**Audit of the manufacturer safety management system for Automated Driving Systems (ADS)**

**General (from NATM master document)**

The purpose of the audit of the safety management system of the manufacturer is to demonstrate that the manufacturer has robust processes to manage safety risks and to ensure safety throughout the ADS lifecycle (development phase, production, but also operation on the road and decommissioning). It shall include taking the right measures to monitor the vehicle in the field and to take the right action when necessary.

**Safety management system**

1. The documentation provided by manufacturer shall demonstrate that a safety management system provides that effective processes, methodologies and tools are in place, up to date and being followed within the organization to manage the safety and continued compliance throughout the product lifecycle (design, development, production, operation including respect of traffic rules, and decommissioning).

*Guidelines:*

*Note: Safety risk management is a core activity that supports the safety management system and also contributes for the effectiveness of other organizational processes. The term safety risk management, as opposed to the more generic term risk management, is meant to restricts itself to the management of safety risks.(e.g. without considering financial risk, legal risk, economic risk and so forth)*

*The control of risk can be achieved addressing 3 critical dimensions:*

*1) Human component thanks to people with appropriate skills, training and motivation,
2) Organisational component consisting of procedures and methods defining the relationship of tasks and
 3) Technical component by using appropriate tools and equipment.*

*The establishment of an adequate SMS serves to monitor and improve all three dimensions and control the relevant risks. The Safety Management System (SMS) evaluation is based on automotive engineering standards, guidebooks and best practice documents relevant to safety.*

*Examples of processes and aspects to be documented:*

*A. Safety governance*

*a. Safety policies and principles (in line with the concept stated in ISO 21434 5.4.1 and ISO 9001 Automotive 5.2, but from safety perspective)*

*b. Management commitment (in line with the concept stated in ISO 21434 5.4.1 and ISO 9001 Automotive 5.1, but from safety perspective)*

*c. Roles and responsibilities (ISO 26262-2 6.4.2, this relates to the organizational as well as to the project dependent activities )*

*B. Safety culture (ISO 26262-2 5.4.2)*

*C. (periodic) internal and external audit to ensure that all SMS processes are implemented consistently (R157 3.5.5, ISO 26262-2 6.4.11)*

*D. Effective communications within the organization ( ISO 26262-2 5.4.2.3)*

*E. Information sharing outside of the organization (in line with the concept stated in ISO 21434 5.4.5 and ISO 9001 Automotive 5.1, but from safety perspective)*

*F. Quality management system (like IATF 16949) to support safety engineering, including change management, configuration management, requirement management, tool management etc.*

*G. Tool management*

2. The design and development process shall be established including safety management system, risk management, requirements management, requirements’ implementation, testing, failure tracking, remedy and release

*Guidelines:*

*The product operational risks are specifically dealt in the Design and Development chapter and implemented in the product assessment. Thus, this section must shall show the link between the overall risk management process (as per this chapter) and product operational risks.*

*Examples of processes and aspects to be documented:*

*A. Risk identification (in line with ISO 3100 6.4.2 or equivalent standard)
B. Risk analysis (in line with ISO 3100 6.4.3 or equivalent standard)
C. Risk evaluation (in line with ISO 3100 6.4.4 or equivalent standard)
D. Risk treatment (in line with ISO 3100 6.4.5 or equivalent standard), including
E. Processes used for keeping the risk assessments as current as possible
F. Safety performance of the organization and effectiveness of safety risk controls.*

*Examples of processes and aspects to be documented to ensure the robustness of the design and development phase:*

*A. A general description of the way in which the organisation performs all the design and development activities*

*B. Vehicle\system development, integration and implementation.*

*a. Requirements management (e.g. Requirement capture and validation)*

*b. Validation strategies, including but not limited to*

*i. Credibility assessment for simulation (link to Sub Group 2)*

*ii. System Integration level*

*iii. Software level*

*iv. Hardware level*

*c. Management of functional Safety and SOTIF, including the continuing evaluation and update of risk assessments and relationship with In-Service Safety*

*C. Management of design changes and design assurance system changes*

1. The manufacturer shall institute and maintain effective communication channels between manufacturer departments responsible for functional/operational safety, cybersecurity and any other relevant disciplines related to the achievement of vehicle safety.

*Guidelines:*

*Examples of processes and aspects to be documented to assure that responsibilities are properly discharged:*

*A. Roles and responsibilities during the design and development*

*B. Qualifications and experience of persons responsible for making decisions affecting safety*

*C. Coordination between design and production*

*Examples of processes and aspects to be documented to ensure the robustness of the production phase:*

*A. Quality Management System accreditation (e.g. as per IATF 16949 or ISO 9001 or equivalent)*

*B. A general description of the way in which the organisation performs all the production functions including management of working conditions and the environment and equipment and tools.*

*Examples of processes and aspects to be documented to assure robustness of distributed production:*

*A. Liaison between the vehicle manufacturer and all other organisations (partners or subcontractors) involved in the production of the system/vehicle*

*B. Criteria for the for the acceptability of “subsystem/components” manufactured by other partners or subcontractors. (i.e. deployment of production assurance requirements to supply chain)*

4 The manufacturer shall have processes to monitor safety-relevant incidents/ crashes/collisions caused by the engaged automated lane keeping system and a process to manage potential safety-relevant gaps post-registration (closed loop of field monitoring) and to update the vehicles. They shall have processes to report critical incidents (e.g. collision with another road users and potential safety-relevant gaps) to the certification authorities when critical incidents occur.

*Guidelines: Link with the in service monitoring/reporting pillar.The manufacturers should set up process for the operational phase for confirmation of compliance to the safety requirements in the field, early detection of new unknown scenarios (in line with SOTIF safety development goal to minimize the unknown scenarios area), event Investigation, to share learnings derived from incidents and near-miss analysis to allow the whole community to learn from operational feedback and to contribute to the continuous improvement of Automotive Safety*

*Example of guiding principles: Is there a document describing the appropriate procedure of reporting incidents to the management? Is there evidence that the company is complying with that procedure? Is there a document describing the appropriate procedure of investigation and documentation of incidents? Is there evidence that the company is complying with that procedure?*

1. The manufacturer shall demonstrate that periodic independent internal process audits are carried out to ensure that the processes established according with paragraphs 1. to 4. are implemented consistently.

*Guidelines:*

*Examples of processes and aspects to be documented to assure independent design audit and assessment:*

*A. Assurance that all practises and procedure to be applied during the vehicle\system development are followed. (process assurance)*

*B. Assurance an independent checking for the compliance with the applicable requirements and regulations. (Independent assessment from person not creating the compliance data)*

*C. Process to assure the continuing evaluation of the design assurance system in order to ensure that it remains effective. (system audit that can be undertaken by the existing Quality Management System)*

6. Manufacturers shall put in place suitable arrangements (e.g. contractual arrangements, clear interfaces, quality management system) with suppliers to ensure that the supplier safety management system comply with the requirements of paragraphs.1. (except for vehicle related aspects like "operation" and "decommissioning"), 2,.3 and 5

*Guidelines:*

*Examples of processes and aspects to be documented*

*A. Organizational policy for supply chain*

*B. Incorporation of risks originating from supply chain*

*C. Evaluation of supplier SMS capability and corresponding audits*

*D. Processes to establish contracts, agreements for ensuring safety across the phases of development, production and post production*

*E. Processes for distributed safety activities.*

**Expiration/renewal of the SMS**

1 The documentation shall be considered valid for a maximum of three years if there is no change to the SMS. The documentation shall no longer be valid anymore if the requirements on the SMS are no longer met.

2. At the end of the period of validity of the SMS, the validity of the documentation may be extended for a further period of three years if the requirements on the SMS are still met .

3. Changes to the SMS shall be reflected in the documentation as soon as they happen.