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

A. PURPOSE AND SCOPE OF THE GUIDELINES

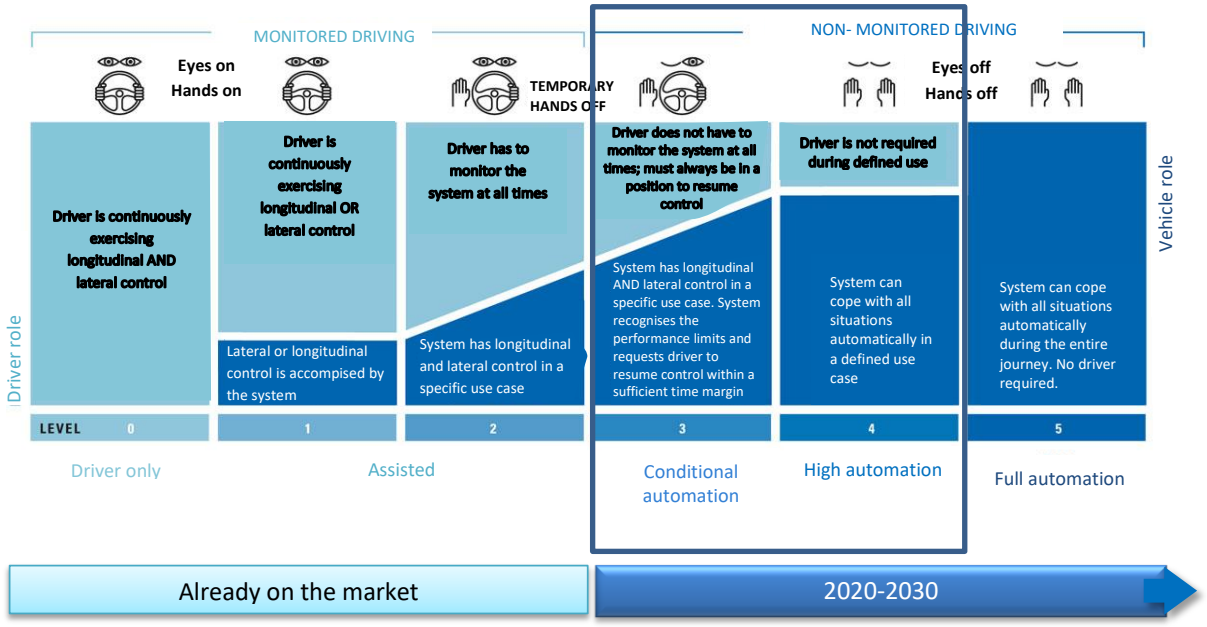
The Commission adopted on 17 May 2018 an EU strategy on automated and connected mobility (CAM)[1]. As part of the strategy, the Commission announced its intention to work with Member States in 2018 on guidelines to ensure a harmonised approach for exemption procedure for the EU approval of automated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

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. In case a discussion is already on going to amend the relevant EU or UNECE requirements, the baseline draft version may be used. The draft version is assigned at the date of application at the Type Approval Authority on the basis of the description of the system provided by the Member State to the other Member states and the Commission. Deviation to the draft version(s) at the date of granting the approval shall be indicated, explained and proposal for modification made. In case of missing items in the draft, the appropriateness of OEM internal requirements shall be assessed by the Member state in accordance with these guidelines.

(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. The Commission decision shall be based on these guidelines shall clearly identify the functionality concerned, the basis under which the approval was granted and be made available upon request.

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.

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

C. SAFETY REQUIREMENTS

1. SYSTEM PERFORMANCE IN THE AUTOMATED MODE

xx. When in the automated mode ("Operational Domain"-OD), the automated vehicle drives in accordance with the traffic rules and shall replace the driver for all the situations which can be reasonably expected in the OD (shall a minimum OD should be required?).

xx. The vehicle shall not cause any traffic accidents within the OD.

xx. When in the automated mode, the vehicle shall have a predictable and careful behaviour and shall allow an appropriate interaction with other road users and law enforcement authorities.

xx. The manufacturer shall declare to the type-approval authority the scope of the automated 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 vehicles, etc.)
- Geographical area (urban and mountainous areas, Geofence setting, etc.)
- Environmental conditions (weather, night-time limitations, etc.)
- Speed range
- Other conditions

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

xx. The system shall be designed to cope with any situation within the OD (environment perception capabilities, ability to take right decisions and perform the right dynamic driving tasks and 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.

xx. The OD shall be set in a way that it allows the driver to take over safely from the automated system and in compliance with the relevant traffic rules.

2. DRIVER/OPERATOR/PASSENGER INTERACTION

xx. The activation of the automated 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) to deactivate immediately in an easy manner the automated mode. The system may however momentarily delay deactivation when immediate human deactivation could compromise safety.

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

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

xx. The driver shall be made aware of the use and the limits of the automated mode as well as the side tasks for the driver that may be enabled by the system.

xx. For driverless systems, 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. A function shall be provided to send an emergency notification to the operation control centre.

xx. If the system is designed to request the driver to take over under some circumstances, the system shall monitor permanently whether the driver is ready to take over driving from the system. It shall ensure through appropriate design (driver monitoring system, etc.) 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.

3. TRANSITION OF THE DRIVING TASKS

xx. 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, such as when the situation becomes outside the OD, or when a problem has occurred to the automated vehicle.

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

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

xx. The system shall be able to determine whether or not control authority has been transferred from the system to the driver.

4. MINIMUM RISK MANOEUVRE

xx. When the system determines that it is difficult to continue automated driving, it shall be able to transfer to a minimal risk condition (with or without take over request) through a minimal risk manoeuvre in accordance with national traffic rules.

xx. The Minimum Risk Manoeuvre (MRM) shall comply with traffic rules(need for specific traffic rules for MRM?) . 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. The driver may be asked to take over at the minimum risk manoeuvre (e.g. to park on the side of the road in case of level 3 lane keeping system).

xx. Other road users shall be informed unambiguously that the vehicle is performing a minimum risk manoeuvre in accordance with applicable traffic rules.

5. INSTALLATION OF DATA STORAGE SYSTEM

xx. 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.

xx. The data shall at least include the operation status of the automated driving system, state of the driver, information on surrounding, control information of the vehicle. Further Specific data to be recorded need further discussion.

xx. Specific requirements for data recording devices (recording time, retention time, for what purposes data is used, standardized access, how to handle personal information, etc.) need further discussion.

xx. The on-board device shall be able to cope with a vehicle crash.

6. CYBERSECURITY

xx. The Vehicle shall be designed to protect the vehicle against automated vehicle hacking[3].

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

7. SAFETY ASSESMENT AND TESTS

xx. Automated vehicles, their systems, components and technical units shall comply to the largest extent with the existing EU Safety Regulations unless it is incompatible with the purpose of the automated vehicles.

xx. The Type-approval authority shall check 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 in particular will not cause accident and will provide safe take over requests and minimum risk manoeuvres an.

xx. The manufacturer shall in particular conduct 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).

xx. System shall in particular be designed to cope with risks that could impact safety critical functionality due to fault, cyber-attacks and failure (functional safety) but also potential inadequate control, undesirable control actions, misuse and inadequate interaction with other road users (operational safety). Relevant methods include the latest version of Annex 6 of UN Regulation 79 and ISO 26262 for functional safety and a system-theoretic process analysis (STPA) for operational safety.

[3] See for instance the most recent requirements on cybersecurity by the UN (WP.29) or other organizations

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

xx. The type-approval authorities shall carry out a minimum number of check and tests to verify that the process put in place by the manufacturer for the particular type of vehicle subject to the exemption is safe from the functional and operational safety point of view.

xx. The type-approval authority and the technical services acting on its behalf shall have the necessary competences and training to carry out the vehicle safety assessment and tests.

8. INFORMATION PROVISION TO AUTOMATED VEHICLE USERS

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

- Operational conditions of the system, scope of OD, functional limitations
- 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)
- Information related to indications by HMI (whether or not the automated driving system is operating, etc.)
- 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 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) Allowed side tasks

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

B. DYNAMIC DRIVING TASK AND INTERACTION WITH OTHER ROAD USERS

a) Comply with relevant Traffic Rules
    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
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
    3. Police and Emergency Vehicles

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 (planned unplanned event)

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

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