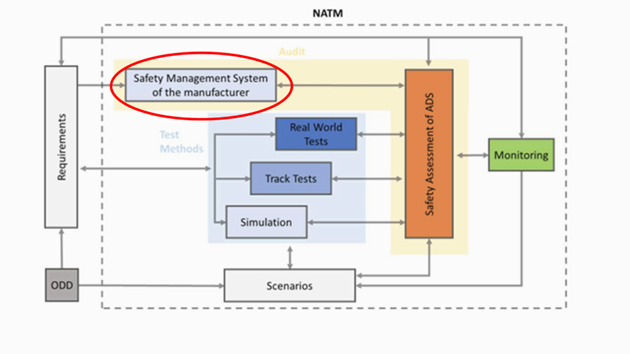
**Building blocks - Audit of the Safety Management System**

VMAD-SG3-09-05-Rev1



**SMS**

SMS

Requirements

Design of the SMS

Implementation of the SMS

Identification of risks

Continuous management of risks

Other actors (e.g. suppliers, infra)

ADS

AUDIT of the SMS

**INTERFACE**

**ORANGE:** APPLICANT LEVEL

**BLU:** OTHER ACTORS (Authority, Suppliers, Infrastructure Manager, ….)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirements (based on January 2020 discussion)** | | | **UN R 157 - Annex4** | |
| **1** | A safety management system shall be established, documented and implemented by the manufacturer and shall demonstrate a clear safety culture through adequate processes within the manufacturer | | *3.5. Safety management system (Process Audit)*  *3.5.1 In respect of software and hardware employed in "the ADS", 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).* | |
| **2** | It shall include a clear process for: Safety by design (high level safety rules), hazard and risk analysis, verification and validation through simulation, test track and on road tests.  Manufacturers shall document and demonstrate how they ensure a safety culture and the capability to manage safety during the lifecycle of the vehicle  (development phase, production, postproduction phase, operation,  respecting/updating traffic rules, , decommissioning).  The organization shall institute and maintain effective communication channels  between functional/operational safety , cybersecurity and any other disciplines  related to the achievement of vehicle safety. | | *3.5.2. The design and development process shall be established including 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 manufacturer departments responsible for functional/operational safety, cybersecurity and any other relevant disciplines related to the achievement of vehicle safety.* | |
| **3** | They shall have processes to monitor incident/accidents with their vehicles  overtime and react appropriately (closed loop of field monitoring). | | *3.5.4. 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.* | |
| **4** | Manufacturer processes shall include continuous independent internal audit to  ensure that the process is implemented consistently throughout the different  phases of vehicle lifetime (development phase, postproduction phase,  respecting/updating traffic rules, etc). | | *3.5.5 The manufacturer shall demonstrate that periodic independent internal process audits are carried out to ensure that the processes established according with paragraphs 3.5.1 to 3.5.4 are implemented consistently.* | |
| **5** | Manufacturers shall put in place suitable arrangements (e.g. contractual  arrangements, clear interfaces, quality management system) with suppliers to  ensure that to ensure that the manufacturer safety management scheme is  implemented by suppliers | | *3.5.6 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 3.5.1. (except for vehicle related aspects like "operation" and "decommissioning"), 3.5.2, 3.5.3 and 3.5.5.* | |
| **6** | Pass/fail criteria for SMS  Failed/pass audit (Reference to Annexes B and C of ISO 26262-2 for criteria??) :  2 levels: Major/minor non-conformity  Major: process not documented, no demonstration that there is an appropriate  level of management, process not implemented in a consistent manner  Minor: the demonstration exists but is not convincing enough  Both Major/minor issues have to be close before any vehicle is placed on the  market.  No grading in Annex 6 in CEL at this stage.  Both parts are covered by Annex 6. | | No criteria in R157 | |
| **7** | Timing and renewal of the audit of the SMS  Initial assessment and monitoring by authorities.  Frequency of internal and external audits.  Action in case of changes to the SMS.  Impact on the assessment of a given ADS?  Supervision by authority  Validity of the SMS limited in time (See R155 on cybersecurity).  Renewal by annual review and report (documentations, interviews, technical inspections, monitoring, findings)? | No criteria in R157. | | |
|  | | | | |
| **Additional requirements** | | | **UN R 157 - Annex4: Outstanding issues NATM after September 2021** | |
| **8** | Auditors  Competences/skills and criteria for the independent auditor  multiple eyes principle  objective & independent | The assessments under this Annex shall only be conducted by auditors/assessors with the technical and administrative knowledge necessary for such purposes. They shall in particular be competent as auditor/assessor for ISO 26262-2018 (Functional Safety - Road Vehicles), and ISO/PAS 21448 (Safety of the Intended Functionality of road vehicles); and shall be able to make the necessary link with cybersecurity aspects in accordance with ISO/SAE 21434. This competence should be demonstrated by appropriate qualifications or other equivalent training records. | | |
| **9** | Which responsibility of the different actors (within the supply chain)? |  | | |
| **10** | Which differences between type approval and self certification systems? | . | | |
| **11** | Requirements/Guidelines on SMS  Guidelines to manufacturers on how to establish run and maintain a SMS.  Requirements on SMS and documentation to be provided to the authority.  Available in other sectors, e.g. aviation, railway (see references) | | What documentation shall be made available to authorities.  Possible guiding principles:  a) 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?  b) 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?  c) Is there a document describing the appropriate procedure of using information related to the investigation and causes of incidents in order to implement preventive actions? Is there evidence that the company is complying with that procedure? | |
|  | | | | |
| **References** | | | |  |
| Cyber security UN regulation  ISO 26262/SOTIF 21448  UL 4600  Conformity of Production provisions in Regulation 858/2018  Annex 6 of Regulation 79  ISO9001  ISO 39001  Aviation SMS building blocks (SG3 repository)  SMS manual from ICAO (SG3 repository)  SMS Auditing/Assessment Tool from EASA (SG3 repository)  ERA Guide on SMS requirements (SG3 repository)  ERA Common safety Methods on SMS requirements (SG3 repository)  ERA SMS App (<https://t.co/TKKQ548Fl7>)  https://mtu.gov.ua/files/GUIDE\_en\_2016.pdf  Other? | | | |  |

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

