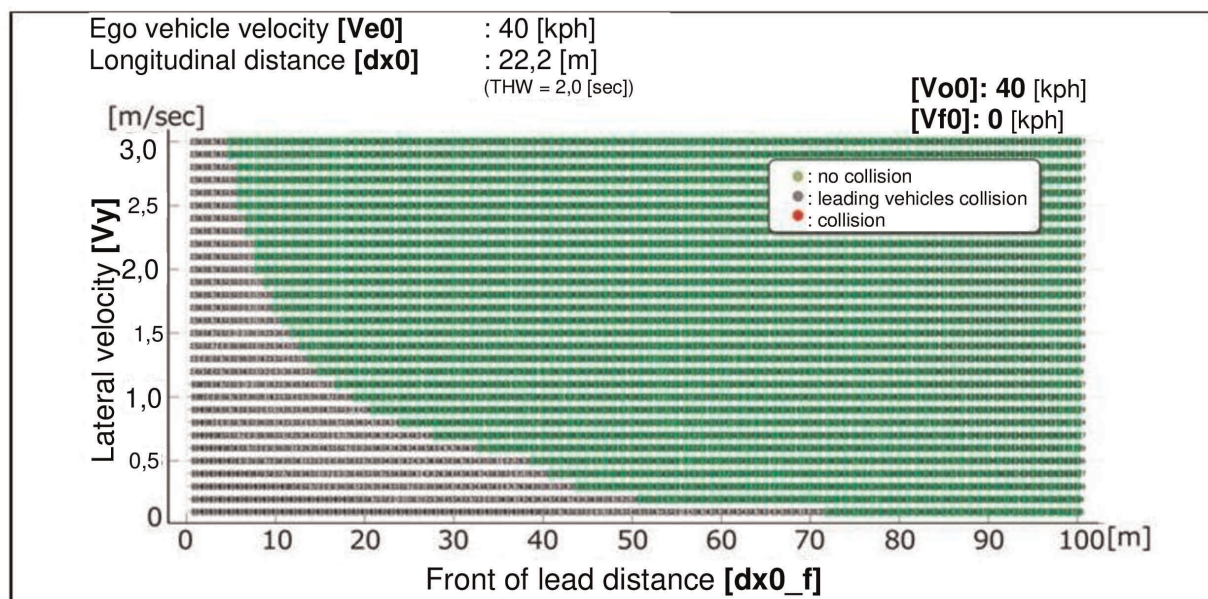
It is possible to avoid all the deceleration (stop) vehicles ahead of the preceding vehicle cut-out in the following running condition at THW 2,0 sec.

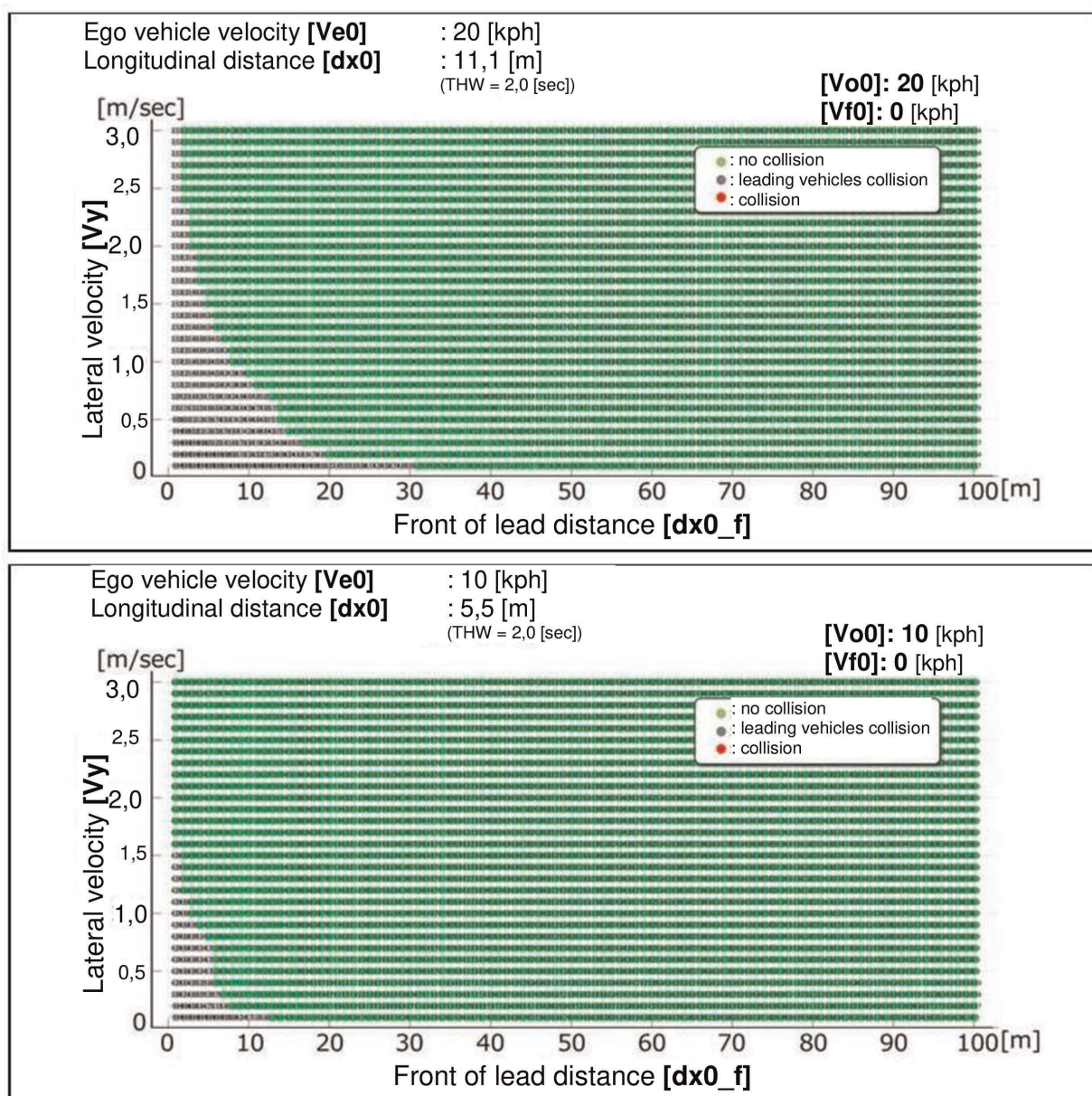
(Data sheets image)

Figure 13

Parameters







5.3. Deceleration

It is possible to avoid sudden deceleration of -1,0G or less in the follow-up driving situation at THW 2,0 sec.

(Data sheet image)

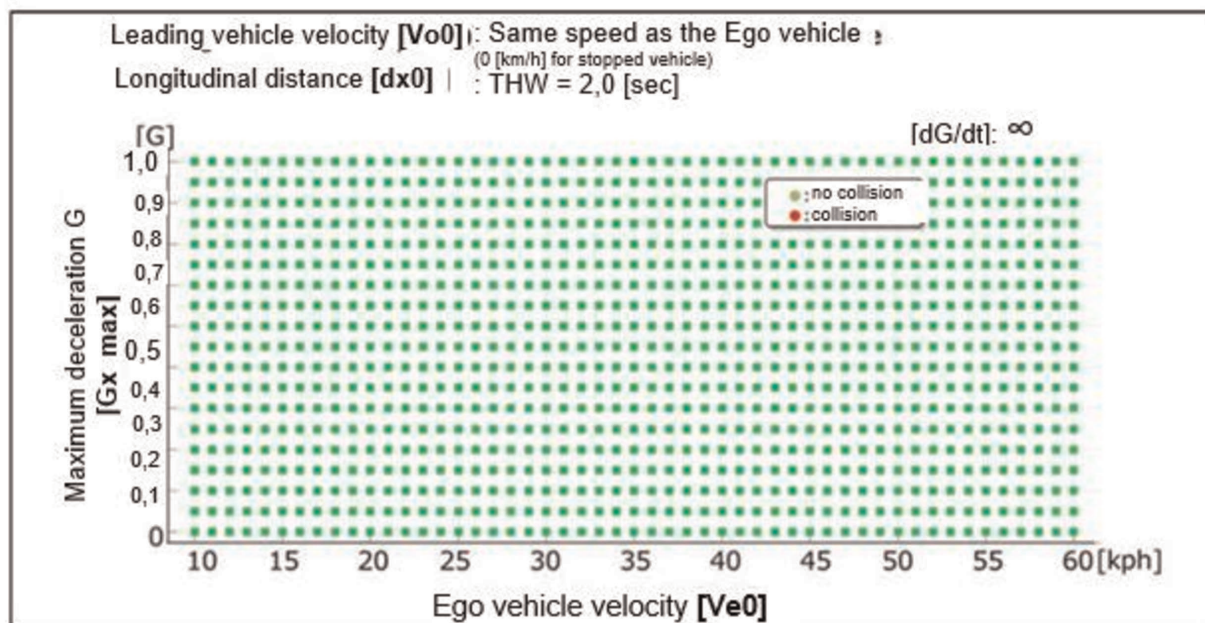
	Initial condition	Initial velocity	Ve0	Ego vehicle velocity
		Initial distance	Vo0	Leading vehicle velocity ¹
Vehicle motion			dx0	Longitudinal distance ²
	Deceleration		Gx_max dG/dt	Maximum deceleration G Deceleration rate ³

¹ Vo0 = Ve0 (Same speed as the leading vehicle)
 0 [km/h] for a stopped vehicle

² Follow the leading vehicle in THW = 2 sec

³ The most severe conditions ∞

(Data sheets image)



ANNEX 5

Test Specifications for ALKS**1. INTRODUCTION**

This annex defines tests with the purpose to verify the technical requirements on ALKS.

Until such time that specific test provisions have been agreed, the Technical Service shall ensure that the ALKS is subject to at least the tests outlined in Annex 5. The specific test parameters for each test shall be selected by the Technical Service and shall be recorded in the test report in such a manner that allows traceability and repeatability of the test setup.

Pass- and Fail-Criteria for tests are derived solely from the technical requirements in paragraphs 5 to 7 of the Regulation. These requirements are worded in a way that they allow the derivation of pass-fail-criteria not only for a given set of test parameters, but for any combination of parameters in which the system is designed to work (e.g. operating speed range, operating lateral acceleration range, curvature range as contained in the system boundaries).

The test specifications in this document are meant to be a minimum set of tests, the technical service authorities may perform any other test within the system boundaries and may then compare the measured results against the requirements (concrete: expected test outcome).

2. DEFINITIONS

For the purposes of this Annex,

- 2.1. 'Time to Collision' (TTC) means the value of time obtained by dividing the longitudinal distance (in the direction of travel of the subject vehicle) between the subject vehicle and the target by the longitudinal relative speed of the subject vehicle and the target, at any instant in time
- 2.2. 'Offset' means the distance between the vehicle's and the respective target's longitudinal median plane in driving direction, measured on the ground, normalized by the half the vehicle width excluding devices for indirect vision and corrected by adding 50 per cent.
- 2.3. 'Pedestrian Target' means a soft target that represents a pedestrian.
- 2.4. 'Passenger car Target' means a target that represents a passenger car vehicle.
- 2.5. 'Powered Two-Wheeler Target (PTW)' means a combination of a motorcycle and motorcyclist.

3. GENERAL PRINCIPLES**3.1. Test conditions**

- 3.1.1. The tests shall be performed under conditions (e.g. environmental, road geometry) that allow the activation of the ALKS.
- 3.1.2. If system modifications are required in order to allow testing, e.g. road type assessment criteria or road type information (map data), it shall be ensured that these modifications don't have an effect on the test results. These modifications shall in principle be documented and annexed to the test report. The description and the evidence of influence (if any) of these modifications shall be documented and annexed to the test report.
- 3.1.3. The test surface shall afford at least the adhesion required by the scenario in order to achieve the expected test result.

3.1.4. Test Targets

- 3.1.4.1. The target used for the vehicle detection tests shall be a regular high-volume series production vehicle of Category M or N or alternatively a 'soft target' representative of a vehicle in terms of its identification characteristics applicable to the sensor system of the ALKS under test according to ISO 19206-3:2018. The reference point for the location of the vehicle shall be the most rearward point on the centreline of the vehicle.
- 3.1.4.2. The target used for the Powered-Two-wheeler tests shall be a test device according to ISO CD 19206-5 or a type approved high volume series production motorcycle of Category L3 with an engine capacity not exceeding 600 cm³. The reference point for the location of the motorcycle shall be the most backward point on the centreline of the motorcycle
- 3.1.4.3. The target used for the pedestrian detection tests shall be an 'articulated soft target' and be representative of the human attributes applicable to the sensor system of the AEBS under test according to ISO 19206-2:2018.
- 3.1.4.4. Details that enable the target(s) to be specifically identified and reproduced shall be recorded in the vehicle type approval documentation.

3.2. Test parameter variation

The manufacturer shall declare the system boundaries to the Technical Service. The Technical Service shall define different combinations of test parameters (e.g. present speed of the ALKS vehicle, type and offset of target, curvature of lane) in order to cover scenarios in which a collision shall be avoided by the system as well as those in which a collision is not expected to be avoided, where applicable.

If this is deemed justified, the Technical Service may test additionally any other combination of parameters.

If a collision cannot be avoided for some test parameters, the manufacturer shall demonstrate either by documentation or, if possible, by verification/testing that the system doesn't unreasonably switch its control strategy.

4. TEST SCENARIOS TO ASSESS THE PERFORMANCE OF THE SYSTEM WITH REGARD TO THE DYNAMIC DRIVING TASK

4.1. Lane Keeping

- 4.1.1. The test shall demonstrate that the ALKS does not leave its lane and maintains a stable position inside its ego lane across the speed range and different curvatures within its system boundaries.

- 4.1.2. The test shall be executed at least:

- (a) With a minimum test duration of 5 minutes;
- (b) With a passenger car target as well as a PTW target as the lead vehicle / other vehicle;
- (c) With a lead vehicle swerving in the lane; and
- (d) With another vehicle driving close beside in the adjacent lane.

4.2. Avoid a collision with a road user or object blocking the lane

- 4.2.1. The test shall demonstrate that the ALKS avoids a collision with a stationary vehicle, road user or fully or partially blocked lane up to the maximum specified speed of the system.

- 4.2.2. This test shall be executed at least:

- (a) With a stationary passenger car target;

- (b) With a stationary powered two-wheeler target;
- (c) With a stationary pedestrian target;
- (d) With a pedestrian target crossing the lane with a speed of 5 km/h;
- (e) With a target representing a blocked lane;
- (f) With a target partially within the lane;
- (g) With multiple consecutive obstacles blocking the lane (e.g. in the following order: ego-vehicle -motorcycle - car);
- (h) On a curved section of road.

4.3. Following a lead vehicle

4.3.1. The test shall demonstrate that the ALKS is able to maintain and restore the required safety distance to a vehicle in front and is able to avoid a collision with a lead vehicle which decelerates up to its maximum deceleration.

4.3.2. This test shall be executed at least:

- (a) Across the entire speed range of the ALKS;
- (b) For a passenger car target as well as a PTW target as lead vehicle, provided standardized PTW targets suitable to safely perform the test are available;
- (c) For constant and varying lead vehicle velocities (e.g. following a realistic speed profile from existing driving database);
- (d) For straight and curved sections of road;
- (e) For different lateral positions of lead vehicle in the lane;
- (f) With a deceleration of the lead vehicle of at least 6 m/s² mean fully developed deceleration until standstill.

4.4. Lane change of another vehicle into lane

4.4.1. The test shall demonstrate that the ALKS is capable of avoiding a collision with a vehicle cutting into the lane of the ALKS vehicle up to a certain criticality of the cut-in manoeuvre.

4.4.2. The criticality of the cut-in manoeuvre shall be determined according to TTC, longitudinal distance between rear-most point of the cutting in vehicle and front-most point of the ALKS vehicle, the lateral velocity of the cutting-in vehicle and the longitudinal movement of the cutting-in vehicle, as defined in paragraph 5.2.5 of this Regulation.

4.4.3. This test shall be executed taking into consideration at least the following conditions:

- (a) For different TTC, distance and relative velocity values of the cut-in manoeuvre, covering types of cut-in scenarios in which a collision can be avoided and those in which a collision cannot be avoided;
- (b) For cutting-in vehicles travelling at constant longitudinal speed, accelerating and decelerating;
- (c) For different lateral velocities, lateral accelerations of the cut-in vehicle;
- (d) For passenger car as well as PTW targets as the cutting-in vehicle, provided standardized PTW targets suitable to safely perform the test are available.

4.5. Stationary obstacle after lane change of the lead vehicle

4.5.1. The test shall demonstrate that the ALKS is capable of avoiding a collision with a stationary vehicle, road user or blocked lane that becomes visible after a preceding vehicle avoided a collision by an evasive manoeuvre.

4.5.2. The test shall be executed at least:

- (a) With a stationary passenger car target centred in lane;
- (b) With a powered two-wheeler target centred in lane;
- (c) With a stationary pedestrian target centred in lane;
- (d) With a target representing a blocked lane centred in lane;
- (e) With multiple consecutive obstacles blocking the lane (e.g. in the following order: ego-vehicle – lane change vehicle – motorcycle – car).

4.6. Field of View test

4.6.1. The test shall demonstrate that the ALKS is capable of detecting another road user within the forward detection area up to the declared forward detection range and a vehicle beside within the lateral detection area up to at least the full width of the adjacent lane.

4.6.2. The test for the forward detection range shall be executed at least:

- (a) When approaching a motorcycle target positioned at the outer edge of each adjacent lane;
- (b) When approaching a stationary pedestrian target positioned at the outer edge of each adjacent lane;
- (c) When approaching a stationary motorcycle target positioned within the ego lane;
- (d) When approaching a stationary pedestrian target positioned within the ego lane.

4.6.3. The test for the lateral detection range shall be executed at least:

- (a) With a motorcycle target approaching the ALKS vehicle from the left adjacent lane;
- (b) With a motorcycle target approaching the ALKS vehicle from the right adjacent lane.

5. ADDITIONAL VERIFICATION

5.1. (Reserved)

5.2. Compliance with the following provisions shall be demonstrated by the manufacturer and assessed by the Technical Service at the time of type approval:

	Test/Check
6.2.2.	Off mode after new engine start/run
6.2.3	System can only be activated if (a) The driver is in driver seat & belt is fastened (b) The driver is available (c) No failures (d) DSSAD operational (e) Conditions are within system limits
6.2.1	Means of deactivating
6.2.4	Dedicated means to activate and deactivate
6.2.5	protected against unintentional action
6.2.6	Steering (a) Holding wheel and brake/accelerate (b) Driver holds steering wheel in response to transition and MRM (c) After deactivation
6.3	Means to override the system (a) Steering control (b) Braking input higher than system (c) Accelerating to speed within system limits
6.1.3.1.	Criteria for deeming driver available

	Test/Check
5.1.3	Driver support systems active
6.3.1.1.	Driver attentiveness
5.5	System behaviour during a Minimal Risk Manoeuvre (a) Driver take over (b) Standstill (hazard lights) (c) Re-activation disabled if reached standstill
5.1.4	Transition demand & behaviour/escalation
5.1.5	Driver resumes control
5.4	Without driver response (MRM) (a) Planned transition (b) Unplanned transition
6.1.2	Transition demand during operation
6.1.3	Exceed system parameters
5.4.	Failure (a) Detectable collision (b) Driver not present
5.3	System behaviour for Emergency Manoeuvre (a) Resulting in standstill (b) Not resulting in standstill
7.1	System detection areas
7.1.1	Front
7.1.2	Sides
7.1.3	Visibility

5.3. Additional other test cases may be assessed if it is deemed justified by the Technical Service. Some of the cases may include:

- (a) Y-split of highway lanes
- (b) Vehicles entering or exiting the highway
- (c) Partially blocked ego lane, tunnel
- (d) Traffic lights
- (e) Emergency vehicles
- (f) Construction zones
- (g) Faded/erased/hidden lane markings
- (h) Emergency/Service personnel directing traffic
- (i) Change in road characteristics (no longer divided, pedestrians permitted, roundabout, intersection)
- (j) Normal traffic flow resumed (i.e. all vehicles moving > 60km/h).

5.4. Real-world test

The Technical Service shall conduct, or shall witness, an assessment of the system, in a fault-free condition, in the presence of traffic (a 'real-world' test). The purpose of this test is to support the Technical Service in understanding the functionality of the system in its operating environment and to complement the assessment of the documentation provided under Annex 4.

Together, the assessment of Annex 4 and the real-world test shall enable the Technical Service to identify areas of system performance that may require further assessment, either through testing or further review of Annex 4.

During the real-world assessment, the Technical Service shall assess at least:

- (a) Prevention of activation when the system is outside of its technical boundaries/requirements for ALKS

- (b) No violation of traffic rules
- (c) Response to a planned event
- (d) Response to an unplanned event
- (e) Detection of the presence of other road users within the frontal and lateral detection ranges
- (f) Vehicle behaviour in response to other road users (following distance, cut-in scenario, cut-out scenario, etc.).
- (g) System override

The location and selection of the test route, time-of-day and environmental conditions shall be determined by the Technical Service.

The test drive shall be recorded and the test vehicle instrumented with non-perturbing equipment. The Technical Service may log, or request logs of any data channels used or generated by the system as deemed necessary for post-test evaluation.

It is recommended that the real-world test is undertaken once the system has passed all of the other tests outlined in this Annex and upon completion of a risk assessment by the Technical Service.

ISSN 1977-0677 (electronic edition)
ISSN 1725-2555 (paper edition)



Publications Office
of the European Union
L-2985 Luxembourg
LUXEMBOURG

EN