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.

Commented [RE(1]: In the credibility section we have the following general requirements:
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.

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) Inventory of components

A list shall be provided, including all the ~~units~~ components of the ADS and mentioning the other vehicle systems which are needed to achieve the control function in question. An outline schematic showing these units 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 units

The function of each unit of the ADS 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. 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 units. Priorities of signals on multiplexed data paths shall be stated wherever priority may be an issue affecting performance or safety.

(c) Identification of units

Each unit 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 indeed 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.

~~Physical Capabilities of the System~~

~~A description of the physical capabilities of the system shall be provided. This shall include:~~

Commented [FH2]: Should require only a list of general units like radar xyz instead of radar 1, left with part no. 123456 etc.

Commented [RJM(3R2]: Does components help?

(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.

~~The nominal range, placement and coverage area of each sensor~~

T~~he nominal capabilities of control actuators~~

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

A list of all of the ADS output variables ~~which are controlled by the ADS~~ shall be provided and an explanation given, in each case, of whether the output directly control the vehicle or is processed~~is direct or~~ 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 ~~for~~ with regards to risk identification, risk analysis, risk evaluation, risk treatment (including acceptance) and ~~update of~~keeping the risk assessments up to date ~~in their SMS~~ have been applied to the ADS according to [SMS section 5.6 Risk Management and SMS section 5.7 Design and Development Process].

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
- ~~Control strategies and methods employed while performing the dynamic driving task including a statement of the mechanisms by which control is exercised~~
- Design provisions for functional and operational safety (e.g. redundancies)
- An ~~A~~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 ~~A~~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]

Commented [FH4]: Isn't this handled in the credibility assessment, including the quality (changes) of those input variables and possible effects to the output and system robustness / sensitivity?
Should this really be part of the safety case?

Vehicle behavior might be derived on a way more complex way than just being triggered by 1-2 input variables!

Commented [RJM(5R4]: The Credibility section is with regards to credibility of testing. This section is with regards to design/operation. Tried to address 2nd part by modifying text to give more clarity on intent

Commented [RE(6]: The SMS concerns the overall management of the Safety by the Organization.
In this perspective, the risk management in the 5.6 covers all kinds of risk which can affects the safety (e.g. also organizational risks).
In our view, the safety case shall refer to the processes applied during the development phase for the identification/assessment and control of the Fusa and Sotif related hazards.
We suggest to use the following text based on the Integration Document:
The manufacturer shall demonstrate how the processes ***for the management of the functional and Operational Safety [SOTIF] in their SMS*** *have veen applied to the ADS* ***[SMS, 5.7. Design and Development Process]***

Commented [RJM(7R6]: Tried to include this concept however 5.6 does have content on risk management which I think should be kept.

Commented [RE(8]: We suggest to use the information concerning the safety analysis (yellow part) to be performed as included in the Integration document 5.10.4.4.

The auditor should perform an assessment of the application of these analytical approaches, including:
(b) It is recommended that this approach be based on a Hazard/Risk analysis appropriate to system safety;
(c) Inspection of the safety approach at the ADS level including a top down (from possible ...

Commented [RJM(9R8]: Would this be contained within SMS Section 5.6.2. Additional content above (ie top down, bottom up, FMEA, FTA, STPA) are processes which seem to be applicable to SMS in general and may be better placed in that section?

Commented [RE(10]: We suggest to include the text from the Integration document at 5.10.4.5:
5.10.4.5. It is recommended that the documentation confirms that at least each of the following items are covered where applicable:
(a) Issues linked to interactions with other vehicle systems (e.g., braking, steering); ...

Commented [JR11R10]: I believe we had discussed keeping this list as a reference in the interpretation document as it is not exhaustive and covers a number of different topics.

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)

Operating Environment

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)
- Road conditions

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

Commented [RE(12]: 1)We do suggest to rename as: **System Monitoring** and update management.
2)it is a bit unclear what we want to cover in the system update management
- the modification to the design of the ADS are generally covered in the SMS (5.7 Design and Development)
- Regarding the modification of the system after the approval, the draft text of the UNR from the workshop is already covering this aspect:

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 ...

Commented [RJM(13]: Open Item - Monitoring and update of Safety Case based on deployed performance

Commented [RJM(14R13]: 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 allow ...

Commented [RE(15]: Question? Do we expect the manufaturere tio declare a generic ODD (e.g urban environment) or a specific ODD (the cities in which can operate)

Commented [RJM(16R15]: I think it will depend on their design and various considerations.

- 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 minimal risk conditions 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 it detects and responds to 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].

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).

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(17]: 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.

5.4.2.3 Verification and Validation

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

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 [types/categories] and situations

Commented [RE(18]: We also suggest to use part of the text included in the Integration Document to clarify that the validation shall cover use 2 approaches/steps:
(a) Overall validation targets (i.e., validation acceptance criteria) supported by validation results demonstrating that entry into service of the ADS will not increase the overall level of risk to the ADS vehicle user(s) and other road users compared to manually driven vehicles within the ODD; and
(b) A scenario-specific approach showing that the ADS will not increase the overall level of risk to the ADS vehicle user(s) and other road users compared to a manually driven vehicles within the ODD for each of the safety relevant scenarios.

Commented [RJM(19R18]: I think this is captured? The validation acceptance criteria are in a). The absence of unreasonable risk is the overall goal. Appropriate coverage of the ODD.

Commented [RJM(20]: Open item for future iterations - better description/definition of requirements for selection process

5.4.3 Presentation of Safety Case

5.4.3.1 General requirements

Each of the requirements in (DDT, User, ISMR, Absence of unreasonable risk) must have at least 1 Claim, each Claim must have at least 1 argument and each argument at least 1 piece of evidence

- Claims, arguments and evidence are uniquely labelled, can be re-used
- Hierarchy/links identified.
- Summary document identifying claims support which requirements

The safety case shall be composed of a series of claims for 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 the ADS is free of unreasonable risk to ADS user(s) and other road users and in addition that the requirements in each of following items are met:

- 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 requirement required 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

- Claims for validity with supporting arguments and evidence
- Credibility assessment

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.

5.4.3.2 Claims

Provide claim that a specific goal/requirement is met

There shall be at least one claim for each 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.

5.4.3.3 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.

5.4.3.4 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.).

Commented [FH21]: Very extensive requirement. Better to focus on what affects the validity of the test.

Commented [RJM(22R21]: Yes but this may be required for repeatability tests. We must be able to test the exact path taken to achieve compliance.

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.

Commented [FH23]: This should be limited to the period of assessment and not to unlimited period beyond that.

Commented [RJM(24R23]: This may vary between type approval and self-certification. We may do compliance audits after market introduction. - In the assessment of safety case, we have left this up to a discussion between the manufacturer and the authority instead of specifying particular tools. Maybe the addition of some wording could help narrow?

Submitted by the OPI on Safety Assessment provisions

Document ADS-05-06
5th ADS IWG session
9-13 December 2024

General Requirements [New section under ADS Requirements]

The ADS shall be designed to protect against unauthorized access to and modification of the ADS features and functions. The measures ensuring protection from unauthorized access shall be provided in alignment with engineering best practices.

The ADS shall provide an interface for the purposes of maintenance and repair by authorized persons.