**Building blocks – Safety Assessment of ADS**

VMAD-SG3-09-06

**SAFETY REPORT BY MANUFACTURER**

****

7. Validation & Verification

**ASSESSMENT REPORT BY AUTHORITY**

|  |  |
| --- | --- |
| **A) A Safety report by manufacturers (based on January 2020 discussion)** | **UN R157 - Annex4, Information Document (rev)** |
|  | **Introduction**1. Definitions and acronyms used for the purpose of this report.
2. The identification of the ADS, including implemented ADS features;
3. A description of the existing authorization status.
4. A statement of any similar (or identical) vehicle that the regulatory body has already reviewed and approved and a statement of the specific differences and improvements that have been made since such an authorization was granted.
5. A description of the structure of the Information Document, the objectives and scope of each of its sections and the intended connections between them.

A comprehensive list of applicable regulations, codes and standards should be provided as Annex. |
| 1. **Description of the system (ODD, function, type)**
 | **Section 1 - System description**General description of the ADS definition of the ODD (§1.1), basic performance of the vehicle (§1.2) and of the means to activate, override or deactivate the ADS (§1.3). |
| The manufacturer shall declare to the type-approval authority the scope of the automated driving mode (so-called operational design domain(s) (ODD): Road conditions, Geographical area, Speed range, Other conditions that must be fulfilled for the safe operation in the automated driving mode or will otherwise trigger a transition demand/minimum risk maneuver. |
| The manufacturer shall declare the main functionality of the system (functional architecture), its dependencies on, and interaction with, other vehicle systems, the driver, the environment and other road users (see section 1 of the Annex 1- See also main sections of the framework document). |
| The manufacturer shall declare the overall system architecture (see generic architecture “sense, plan, act” in the safety first white paper from industry) as well as the safety concept put in place to meet the safety requirements. Follow the principle of RXSWIN vs Software number.It shall provide an identification of safety critical components and software in particular for the following subsystems:-Perception and objects detection including mapping and positioning- Characterization of the decision-making safety - Documented data processing in case of continuous learning implemented.- Human-machine interactions including the driver but also other road users - Supervision and remote monitoring (if applicable). | **Section 2 - Description of the functions of the ADS**Description of ADS software architecture: vehicle-internal (§2.1) and vehicle-external functions (§2.1), as well as the control strategies (§2.3).**Section 3 - Overview major components of the ADS**Description of the hardware relevant to the ADS: control units (§3.1), sensors (§3.2), actuators (§3.3) and other hardware (§3.4).**Section 4 – ADS Layout and Schematics**Description of schemes, layouts and flowcharts of systems (§4) and sub-systems (§4.1), as well as their interfaces (§4.2). |
|  | **Section 5 – Specifications**Description of ADS specifications in Normal (§5.1) and Emergency Conditions (§5.1), the acceptability criteria (§5.3) and the demonstration of compliance with those criteria (§5.4). |
| **Type definition??** |  |
| **2) Hazard and Risk analysis (functional and operational safety, link with cyber risk as well), Safety concept and safety by design by manufacturers**NOTE: Avoid duplication (cross reference to cyber regulation?): Important is the link between cyber analysis and the safety of the function. CSMS in application. | **Section 6 – Safety Concept implementation**Description of the implementation of the safety concept, i.e. the approaches adopted to assure the safety of passengers and other road users, as well as compliance with road rules, starting from the definition of safety objectives. The Section includes the manufacturer statement (§6.1), the description of software architecture (§6.2) and hardware solutions (§6.3) adopted to achieve the safety objectives, system self-diagnostics and main design provisions adopted to obtain safe operation (§6.4 = ex 5.1+ex 6.4 + ex 6.5), transition demand (§6.5), human-machine interface (§6.6), protection against simple unauthorized interventions (§6.7 = ex 5.2), ~~validation and verification by the manufacturer (§6.8)~~, simulation tools and tool-chains description and validation ((§6.7, input from VMAD-SG2). |
| General safety requirements are at this stage set by the framework document and future more detailed requirements development in FRVA (prevent accident, traffic rules, duty of care, failsafe response, HMI, OEDR, cyber/software updates, etc.) .  |
| The manufacturer shall declare the high-level safety rules and the safety concept used for the design and described how this concept is implemented in the vehicle design. |
| The manufacturer shall in particular demonstrate that it has conducted a hazard and 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 address these risk and hazards (safety concept) and that the design leads to an acceptable residual risk for the ODD concerns). |
| Systems shall in particular be designed to address risks that could impact critical functions of the system (for the driver and other road users) due to cyber-attacks and failure (functional safety) but also potential inadequate control, undesirable control actions, reasonably foreseeable misuse by the driver or other road users(to be further defined), tampering and inadequate interaction with other road users (operational safety) during the lifetime of the vehicle. Relevant demonstration methods include ISO 26262 for functional safety and a system-theoretic process analysis (STPA) for operational safety or an equivalent method such as draft ISO PAS 21448. |
| The manufacturer shall describe how the current responses of the ADS to non-critical driving situations, expressing carefulness/duty of care of the ADS. |
| The manufacturer should identify critical scenarios in the ODD and responses to these critical scenarios. This includes traffic challenging scenarios for the ODD with other road users, emergency situation, severe failures). |
| Traffic rules/lifetime: The manufacturer shall describe how the ODD will be managed during the lifetime of the vehicle and how the function will be prevented from being activated in case the conditions required for the ODD cannot be guaranteed anymore by the manufacturer.The manufacturer shall describe how the compliance with traffic rules will be managed through the lifetime of the vehicle. |  |
| **3) Verification and Validation by manufacturer** | **Section 7 - Verification and Validation [ex 6]**Description of verification and validation performed by the manufacturer. |
| Need to include definition of verification/validation |
| The manufacturer shall demonstrate that all design solutions have been verified and validated (through simulation and physical testing including real world testing) by the manufacturer as individual subsystem and as part of the entire vehicle architecture and that the residual risk is acceptable for the driver and other road users.In case the manufacturer rely on sub-contractors for subsystem, for the demonstration, the manufacturer may use documentation on the verification, validation carried out by its suppliers but remains responsible of the overall safety of the ADS (from the type approval point of view).  |
| The manufacturer shall declare the scenarios taken into account for the ADS design, and declare the scenario management method used to select scenarios and choose a validation tool.NOTE: After market retrofitting  |
| The manufacturer shall demonstrate how the performance of the following subsystems have been validated- Perception and objects detection including mapping and positioning- Characterization of the decision-making safety - Documented data processing in case of continuous learning implemented.- Human-machine interactions including the driver but also other road users - Supervision and remote monitoring (if applicable) |
| The safety demonstration shall combine - a quantitative pre-validation target (e.g., using validation acceptance criteria), documented by the manufacturer, demonstrating that the introduction of the ADS will not increase the overall level of risk for the driver and other road users.- a scenario-based approach, taking into account that the most relevant critical scenario have been addressed and that the residual risk is acceptable for the driver and other road users.Acceptable risk level for AD function are not defined for now. OEM shall explain why the risk is acceptable. | *Relevant to Section 6* |
|  | **Section 8 - Data Storage System**Description of DSSAD in terms of type of data stored (§8.1), storage location and crash survivability (§8.2), data recorded during vehicle operation and occurrences (§8.3), data security and protection against unauthorized access or use (§8.4), means and tools to carry out authorized access to data (§8.5). |
|  | **Section 9 -**  **Cybersecurity aspects**Summary of compliance with Cybersecurity & OTA Regulations, namely: cyber security and software update management (§9.1), identification of risks, mitigation measures, secondary risks and assessment of residual risk (§9.2), software update procedure and management put in place to comply with legislative requirements (§9.3). |
|  | **Section 10 -**  **Information provided to the users** Description of information provided to the users to properly inform them about the ADS characteristics and their responsibilities; it includes models of the information provided (§10.1), as well as excerpts from owner’s manual (§10.2). |
|  | **Annex I -**  List of applicable regulations, codes and standards |
|  |
| **B) Evaluation by authorities** | **Assessment report by Authorities** |
| **1) Evaluation of the design and its verification/validation by the manufacturer** |  |
| Before assessing the manufacturer’s safety concept” the type-approval authority or the technical services acting on its behalf (hereafter referred to as type approval Authority) shall check that a valid safety management scheme is implemented within the manufacturer (See paper on the audit of the safety management scheme). | Assessment of verification and validation performed by the manufacturer, including both the vehicle safety functions (§7.1) and the vehicle behavior when facing failures, operational disturbance, boundary and emergency conditions (§7.2). |
| The type-approval authority shall make a finding of at least safety equivalence compared to at least to manual driving including driver assistant systems within the ODD (i.e. quantitative and qualitative target above)) based on the manufacturer’s safety evaluation report documenting scenarios taken into account, testing, validation methods listed above). |  |
| They shall verify that the hazard and risk analysis (i.e. hazards, occurrence and criticality) covers the scenarios of the system that are relevant to the ODD concerned.(link with subgroup 1). |  |
| They shall assess that the logical chart of responses to risk (e.g. redundancy, manoeuvers) covers the range of identified scenarios. They shall check that the safety concept is implemented consistently in the design of the different functions of the AD system |  |
| They shall check that the verification/validation process is robust enough (simulation, track test, in use data) and manufacturer has mitigated risks as reasonably possible and meet the minimum performance requirements. . The validation shall in particular show that the human – machine interactions (including misuses by the driver and other road users) have been properly assessed, based on a relevant set of tests and users. |  |
| They shall ensure that there is a transparent method of measuring the operational/run-time performance of the system. |  |
| The assessments is to be concluded in several steps: audit of the processes in place in the manufacturer organization, assessment once the safety concept is established and assessment of the validation of the manufacturer, monitoring of the manufacturer once the product is on the market. |  |
|  |  |
| **2) Evaluation tests by authorities** | *Relevant to the Testing Pillar* |
| The authorities might carry out a minimum number of track tests to verify that the vehicle operates safely from the functional and operational safety point of view.Check that the safety concept is implemented by the manufacturer. Confirm that the safety concept is valid to the vehicle type variant version to be covered by the assessment |  |
| Check the basic functionality as well as critical failure and driving scenarios through (track) testing. However, simulation can be used in case some critical scenarios/failure may prove to be difficult to be tested on track. |  |
| The authorities might carry out test drives in real-world traffic to verify the carefulness and understandability of operation by other road users in non-critical scenarios and the respect of basic traffic rules. |  |
| The minimum number of tests should include false negative and false positive test scenarios.NOTE: Goal : Inject perception problem.Question: What does this technically mean? A perfect system would not have FNs and FPs…How to test false positive and especially false negative on the road?? Even for a track test, how can one induce a system to fail by influencing its objects detection capabilities? The assessment of false or true is due to the system reaction.  |  |
| The authority carrying out the tests shall have access to the system that is necessary to carry out the test under this section.OICA comments: What is meant by “shall have access to the system”?For type-approval, manufacturers will make all the relevant documents and test results open for inspection (accessible). However, it must be clear that neither a source code review nor a direct copy of the verification toolchain (databases, simulation toolchains, sensor models, reprocessing data) will be practicable due to Intellectual Property, time constraint and intrinsic complexity. |  |
|  |  |
| **3) Simulation evaluation by authorities (see Regulation 858/2018)** | *Relevant to Section 6 of the Information Document/Safety Report* |
| Simulation method may be used by manufacturers to demonstrate safety, subject to their validation by the approval authorities/technical services in accordance with the procedure for virtual testing in revision 3 of the 1958 Agreement. See Annex 2OICA comments:The purpose for simulation as described in the EU Regulation 2018/858 and Directive 2007/46/EC is different from what is needed for AVs verification. While the general simulation tool validation concept can be transferred, it needs some additional adaptation.  |  |
| Manufacturer shall demonstrate the validation of the simulation tool and its scope (e.g. vehicle model, sensor model, recognition model or environmental model) |  |
| Authorities shall verify the validation done by the manufacturer to demonstrate the correlation of the expected results with track tests/on road tests (tool give representative results), scope, traceability, etc. as well as the validity of the simulation tool for the system concerned(applicability to the ODD concerned). |  |
| 3 different axis have to be analysed : (1)definition of dedicated tests for CAE methodology validation (validity area), (2)evaluation of the CAE process with correlation criteria, application of the validated CAE methodology for approval virtual testing.OICA question: What means CAE?Unclear, what is technically required by this paragraph1. Set of tests to “optimize” and “validate” the simulation tool and understand its boundaries;
2. Correlation between simulation tool and physical tests

The activities are complementary, why is there a need to differentiate them in 2 different stages? |  |
|  |  |
| **4) Assessment to be conducted by a qualified independent 3rd party: criteria to be applied.** |  |
| The authority shall have the necessary competences, certifications and training to carry out the vehicle safety assessment and tests listed above.Reference to ISO standards? |  |
|  |  |
| **5) Outcome of the evaluation by authorities/ Failed evaluation/Follow up:** |  |
| Clear Failed evaluation: the hazard/risk analysis does not cover the hazard risks of the use case, the safety concept does not address the hazard/risk analysis identified, the verification/validation does not guarantee an acceptable level of risk or the scenarios taken into account are not transparent ,test failed. | *Looking at experience in other fields, the dialogue with the authority starts at very early stages of the design & development process, so that minor/major non-conformities are identified and easily corrected. As a result, there are no cases of final failed evaluation.* |
| More elaborated common rating scheme needed? (e.g. observations, recommendations for the different level of criticality). |  |
| What about follow up in case of failed evaluation? |  |
| What about monitoring after a successful evaluation? On road monitoring. | *Covered by the pillar on in-service monitoring* |
|  |  |
| **6) Transparency/information sharing amongst authorities on the assessment carried out.** |  |
| As the future new assessment, method will rely more on the assessment by authorities than standardized technical requirements, to continue to ensure mutual recognition more transparency will be needed on what was done by the authorities while at the same time guaranteeing the protection of intellectual property for vehicle manufacturers. Where do we put the limit between the two objectives? Minimum set of information required to understand the system (functionality, operation) can be shared.Description of the function (ODD) focusing on the functions available to the driver and other road users + test report done by the TAA |  |
| Systematic transmission or on request? |  |
| Shall some information be available to some stakeholders beyond authorities (e.g. consumer, registration authorities, insurers, police)?OICA comments:**Consumer:** Educated and trained as requested by the provisions of the UNECE Framework Document on AVs. **Registration authorities**: Detailed Type Approval information out of their scope. They need to be aware of the vehicle being “capable of automation” and “system being enabled in the vehicle”. **Insurers:** No rational behind sharing technical information with insurers.**Police:** DSSAD / EDR provisions will be applied. |  |
|  |
| **References :** |  |
| UN Framework document on automated vehiclesFRVA functional requirementsVMAD subgroup work on scenarios.ISO 26262/SOTIF 21448UL 4600EU guidelines: https://ec.europa.eu/growth/content/guidelines-exemption-procedure-eu-approval-automated-vehicles\_en Annex 6 o UN Regulation 79.EU Regulation 858/2018 UN R157Others??OICA comments: UL4600 is not a reference in this document; it is not a standard rather a compendium. Should be deleted here.  |  |

\*From OICA CLEPA Presentation GRVA-09-10e

