Table of Contents

5.4 Safety Case

5.4.1 General Description

The manufacturer shall provide a safety case that includes:

1. the safety concept, which describes the hazard identification and mitigation measures designed into the ADS to meet the requirements of this regulation and achieve the goal of avoidance of unreasonable risk with regard to functional and operational safety;
2. information and documentation necessary to describe the ADS covered by the safety case, including the intended use, the operating environment, the interactions with humans, sub-systems and components, control strategies;
3. structured claims, argumentation, and evidence (including validation tests) that affirms and demonstrates that the ADS meets the requirements in [Requirements section] and is free from unreasonable risks for the ADS vehicle user(s) and other road users;
4. demonstration of credibility and suitability of test tools used in generating evidence; and
5. explanation of the processes for reinforcing ADS safety throughout the life of the ADS.

5.4.2 Safety Concept and Other Required Documentation

5.4.2.1 System-Level

The requirements in this section shall apply to the ADS system as a whole.

5.4.2.1.1 Systems, sub-systems & components

Listing of System components & interactions

The manufacturer shall provide documentation listing the components in the ADS and their link to the function of each ADS feature which shall include:

(a) Description of components

A description shall be provided, including all the components of the ADS and the other vehicle systems which are needed to meet the requirements of this regulation. An outline schematic showing these components and systems and their relationships shall be provided, with both the equipment distribution and the interconnections made clear. The outline shall include how the following elements are addressed:

(i) Perception and objects detection including mapping and positioning
(ii) Characterization of decision - making
(iii) Remote supervision and remote monitoring by a remote supervision centre (if applicable).
(iv) Information display/user interface
(v) The data storage system (e.g., DSSAD).
(vi) Redundancies of components and/or connections

(b) Functions of the components

The function of each component of the ADS shall be outlined and the signals linking it with other components 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. Interconnections within the ADS 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. There shall be a clear correspondence between transmission links and the signals carried between components and systems. Priorities of signals on multiplexed data paths shall be stated wherever priority may be an issue affecting performance or safety.

(c) Identification of components

Each component shall be clearly and unambiguously identifiable (e.g. by marking for hardware, and by marking or software identification for software content). This will provide a clear method for identifying the hardware and software in the associated documentation. Where the software version can be changed without requiring replacement of the marking or component, the software identification must be updated by means of the newly released software. Where functions are combined within a single control unit or within a single computer, but shown in multiple blocks in the diagram, then for clarity and ease of explanation, only a single hardware identification marking shall be used. The identification defines the hardware and software version and, where the software changes and alters the function of the unit, the identifier associated with that software shall also be changed.

(d) Installation of sensing system components

The manufacturer shall provide information regarding the installation options that will be employed for the individual components that comprise the sensing system. These options shall include, but are not limited to, the location of the component in/on the vehicle, the material(s) surrounding the component, the dimensioning and geometry of the material surrounding the component, and the surface finish of the materials surrounding the component, once installed in the vehicle. The information shall also include installation specifications that are critical to the ADS's performance, e.g., tolerances on installation angle. Any changes to the individual components of the sensing system, or the installation options, shall be updated in the documentation.

Inputs & outputs, ranges & limits

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 is linked to the control functions of the ADS and potential impacts on system behaviour. This shall include the nominal range, and coverage area of each sensor.

A list of all of the ADS output variables shall be provided and an explanation given, in each case, of whether the output directly controls the vehicle or is processed via another vehicle system. The range of control exercised on each variable shall be defined as well as the nominal capabilities of control actuators.

5.4.2.1.2 Identification of hazards - risk & severity

Using process in SMS

The manufacturer shall demonstrate how their SMS processes with regards to functional and operational safety with regards to risk identification, risk analysis, risk evaluation, risk treatment (including acceptance) and keeping the risk assessments up to date have been applied to the ADS according to [SMS section 5.6 Risk Management and SMS section 5.7 Design and Development Process].

The manufacturer shall demonstrate how it has taken both a top down (from possible hazard to design) and bottom-up approach (from design to possible hazards) in its identification of hazards. This shall 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 system functional and operational safety;

Commented [RJM(1]: This may be better placed within the SMS section - further discussion

In-operation hazard identification & avoidance

The manufacturer shall describe how the ADS features detect, identify, and respond to hazards including:

- Detection and identification of hazards
- Design provisions for functional and operational safety (e.g. redundancies)
- An analysis which shows how the ADS will behave (e.g. control strategies) to mitigate or avoid hazards which can have a bearing on the safety of the ADS vehicle user(s) and other road users.
- An analysis, which shows how unknown hazardous scenarios will be managed.

Cybersecurity

[Open Item as this may need to point to UN R155 which is not part of the 1998 agreement. We will have to wait until some discussions move forward before deciding content here – placeholder text below]

The manufacturer shall describe measures taken to assure the cybersecurity of the ADS and the analysis performed to identify and disposition likely security threats. Where UN R 155 applies, the manufacturer shall describe how the ADS meets the requirements of that regulation.

Physical Security

The manufacturer shall document measures it has implemented to prevent or deter abuse or misuse of the ADS or its occupants which may normally be performed by a driver. (e.g. unauthorised persons attempting to access a vehicle with occupants, occupant attempting to access driving controls, objects placed on vehicles during operation, attempts to damage a vehicle).

5.4.2.1.3 System Monitoring and update management

Process for monitoring performance, updating claims, arguments and evidence (as per sms)

[open item – some reference in SMS [5.9.2] to check and include -- Discussion on how to tackle software updates required – Some provisions exist in UNR provisions of ADS workshop but may not be in line with 1998 agreement]

Process for validating and distributing new software releases

[Open Item as this may need to point to UN R156 which is not part of the 1998 agreement. We will have to wait until some discussions move forward before deciding content here] The manufacturer shall demonstrate that software updates are validated and confirmed in accordance with SMS section [5.9.4].

Data Storage System

The manufacturer shall describe the following aspects of the data storage system:

1. Storage location and crash survivability ;
2. Data recorded during vehicle operation and occurrences;
3. Data security and protection against unauthorized access or use;
4. Means and tools to carry out authorized access to data

5.4.2.2 Feature-Level

The requirements in this section shall apply to each feature of the ADS

5.4.2.2.1 Summary of intended use

The safety case provided by the ADS manufacturer shall include a description of each ADS feature configuration including ADS functions applicable to that specific feature, the intended uses and limitations on the use of the feature which gives a simple explanation of its operational characteristics.

5.4.2.2.2 Operational Design Domain (ODD), Expected Operating Conditions, and Use Case

Operational design domain

The manufacturer shall document how it has defined the Operational Design Domain for the ADS feature and the boundaries within which it is designed to operate. The manufacturer shall document how the ADS determines the presence/absence of the conditions and any linked/dependent conditions (e.g. reduced speed in icy weather). This shall include at least the following characteristics:

- Road speed limits
- Road type and roadway characteristics
- Intended area of operation (e.g. Jurisdictions)
- Any geographic limitations
- Environment (e.g. Weather conditions, surroundings)

Commented [JR2]: Draft provisions from UNR Workshop:
7. Modifications and extension of approval of the vehicle type
Every modification of the vehicle type with regard to this Regulation shall be notified to the Type Approval Authority which approved that vehicle type. The Type Approval Authority may then either:
(a) Decide, in consultation with the manufacturer, that a new type approval is to be granted; or
(b) Apply the procedure contained in paragraph 7.1.1. (Revision) and, if applicable, the procedure contained in paragraph 7.1.2. (Extension).
7.1.1. Revision
When particulars recorded in the information documents of Annex 1 - Appendix 1 have changed and the Type Approval Authority considers that the modifications made are unlikely to have appreciable adverse effect, and that in any case the vehicle still meets the requirements, the modification shall be designated a "revision".
In such a case, the Type Approval Authority shall issue the revised pages of the information documents of Annex 1 - Appendix 1 as necessary, marking each revised page to show clearly the nature of the modification and the date of re-issue. A consolidated, updated version of the information documents of Annex 1 - Appendix 1, accompanied by a detailed description of the modification, shall be deemed to meet this requirement.
7.1.2. Extension
The modification shall be designated an "extension" if, in addition to the change of the particulars recorded in the information folder:
(a) Further inspections or tests are required; or
(b) Any information on the communication document (with the exception of its attachments) has changed; or
(c) Approval to a later series of amendments is requested after its entry into force.

Commented [RJM(3]: Open Item - Monitoring and update of Safety Case based on deployed performance

Commented [RJM(4R3]: From SMS -> 5.9.2. The processes for ISMR shall demonstrate the capabilities:
(a)To monitor ADS operations;
(b)To confirm the compliance with the defined safety case and compliance to the performance requirements;
(c) To identify safety risks related to ADS performance that need to be addressed in the frame of the SMS activities, including instances of non-compliance with ADS safety requirements
(d)To manage potential safety-relevant gaps during the in-service operation and to provide the information that allows the ADS to be updated according to the appropriate manufacturer processes;
(e)To support the development of new or revise existing scenarios
(f)To perform event investigation
(g)To report occurrences to the relevant authority when they occur;
...

Commented [RJM(5]: Exact term in discussion in SAE/ISO groups

- Road conditions

Expected Operating Conditions

The manufacturer shall describe the conditions that the driving automation system is reasonably likely to encounter on its trip(s), including, but not limited to, environmental and geographical conditions, and/or the presence or absence of certain traffic or roadway characteristics, and explain how those expected conditions compare to the ODD of the ADS.

Use case

The manufacturer will explain the type of use(s) for which the ADS is intended, such as personal car ownership, urban taxi fleet, goods transportation, highway use, etc.

Conditions for activating & deactivating (incl fallback)

The manufacturer shall document:

- the conditions that must be present to permit activation of the feature
- the conditions that trigger a fallback response
- the conditions that must be present to permit deactivation of the feature
- the conditions which may prompt the user to voluntarily take back control, if applicable

5.4.2.2.3 ADS Interactions

Identification of users and possible interactions

The manufacturer shall identify the other road users with whom it is designed to interact.

The manufacturer shall identify the ADS users, including remote users with whom it is designed to interact.

Methods of activating and deactivating

The manufacturer shall describe the methods of activating, overriding, or deactivating the ADS feature by any or all of: the ADS user (where relevant), the remote assistant or operator (where relevant), passengers (where relevant) or other road users (where relevant).

5.4.2.2.4 ADS Functions & Control Strategies

Minimal Risk Condition (definition, possibilities/scenarios)

The manufacturer shall describe the range of end states constituting a minimal risk condition that can be achieved by the ADS feature. This shall include:

- The conditions which may trigger an attempt to reach a minimal risk condition
- The processes by which the ADS feature attempts to reach a minimal risk condition
- The evaluation of risk related to minimal risk condition end states

Operation near ODD boundaries, foreseeable ODD exit, sudden ODD exit

The manufacturer shall describe how the ADS detects and responds to approaching and crossing of ODD boundaries. This shall include strategies to limit sudden ODD exits and frequent activation/deactivation situations.

The manufacturer shall describe the process by which the ADS determines if the situation it is faced with is critical or nominal for the purposes of meeting the requirements of [DDT section].

Commented [RJM(6]: Exact term in discussion in SAE/ISO groups

Commented [RJM(7]: Additional discussion required - Intent is to avoid labelling everything as critical situation (and thus reducing requirements of DDT section) however, ADS are unlikely to "label" situations as nominal vs critical. Current text is not accepted but left as placeholder for discussion.

Fault identification, diagnostic, fallback/minimal risk condition in failure conditions, reduced performance modes

The manufacturer shall describe how the ADS feature responds to failure situations including:

a) Fallback (or fail safe) operation using a partial system;
b) Redundancy using separate systems;
c) A list of the potential faults identifiable by the diagnostic system(s) of the ADS feature;
d) Removal of some or all automated driving function(s).
e) Failure of a vehicle system or component other than the ADS that precludes the ADS from performing the DDT.

If a chosen provision utilizes a partial performance mode of operation under certain fault conditions (e.g. in case of severe failures), then these conditions shall be stated (e.g. type of failure). The resulting ADS feature behaviour and capabilities shall be defined (e.g. achievement of a minimal risk condition immediately) as well as the warning strategy to the driver/remote supervision centre (if applicable).

Commented [RJM(8]: Modify accordingly to what is defined

If the chosen provision selects a second (backup) means to realize the performance of the dynamic driving task, the principles of the change-over mechanism, the logic and level of redundancy and any built-in backup checking features shall be explained, and the resulting limits of backup effectiveness defined.

If the chosen provision selects the removal of an ADS function, it shall be done in compliance with the relevant provisions of this regulation. In this case, all the corresponding output control signals associated with this function shall also be inhibited.

5.4.3 Verification, Validation and Acceptance Criteria

Commented [JR9]: Text from credibility may better fit here - to be discussed:
4.6. The manufacturer shall demonstrate that the approach to testing is suitable for the demonstration of the safety case and the compliance with performance/functional requirements
4.6.1. The manufacturer shall demonstrate that the physical testing (proving ground and/or public road) facilities and environment are suitable for the tests that are being conducted.
4.6.2. The manufacturer shall demonstrate that the simulation toolchain(s) is suitable for conducting virtual tests. The requirements for the simulation toolchain(s) are listed in 5.8.1.

The manufacturer shall provide the following information as part of its safety case:

a) Validation/verification plans including appropriate acceptance criteria
b) Analysis of coverage of the different tests and setting minimal ODD coverage thresholds for various metrics and includes ODD boundaries. [reference to DDT Annex]
c) Validation/verification results including evidence that the Validation targets (i.e., validation acceptance criteria) are met
d) Evidence that the scenarios tested provide reasonable coverage of the ODD
e) How it assess that the validation methods are robust
f) Scenario selection process is reasonably designed to provide reasonable coverage of the ODD and its boundaries
g) Any comparisons drawn between the performance of an ADS feature and that of a manually driven vehicle reflect comparable vehicle categories (e.g. category M1 or category 1-1) and situations

Commented [RJM(10]: Open item for future iterations - better description/definition of requirements for selection process

The manufacturer shall state how it has determined that the acceptance criteria it has used in its safety case is deemed to be sufficient. Such a statement shall include:

- Identification of metrics used in evaluating the Safety Case
- Justification of the chosen acceptance criteria for those metrics
- The scoring/evaluation of the evidence in generating metrics

Commented [RJM(11]: From Assessment of Safety Case

5.4.4 Presentation of Safety Case

5.4.4.1 General requirements

The safety case shall be composed of a series of claims for each of which there must be at least one supporting argument. Each argument shall be supported by at least one piece of evidence.

Each claim, argument and evidence shall be uniquely labelled but may be used more than once (i.e. a piece of evidence may support more than one argument).

The safety case shall include claims, arguments and evidence that are understandable, logical, correct and robust and that demonstrate that (1) the ADS is free of unreasonable risk to ADS user(s) and other road users and (2) the ADS meets applicable requirements of this regulation in each of following areas:

- DDT requirements
- User requirements
- Monitoring requirements
- [Cybersecurity]
- [DSSAD]

The following summary information shall be provided by the manufacturer:

- A summary identifying the relationships between claims and their supporting argument and evidence
- A summary identifying each regulatory requirement noted above and the claims that demonstrate the requirement is met

Lifecycle validity

The manufacturer shall demonstrate through the safety case that the application of the SMS is suitable for managing ADS safety throughout the lifecycle of the system in accordance with [SMS section]

The manufacturer shall demonstrate through the safety case its ability to monitor the ADS over its lifetime in accordance with [ISMR section]

Statement of Assumptions

The manufacturer shall state relevant assumptions it has made in relation to claims, arguments and evidence.

Test tools used for producing evidence have been validated

The manufacturer shall demonstrate that the credibility of the simulation toolchain in accordance with" X" [Credibility section] and that the credibility of physical testing used for the generation of evidence with regards to safety have been assessed.

5.4.4.2 Claims

Provide claim that a specific goal/requirement is met

There shall be at least one claim for each goal or regulatory requirement.

Use of sub-claims permitted

The manufacturer may create multiple sub-claims for a claim, where a broader claim may not be sufficient or where additional justification is warranted as long as said sub-claims are sequenced logically and their relationships are included in the summary documents.

5.4.4.3 Argumentation

Analysis supporting claim, providing contextual information how/why claim met

Each argument supporting a claim shall provide contextual information and supporting information that explains how a claim is met based on an appropriate set of evidence.

5.4.4.4 Evidence

Testing results, individual or in aggregate -(including ability to produce specific test cases, parameters, tool versions and can be reproduced upon request)

Evidence supporting argumentation shall consist of test results or analysis (e.g. source code, engineering drawings, photographs, required documentation etc.) as appropriate. Testing results may be provided individually or on aggregate and shall include appropriate acceptance criteria.

Each test shall include enough information or be recorded in such a way that it may be reproduced upon request (e.g. same software/hardware versions, same tool versions, same scenario, same parameters etc.).

The manufacturer shall facilitate access and execution of the necessary tools and analysis software upon request by the authority for the purpose of reproducing this evidence as part of the approval process or during compliance verification.

5.4.5 Self-Assessment

The manufacturer shall assess its safety case prior to certification/approval but may do so during the development process. The assessor(s) chosen for self-assessment shall not be a significant contributor of the design team and may be internal or external to the manufacturer. The assessment shall be documented, available for inspection and include:

- Qualifications of the assessor/team
- Date/period of assessment, version of: the safety case, tools and ADS assessed
- Methods used to assess the Safety Case
- Listing of any Evidence repeated/reproduced
- Identified gaps, questions or areas of lower confidence or unknowns

Following each assessment, the manufacturer shall append a document to the assessment indicating the steps it has taken to remediate or improve upon any findings (e.g. release notes).

Commented [RJM(12]: From Assessment of Safety Case