|  |  |
| --- | --- |
| Transmitted by the expert from EC for subgroup 2a | Document: VMAD-05-06 |

**Draft Annex on audit/assessment to the new UN Regulation on Automated Lane Keeping systems (ALKS)**

I Justification

As agreed at the last VMAD meeting, this text was drafted as an Annex to the new regulation on Automated Lane Keeping systems (ALKS) to address the “audit/assessment/simulation/in use reporting” pillar when applied to Automated Lane Keeping Systems. The track changes show the amendments to the current Annex to UN Regulation 79 (steering systems) on Complexed Electronic Systems (CEL) as lastly amended.

Main changes to current CEL Annex are the following:

-Tailor it to Automated driving functions (i.e. ALKS), not a generic annex for any electronic/driver assistant systems.

-Cover operational safety and not only functional safety

-Clarify the safety target (free from unreasonable risk for humans)

- Clarify that the type-approval authority is main responsible authority (or the technical service on their behalf) for the audit as it is the case for the rest of the type approval.

-Clarify that manufacturer is main responsible for safety

-Documentation layout and transparency of information across authorities

-Competences of the auditor.

-Content of the manufacturer safety management system (safety culture) including lifetime/lifecycle aspects

-Basic requirements for the use virtual testing/ simulation tools

This text is in line with the 3 other papers submitted by subgroup 2a to VMAD at this session, namely the concept paper and the proposed building blocks for audit/assessment reporting pillar. However compared to the building blocks some elements have not been included at this stage due to the time constraints:

-Independent demonstration of safety of subsystems by suppliers

-Several steps of assessment (e.g. at design and at production stages)

- Renewal of the assessment/audit. Monitoring by the authority.

-Rating of audit (major/minor failure,etc).

The discussion on this text is still on-going in subgroup 2a. However a number of issues would benefit from the discussion in VMAD, namely:

-the interaction with the work of other groups in particular with the groups dealing with physical testing (subgroup 2b and ACSF informal group dealing with the ALKS regulation).

-whether some requirements fit better in this annex of as part of the main part of the ALKS regulation.

-whether this annex shall be drafted only for ALKS or already for future AD systems.

-Scope and limits of the inspection done by authorities and responsibility of manufacturers in terms of safety.

-Whether ‘free of unreasonable risk’ can be used instead of ‘shall not induce safety critical risk’. Whether we can go beyond

-Level of information to shared amongst authorities and what shall kept at manufacturer level.

II Proposal

Annex X

 Special requirements to be applied to the functional and operational safety aspects of [automated driving systems/ALKS] (former CEL Annex)

1. General

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

It covers the (How it interlinks with other parts of the regulation) 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 "The System" meets the performance requirements specified in this UN Regulation, that it is designed/developed to operate in such a way that the automated driving system is free of [unreasonable/critical] 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/precesses described in documentation are actually implemented by the manufacturer.

[Based on the provided documentation, evidence and audits/assessments carried out to the satisfaction of the type approval authority concerning this Regulation, the residual level of risk of the assessed ALKS is deemed to be acceptable. The overall vehicle safety remains the responsibility of the manufacturer.]

2. Definitions

 For the purposes of this annex,

2.1. “*The System*” means a “*Higher-Level Electronic Control” system* that provides the automated driving function(s) regulated by this Regulation. This also includes any transmission links to or from other systems that are outside the scope of this Regulation, that acts on the function to which this Regulation applies.

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 fall-back to partial operation or even to a back-up system for vital vehicle functions may 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 vehicle control 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.

2.5. "*Higher-Level Electronic Control*" systems/functions are those electronic control systems, which employ additional processing and/or sensing provisions to modify vehicle behaviour by commanding variations in the function(s) of the vehicle control system. This allows complex systems to automatically change their objectives with a priority which depends on the sensed circumstances.

2.6. "*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.

2.7. "*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.

2.8. "*Range of control*" refers to an output variable and defines the range over which the system is likely to exercise control.

2.9. "*Boundary of functional operation*" defines the boundaries of the external physical limits within which the system is able to maintain control of the dynamic driving task.

2.9.1. “Operational design domain” (ODD) of the automated driving 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 driving system is designed to operate without any intervention by the driver . [It includes [transition demands and minimum risk manoeuvres issued by the system].

2.10. "*Safety Related Function*" means a function of "The System" that is capable of changing the dynamic behaviour of the vehicle. "The System" may be capable of performing more than one safety related function.

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.x.x. Functional safety: absence of unreasonable risks under the occurrence of hazards caused by a malfunctioning behaviour of E/E systems

2.x.x. 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.x.x. Failure means the termination of an intended behaviour of an element or an item.

2.x.x. Operational safety means the absence of unreasonable risk under the occurrence of hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons (safety hazards — without system failure).

[2.xx. “Non-fault” conditions means system operating conditions without occurrence of system-faults, but including the occurrence of external influences within the ODD (e.g. environmental conditions like fog, rain, shadows, sunlight or headlight glare) that may affect the automated lane keeping system’s performance (e.g. reduce the detection range of the sensing system) that can result in safety-relevant system reaction.]

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.

The Type-approval authority shall assess the documentation package to show that "The System" within the declared ODD:

(a) Is designed and was developed to operate, under non-fault and fault conditions, in such a way that it is free from unreasonable risks for the driver, passengers and other road users;

(b) Respects, under non-fault and fault conditions, 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.

(d) Is designed to recognize its ODD limits under non-fault and fault conditions

 (e) Does not operate outside of the declared ODD and any attempt to activate the System outside of the ODD will not lead to activation

3.1.1. Documentation shall be made available in 3 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 section 3. (with the exception of that of paragraph 3.4.4.) which shall be supplied to the Type-approval authority at the time of submission of the type approval application. 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 is definitely discontinued.

(b) Additional material and analysis data of paragraph 3.4.4. which shall be retained by the manufacturer, but made open for inspection at the time of type approval. 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 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 achieve the objectives, including a statement of the mechanism(s) by which control is exercised. The manufacturer shall describe the interactions expected between the system with the driver, passengers and other road users.

Any described function that can be over-ridden shall be identified and a further description of the changed rationale of the function’s operation provided.

Any enabled or disabled automated driving functions providing when 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.

3.2.x For the automated driving function, the manufacturer shall in particular provide a clear description of the system architecture for the following sub-functions of the automated driving systems:

-Perception and objects detection including mapping and positioning

- Characterization of the decision-making safety

- Human-machine interactions including the driver but also passengers and other road users

- Supervision and remote monitoring (if applicable).

- Documented data processing in case of continuous learning implemented.

3.2.x A description of the ODD under which the ALKS is designed to operate

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 indication 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 system performance.

3.2.3.x Interaction concept with the driver when (ODD-) Limits are reached shall be explained including an overview of types of situations in which the system will generate a transition demand to the driver.

.

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:

- Perception and objects detection including mapping and positioning

- Decision-making

- Supervision and remote monitoring (if applicable).

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 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 The manufacturer shall provide a clear identification of safety critical components, functions; units and software for the following sub-systems:

-Perception and objects detection including mapping and positioning

- Characterization of the decision-making safety

- Human-machine interactions including the driver but also passengers and other road users

- Supervision and remote monitoring (if applicable).

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 under fault and non-fault conditions.

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. The manufacturer shall show evidence of the means by which they determined the realisation of the system logic, during the design and development process.

3.4.3. The Manufacturer shall provide the Technical Service 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 conditions, then these conditions shall be stated and the resulting limits of effectiveness defined.

3.4.3.2. If the chosen provision selects a second (back-up) means to realise the vehicle control system objective, 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 Higher Level Function, this shall be done in compliance with the relevant provisions of this regulation (on minimum risk manoeuver and transition demand). All the corresponding output control signals associated with this function shall be inhibited, and in such a manner as to limit the transition disturbance.

3.4.4. The documentation shall be supported, by an analysis which shows, in overall terms, how the system will behave on the occurrence of any of those hazards or faults which will 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).

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 as 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, or any other testing appropriate for validation/verification.

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

(i) interactions with other vehicle systems (e.g. braking, steering);

(ii) Malfunctions (failures) of the automated lane keeping system and system risk mitigation reactions;

(iii) Situations within the ODD when a system free from faults may create safety critical risks for the driver, passengers and other road users (e.g. lack of or wrong comprehension of the vehicle environment, inadequate control, challenging scenarios)

(iv) Identification of the relevant scenarios within the ODD including traffic critical scenarios defined elsewhere in this regulation and management method used to select scenarios and validation tool chosen

(v) Decision making resulting in vehicle control and interaction with other road users and in compliance with traffic rules

(vi) Reasonably foreseeable misuse by the driver

(vii) Intentional modification of the system (tampering)

(viii) Cyber-attacks having an impact on the safety of the vehicle (through the analysis done with the cyber regulation).

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 and have been completed.

It shall demonstrate that the vehicle is free from unreasonable risks for the driver; passengers and other road users in the operational design domain. The safety demonstration shall include:

- a quantitative pre-validation target (e.g., using validation acceptance criteria), documented by the manufacturer, demonstrating that the introduction of the ADS will overall not increase the level of risk for the driver, passengers and other road users compared to a manually driven vehicles.

- a qualitative based approach, showing that the most relevant critical scenarios have been addressed and that the overall level of risks has been minimized to an acceptable level for the driver, passengers and other road users.

The Type-approval authority shall perform or shall require to perform 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 fault condition of the type defined in paragraph 3.4.4. of this annex, the warning signal to be given to the driver/passengers/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, passengers 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

3.5.1 In respect of software and hardware employed in “The System”, the manufacturer shall demonstrate to the type approval authority that effective processes/methodologies are in place, up to date and being followed within the organization throughout the product lifecycle (design, development, production, operation including respect of traffic rules, decommissioning).

3.5.2. The design/development process shall be include 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 functional/operational safety, cybersecurity and any other relevant disciplines related to the achievement of vehicle safety.

3.5.4. The manufacturer shall demonstrate that continuous independent internal audits are carried out to ensure that these processes

3.5.5. Manufacturers shall put in place suitable arrangements (e.g. contractual arrangements, clear interfaces, quality management system) with suppliers to ensure that the manufacturer safety management system is implemented by suppliers

3.5.6. The manufacturer shall have processes to monitor safety-relevant incident/accidents with engaged automated driving systems and a process to manage potential safety-relevant gaps post-registration are implemented consistently (closed loop of field monitoring). They shall report critical incidents (e.g. collision with another road users) to the type-approval authorities when they occur..

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-fault 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,.

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 failure in an~~y~~ individual unit by applying corresponding output signals to electrical units or mechanical elements in order to simulate the effects of internal faults 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 event detection and characterization of the decision-making and HMI functions of the system within the ODD (e.g. object difficult to detect or when the system reaches the boundaries). This shall include checking a number of critical traffic scenarios declared by the manufacturer in section 3 that are revelant for the ODD concerned.

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 by

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.

6. Communication to the other type –approval authorities (See appendix 3- Could also be annexed to the Communication form)

 -Description of the ODD and the high level functional architecture focusing on the functions available to the driver, passengers and other road users.

 -Test results during the verification process by the type approval authorities.

7. Competence of the auditors

 The assessments under this Annex may only be conducted by auditors with the technical and administrative knowledge necessary for such purposes. They shall in particular be qualified as auditor for functional and operational safety in accordance with ISO 26262-2018: on functional safety for road vehicles and ISO PAS ISO/PAS 21448: Safety of the Intended Functionality of road vehicles and being able to make the link with cybersecurity (ISO/SAE DIS 21434).

Annex X - Appendix 1

Model assessment form for automated driving systems

Test report No:

**1. Identification**

1.1. Vehicle make:

1.2. Type:

1.3. Means of identification of type if marked 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":

2.4. General description:

2.5. Description of all the control functions of “The System”, and methods of operation:

2.6. 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, passengers and other road users under fault and non-fault conditions*.*

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

3.4. Explanation of design provisions built into "The System" under fault and non fault conditions:

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 X to UN Regulation No. XX:

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

3.10. Date of test:

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

Technical Service~~[[1]](#footnote-1)~~ carrying out the test
Signed: ....................................... Date: ........................................

3.12. Comments:

Annex X - Appendix 2: Information document to be provided by the manufacturer for the approval

1. **Overall description of the system**
	1. Automated System Type Definition
	2. Operational Design Domain (Speed, road type, country, Environment, Road conditions)
	3. Main conditions for Minimum risk manoeuvres and transition demands
	4. Main automated Driving Functions (functional architecture)
	5. Basic Performance (e.g. max. lateral acceleration, OEDR …)

1.6. Tasks other than driving technically enabled by the system

**2. System performance in the automated driving mode**

2.1. Environment Perception

With respect to operation domain

Lanes / Objects

Redundancy (with respect to system performance)

Sensor monitoring:

Plausibility check with respect to misuse

Implemented monitoring system or degradation considered.

Connectivity used for the system

Maps

2.2. Dynamic Driving Task and interaction with other road users

Have a predictable and careful behaviour

Driving in accordance to the speed limits (explicit and implicit)

Obeying passing restrictions

Adapting the speed of the vehicle to environmental conditions (e.g. rain, fog, curves, hilltops, sun glaring) affecting:

Sensing of the adhesion of the road

Sensing distance(s) of the system

Keeping the required minimum distance to other road users

Rules regarding the preferred lane of travel (“Drive on the rightmost lane”)

Compliance with relevant country specific traffic rules (respecting road markings and road signs)

React to:

-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)

-Vulnerable road users (if applicable in the OD)

-Police and Emergency Vehicles

-Law enforcement injunctions (police control, compliance with officers' regulations)

2.3. Driver Interaction

Activation / Deactivation / Modes (on / off / standby)

Overriding / Human driver priority

Human Machine Interface (HMI):

Driver Information (Operation Status, Failure)

Optical Warning Signal (type and operation mode)

Acoustic / Haptic Warning Signals (type and operation mode)

Driver Presence and Responsiveness Recognition System

Extract of the relevant part of the owner`s manual

Means to prevent misuse and manipulation

**3. Transition of the Driving Task**

Planned:

Boundary conditions

System behaviour

System performance

Unplanned (incl. mayor system failure):

Boundary conditions

System behaviour

System degradation

System performance

**4. Minimum risk manoeuvre**

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

Emergency (only in case of imminent danger of a collision):

Boundary conditions

System behaviour

System performance

**5. EDR/ Data Storage System**

Type of Data stored

Storage location

Storage duration

Means to ensure data security and data protection

Access to the data

**6. Cyber security (cross reference to the cyber regulation is possible**

Description of the cyber security and software update management scheme

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

Description of the update procedure.

7. Safety by design, verification and validation

Design and validation process:

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

Risk analysis

List of critical scenarios identified for the ODD.

Safety by design principles

-Verification/validation used by the manufacturer (simulation, track test, on road tests).

Test of the functionality in nominal conditions

Tests in case of system failure/critical situations:

Measurement equipment used

-Evaluation of the residual risk

-Process used for field monitoring

8. Information provisions to users

Model of the information provided to users.

Annex X - Appendix 3: Information to be shared across type approval authorities (extract from the information system data)

X. DESCRIPTION OF THE FUNCTIONALITIES OF THE SYSTEM AS AVAILABLE TO THE DRIVER, PASSENGERS AND OTHER ROAD USERS

x.x. Description of the ODD and the high level functional architecture focusing on the functions available to the driver, passengers and other road users. It shall include functional limitations.

x.x. The means to activate, override or deactivate the system.

x.x. Expected driver’s tasks within the OD and when going out of the OD.

x.x. A list of situations in which the vehicle may generate a transition demand to the driver.

x.x. The time required from the driver to take over.

xx. Conditions for override by the driver. Description of the possibilities for the driver to override the system and what kind of control is expected from the system in such stituations

x.x. Information on how the status of the system is shown to the driver and other road users (automated driving mode, failure, override,etc).

x.x. Description of the types of situations that will lead the ALKS to initiate a MRM immediately.

x.x. The system behaviour during a MRM.

x.x. Need to conduct proper maintenance (inspection) and software update of in-use automated vehicles.

x.x. Description on how the current operational status of the system can be checked.

X. TESTS AND VERIFICATION DONE BY THE TYPE APPROVAL AUTHORITY THAT GRANTED THE APPROVAL;

x.x. Scenarios tested during the verification process by the type approval authority and test results.

1. ~~To be signed by different persons even when the Technical Service and Type Approval Authority are the same or alternatively, a separate Type Approval Authority authorization is issued with the report.~~ [↑](#footnote-ref-1)