GUIDELINES ON THE EXEMPTION PROCEDURE FOR THE EU APPROVAL OF AUTOMATED VEHICLES

Version 4.1. The guidelines hereafter have been supported by the Technical Committee on Motor Vehicles of 12 February 2019

A. PURPOSE AND SCOPE OF THE GUIDELINES

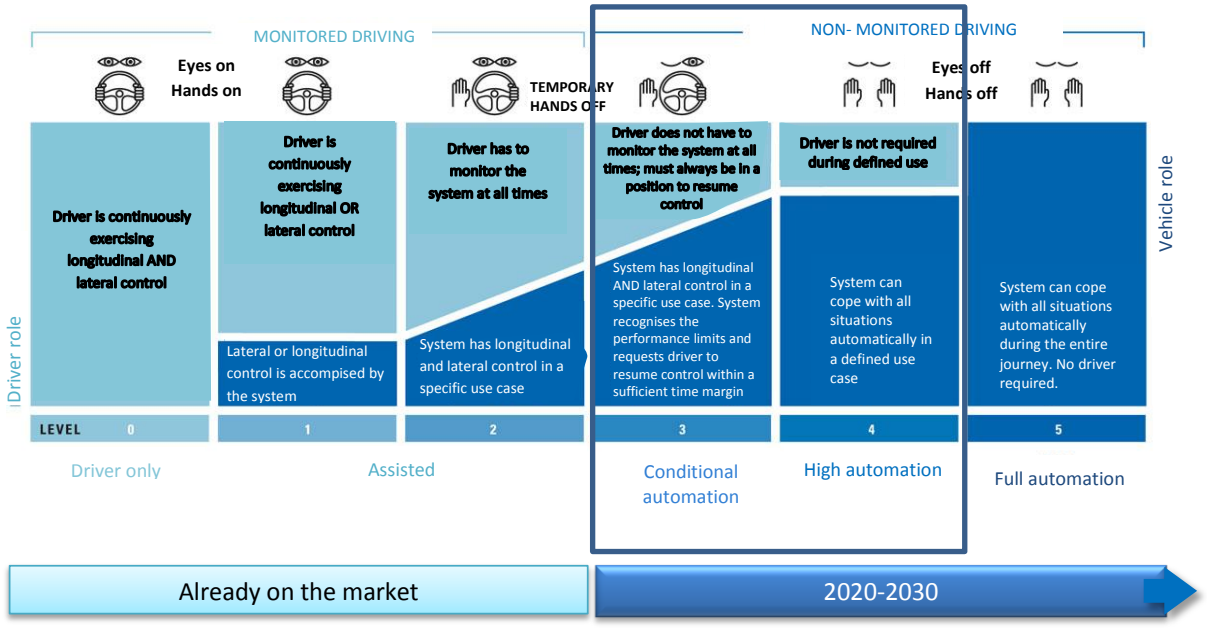
The Commission adopted on 17 May 2018 an EU strategy on automated and connected mobility (CAM)[1]. As part of the strategy, the Commission announced its intention to work with Member States in 2018 on guidelines to ensure a harmonised approach for exemption procedure for the EU approval of automated vehicles. This is the purpose of this document.

Technologies not foreseen by EU vehicle rules such as automated driving can already be approved through an EU exemption procedure[2]. Pending the adoption of harmonised EU requirements, the approval is granted on the basis of a national ad-hoc safety assessment which is mutually recognized by other Member States through a Commission decision. The vehicle type can then be placed on the EU market like any other EU approved vehicle.

The purpose of these guidelines is to harmonize the practice of Member States for the national ad-hoc assessment of automated vehicles and to streamline the mutual recognition of such assessment, as well as to ensure fair competition and transparency.

In line with the priorities of work proposed in the CAM strategy, the focus on these guidelines will be on automated vehicles that can drive themselves in a limited number of driving situations (SAE levels 3 and 4- see figure below) which are already being tested and are expected on a commercial basis by 2020.

Figure: Different levels of automation (source: Society of Automotive Engineers-SAE)



The EU exemption procedure is in principle limited to series production vehicles. For lower volumes or prototypes, other procedures exist (national individual approvals, national small series).

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0283

[2] Directive 2007/46/EC on the approval of motor vehicles (Article 20) to be replaced by Regulation (EU) No. 858/2018 on vehicle approval and market surveillance) (Article 39) from 1 September 2020.

B. PROCEDURE

(From Article 20 of Directive 2007/46 and Article 39 of Regulation (EU) No 858/2018)

1. The manufacturer shall apply in the type-approval authority of one Member State.

The layout of the documentation to be provided by the manufacturer can be found in Annex 1

2. The Member State may grant a provisional approval to the vehicle type, valid only in its territory, in respect of a type of vehicle covered by the exemption sought, provided that it informs the Commission and the other Member States thereof without delay by means of a file containing the following elements:

(a) the reasons why the technologies or concepts in question make the whole vehicle type incompatible with the requirements; It shall describe which systems, component and separate technical units are in compliance with the legislation and which ones are not. Interactions between the different systems of the vehicles for the automated driving function should also be considered.

(b) a description of the safety and environmental considerations concerned and the measures taken. These guidelines shall be used as a basis for the assessment of the automated driving function by the type-approval authority. As an alternative, the Commission and the Member States may agree to use a draft amendment to the relevant EU or UNECE requirements as a basis.

(c) a description of the tests, including their results, demonstrating that, by comparison with the requirements from which exemption is sought, at least an equivalent level of safety and environmental protection is ensured.

3. The Commission shall decide by means of an implementing act (Vote in the Technical Committee Motor Vehicles), whether or not to allow the Member State to grant an EC type-approval in respect of that type of vehicle(converting the provisional approval into an EC approval). The Commission decision shall be based on these guidelines, shall clearly identify the functionality concerned, the basis under which the approval was granted. The decision shall be made public.

Based on the risk assessment and possible upcoming harmonized requirements, the validity of the approval can be limited in time (minimum 36 month) or in numbers. If the necessary steps to adapt the regulatory acts have not been taken, the validity of an exemption may be extended with another Commission decision.

4. Pending the decision of the Commission, other Member States may decide to accept the provisional approval referred to in paragraph 2 on their territory.

5. The scope of an already granted exemption may be extended by another Commission decision on the basis of a simplified documentation provided by the type-approval authority explaning the difference between the new vehicle type and the vehicle type already covered by an exemption.

C. SAFETY REQUIREMENTS

1. SYSTEM PERFORMANCE IN THE AUTOMATED DRIVING MODE

1. When in the automated driving mode ("Operational Domain"-OD), the automated vehicle drives and shall replace the driver for all the driving tasks under the situations which can be reasonably expected in the OD.

2. When in the automated driving mode, the vehicle shall not cause any traffic accidents that are rationally foreseenable and preventable.

3. When in the automated driving mode, the vehicle shall have a predictable and careful behaviour and shall allow an appropriate interaction with other road users (e.g. obey to orders by authorities or communication with other road users when needed).

4. When in the automated driving mode ("Operational Domain"-OD), the automated vehicle shall drive in accordance with the traffic rules.

5. The manufacturer shall declare to the type-approval authority the scope of the automated driving mode (so called operational domain(s) (OD)) where and when the automated driving system is designed to operate. This shall include at a minimum:

- Road conditions (motorways/expressways, general roads, number of lanes, existence of lane marks, roads dedicated to automated driving vehicles, etc.)
- Geographical area (urban and mountainous areas, Geofence setting, etc.)
- Environmental conditions (weather, night-time limitations, etc.)
- Speed range
- Other conditions that must be fulfilled for the safe operation in the driving mode.

6. An automated driving system shall recognize whether or not the situation is within the set OD, and operate only in that OD.

7. The system shall be safe by design to cope with any situation within the OD (environment perception capabilities, ability to take right decisions and perform the right dynamic driving tasks and allow interaction with other road users) without continuous supervision by the driver. The vehicle design shall ensure that the vehicle will not cause any accident within the OD. The vehicle shall also be designed to minimize potential effects of errors from the vehicles' users, inside and outside of the vehicle, and of other road users.

8. In particular, the vehicle shall be able to keep a safe distance with other vehicles in front, exibit caution in occluded areas, leave time and space for others in lateral maneuvers, be cautious with right-of-ways and if an accident can be safely avoided without causing another it shall be avoided.

9. The OD shall be set in a way that it allows the driver to take over safely from the automated system (i.e. only take over requests in low risk situations) and in compliance with the relevant traffic rules.

10. The system shall detect when it is difficult to continue in the automated driving mode, for instance when reaching the boundaries of the OD or in case of failure.

2. DRIVER/OPERATOR/PASSENGER INTERACTION

11. The activation of the automated driving mode shall only be possible when the conditions of the OD are met. Means shall be provided to humans (driver or if no driver, passenger or operation control center) to deactivate or override immediately the automated mode in an easy manner. The system may however momentarily delay deactivation when an immediate human deactivation could compromise safety.

12. The vehicle shall always inform the driver (or person responsible for operation) or passengers about the operational status (operational, failure, etc.) of the system in an unambiguous manner.

13. The driver shall be made aware of the use and the limits of the automated driving mode, as well as which tasks other than driving may be enabled by the system for the driver[3].

14. If the system is designed to request the driver to take over under some circumstances, the system shall monitor whether the driver is ready to take over driving from the system. It shall ensure through appropriate design (e.g. driver monitoring system) and warnings that the driver remains available to respond to take over request and prevent any foreseeable and preventable misuse by the driver in the OD.

15. For vehicles designed to operate only with no driver (e.g. driverless shuttles), a communication function shall be provided to send an emergency notification to an operation control centre. A camera and voice communication device shall be provided in the vehicle so that an operation control centre can monitor the situation inside the vehicle.

3. TRANSITION OF THE DRIVING TASKS

16. The system may request the driver to take over with a sufficient lead time in particular when the system determines that it is difficult to continue automated driving mode, such as when the situation becomes outside the OD, or when a problem has occurred to the automated vehicle.

17. The system shall remain in the automated driving mode as long as the driver has not taken over, and/or will otherwise transfer to a minimum risk manoeuvre.

18. The system shall be designed to enable the driver to clearly recognize the take over request from the system.

19. The system shall be able to determine whether or not the driver has taken over.

4. MINIMUM RISK MANOEUVRE

20. When the system detects that it is difficult to continue in the automated driving mode, it shall be able to transfer to a minimal risk condition (with or without take over request) through a minimal risk manoeuvre.

21. Other road users shall be informed that the vehicle is performing a minimum risk manoeuvre in accordance with applicable traffic rules (e.g. hazard lights, brake lights, turning indicators).

[3] This is only about the technical capability of the system and without predjudice to national traffic rules.

22. The Minimum Risk Manoeuvre (MRM) shall comply with traffic rules. MRM settings for automated vehicles may include measures to stay in or change the lane while warning to the surrounding and automatically stop the vehicle in a safe manner on the side of the road. The driver may be asked to take over at the end of the minimum risk manoeuvre (e.g. to park on the side of the road in case of level 3 lane keeping system).

5. INSTALLATION OF EVENT DATA RECORDERS

23. Automated vehicles should be equipped with an on-board device that records the operational status of the automated driving system and the status of the driver to determine who was driving during an accident.

24. This data collected shall allow to assign liability in case of accident and shall allow to assess if the driver or the vehicle properly reacted to the situation. It shall at least include the operation status of the automated driving system, state of the driver, information on surrounding, control information of the vehicle.

25. The on-board device shall be able to cope with a vehicle crash (similar to ecall e.g resistance to heavy accelearation and fire).

26. The on-board device shall be able to store data in a secured manner, comply with EU data protection legislation and be protected against manipulation. It shall also allow the access by relevant national authorities.

27. More specific requirements for data recording devices (recording time, retention time, for what purposes data is used, standardized access, how to handle personal information, etc.) may be developed on the basis of the experience gained.

6. CYBERSECURITY

28. The Vehicle shall be designed to protect the vehicle against automated vehicle hacking using state of the art techniques[4] and comply with EU data protection legislation. This includes risk assessment by the manufacturer, design measures and adequate processes to avoid, mitigate and react to cyber attacks.

29. Vehicle manufacturers shall take measures such as those related to updating of software, etc., installed in automated vehicles necessary to ensure in-use cybersecurity over its lifetime.

7. SAFETY ASSESMENT AND TESTS

30. Automated vehicles, their systems, components and technical units shall comply to the largest extent with the existing EU Safety Regulations listed in Annex IV to Directive 2007/46/EC, unless they are incompatible with the purpose of the automated vehicles.

31. The Type-approval authority shall assess that the manufacturer has put in place a robust design and validation process of the automated system with the goal to ensure that the vehicle complies with these guidelines, particularly that it will not cause accidents and will provide safe take over requests and minimum risk manoeuvres. The type-approval authority shall make a finding of safety equivalence based on the manufacturer's safety evaluation report documenting testing, validation, and assessment.

[4] See for instance the most recent requirements on cybersecurity by the UN (WP.29) or other organizations (SAE J3061 and ISO/SAE21434).

32. The manufacturer shall in particular demonstrate that it has conducted a hazard and safety risk analysis for the automated system, its integration in the overall vehicle design and the broader transportation ecosystem and put in place adequate design and redundancy to cope with these risk and hazards (safety concept).

33. Systems shall in particular be designed to cope with risks that could impact safety critical functionality due to cyber-attacks and failure (functional safety) but also potential inadequate control, undesirable control actions, driver misuse and inadequate interaction with other road users (operational safety). Relevant demonstration methods include ISO 26262 for functional safety[5] and a system-theoretic process analysis (STPA)[6] for operational safety or an equivalent method such as draft ISO PAS 21448.

34. All design decisions shall be tested, validated and verified by the manufacturer as individual subsystem and as part of the entire vehicle architecture.

35. The type-approval authorities or the technical services acting on their behalf shall make a finding of safety equivalence based on the manufacturer's safety evaluation report documenting testing, validation, and assessment methods listed above. They shall verify that the hazard and safety risk analysis is designed to cover all types of system failures and driving hazards for the system concerned, and to assess their criticity. They shall assess that the logical chart of responses to risk (e.g. redundancy, manoeuvers) covers the range of identified system failures and driving hazards. They shall ensure that the human – machine interactions have been properly assessed, based on a relevant set of tests and users. They shall carry out a minimum number of tests to verify that the vehicle subject to the exemption operates safely from the functional and operational safety point of view considering on one hand the most critical failure and driving scenarios, and on the other hand, the carefulness and understandability of operation by other road users in non critical scenarios. They shall ensure that there is a transparent method of measuring the operational/run-time performance of the system. The minimum number of tests should include false negative and false positive test scenarios. Simulation method may be used, subject to their validation the approval authorities/technical services in accordance with the procedure for virtual testing in Directive 2007/46/EC or Regulation 858/2018.

36. The type-approval authorities or the technical services acting on their behalf shall have access to the system to carry out the vehicle safety assessment.

37. The type-approval authority or/and the technical services acting on its behalf shall have the necessary competences, certifications and training to carry out the vehicle safety assessment and tests listed above.

8. INFORMATION PROVISION TO AUTOMATED VEHICLE USERS

38. Vehicle manufacturers shall inform automated vehicle users of the following points using easy-to-understand materials, etc., and take measures to make them understandable:

- Operational conditions of the system, scope of OD, functional limitations
- Means to deactivate the automated driving mode
- Driver's tasks (such as the need for the driver to take over driving when the system cannot continue driving for level 3 vehicles)
- Possible action to take other than driving according to the performance of the system and its operation status (for level 3 vehicles)

[5] Not covering cyber attacks however.
[6] See for instance http://uspas.fnal.gov/materials/14JAS/JAS14-Thomas-Lecture.pdf

- Information related to indications by HMI (whether or not the automated driving system is operating, etc.)
- User behaviour to adopted in case of urgency
- Behaviours of the vehicle when a problem has occurred to the system
- Need to conduct proper maintenance (inspection) and software update of in-use automated vehicles.

ANNEX I: INFORMATION TO BE PROVIDED BY THE VEHICLE MANUFACTURER

1. SYSTEM PERFORMANCE IN THE AUTOMATED DRIVING MODE

a) Automated System Type Definition
b) Automated Driving Functions
c) Operational Domain:
    1. Speed, road type, country
    2. Environment
    3. Road Conditions
d) Basic Performance (e.g. max. lateral acceleration, …)
e) Tasks other than driving technically enabled by the system

A. ENVIRONMENT PERCEPTION

a) With respect to operation domain
b) Lanes / Objects
c) Redundancy (with respect to system performance)
d) Sensor monitoring:
    1. Plausibility check with respect to misuse
    2. Implemented monitoring system or degradation considered.
e) Connectivity
f) Maps

B. DYNAMIC DRIVING TASK AND INTERACTION WITH OTHER ROAD USERS

a) Have a predictable and careful behaviour:
    1. Driving in accordance to the speed limits (explicit and implicit)
    2. Obeying passing restrictions
    3. Adapting the speed of the vehicle to environmental conditions (e.g. rain, fog, curves, hilltops, sun glaring) affecting:
        - Adhesion of the road
        - Viewing distance of the system
    4. Keeping the required minimum distance to other road users
    5. Rules regarding the preferred lane of travel ("Drive on the rightmost lane")
    6. Compliance with relevant country specific traffic rules (respecting road markings and road signs)
b) React to:
    1. Other vehicles within the ego lane or in the neighbouring lanes (e.g. other vehicle cutting into the ego lane, neighbouring vehicle driving too close or across the lane marking)
    2. Vulnerable road users (if applicable in the OD)
    3. Police and Emergency Vehicles
    4. Law enforcement injunctions (police control, compliance with officers' regulations)

2. DRIVER INTERACTION

a) Activation / Deactivation / Modes (on / off / standby)
b) Overriding / Human driver priority
c) Human Machine Interface (HMI):
    1. Driver Information (Operation Status, Failure)
    2. Optical Warning Signal (type and operation mode)
    3. Acoustic / Haptic Warning Signals (type and operation mode)
d) Driver Presence and Responsiveness Recognition System
e) Extract of the relevant part of the owner`s manual

f) Means to prevent misuse and manipulation

3. TRANSITION OF THE DRIVING TASK

a) Planned:
   1. Boundary conditions
   2. System behaviour
   3. System performance
b) Unplanned (incl. mayor system failure):
   1. Boundary conditions
   2. System behaviour
   3. System degradation
   4. System performance
c) Emergency (only in case of imminent danger of a collision):
   1. Boundary conditions
   2. System behaviour
   3. System performance

4. MINIMUM RISK MANOEUVRE

a) Description of the different risk manoeuvres for the different scenarios (e.g. planned and unplanned events)

5. DATA STORAGE SYSTEM

b) Type of Data stored
c) Storage location
d) Storage duration
e) Means to ensure data security and data protection
f) Access to the data

6. CYBER SECURITY

Description of the different risks and measures put in place to mitigate these risks.
Description of the update procedure.

7. SAFETY ASSESSMENT AND TESTING

Design and validation process to be validated by the technical service and confirmed by the approval authority:

-Assessment of the functional and operational safety for the automated system design.

-Test of the functionality

-Tests in case of system failure:

1. Measurement equipment used
2. Test conducted by the technical service/type-approval authority
3. Description of in-use tests

8. INFORMATION PROVISIONS TO USERS

Model of the information provided to users.