

E. Section [5.3(GTR) / 7.3 (UNR)] – Safety Case

47. Paragraph 5.3.1.3 (GTR) / 7.3.1.3 (UNR)

Pr. Medium

Subject Text:

The system description shall describe how the Operational Design Domain has been defined for each ADS feature and explain the boundaries of each of the conditions in which the feature is designed to operate. This shall include at least the following:

- (a) Geographic limitations,
- (b) Roadway characteristics (e.g., road type, road conditions, speed limit),
- (c) Environmental conditions (e.g., weather, illumination), and
- (d) Dynamic elements (e.g., kinds of other road users).

Explanation:

The manufacturer could choose to define the ODD of its ADS features in a variety of ways depending on their system design, use case, and the expected operating conditions in the intended area of operation. The four categories in the regulation are expected to be broken down one or more levels to appropriately define the operating domain.

Each ADS feature should have its own ODD, which could be defined by the same set of attributes with different boundary conditions (e.g. a highway feature could be restricted to highways while a parking feature could be limited to certain parking lots; the highway feature might not be capable of operating in heavy rain while the parking feature might have no such restriction).

The boundaries of each condition refer to the limits of attribute values beyond which the ADS is outside its ODD (e.g. the ADS feature could be designed to operate only in traffic circumstances in which it can maintain a speed between 20km/h (lower boundary) and 50km/h (upper boundary); The ADS feature would be outside of its ODD in traffic situations not within that speed range.).

Certain ODD attributes may be interdependent – for example, the distance at which the ADS can detect objects may be impacted by weather (e.g. fog, rain, snow, dirt, sensor performance reduction etc.). The impact of reduced capability may lead the ADS to travel at lower speeds and/or avoid certain roads that may require better detection capabilities. The links/dependencies between ODD parameters, if any, should be identified as part of the ODD definition.

The ODD should be defined in a manner that its attributes can be measured/tracked by the ADS directly or indirectly, onboard or offboard to determine if the current operating conditions are within the defined boundaries. (i.e. The ADS needs to know if it is within its ODD)

The ODD defines conditions under which the ADS feature is designed to operate, which might or might not include geographic limitations (sometimes referred to as a geo-fence). These geographic limitations could be used to prevent a feature from operating in an area that has traffic laws for which the ADS was not designed (i.e. outside the ODD) or in certain areas where there is additional complexity that has not been designed for (e.g. different road user behaviour or traffic flows).

These geographic limitations are distinct from the area of operation (not mentioned in the regulation) that reflect a manufacturer's choice of where to operate in light of either available vehicle supply or operational support capacity, or the boundary of an area of permissible operation approved by a government authority. The manufacturer could choose to include area of operation restrictions within its ODD definition.

For example, an ADS feature could be designed to operate on any controlled access highway with speeds up to 120 km/h (which would constitute a road type ODD condition), but the

manufacturer could choose to operate the system in just one geographic area (area of operation), either due to limited vehicle availability or the need to obtain government approval in other geographic areas (i.e. the area is within the ODD, but outside the area of operation).

A single ODD could be substantiated in many areas, that is, all these areas fit the ODD definition and bounds. It is also possible that a new area falls within the existing ODD bounds and therefore deployment in that area (i.e. expanding the area of operation) might not require modification to the ODD, rather confirmation that the new area is within the ODD with no new behaviours or traffic flows. As such, removal or modifications of the area of operation would not on require modification to the ODD as long as the conditions and environment in the new area(s) of operation, including road user behaviour and traffic flows have been considered in the ODD. However, a modification of the area of operation that entails operation in an area with different traffic laws than those for which the ADS's ability to comply has been demonstrated in the safety case (i.e. outside the ODD) would require an amendment to the safety case demonstrating the ADS's ability to comply with those different local/regional/national rules in the new areas area of operation. For clarity, the area of operation, including the reasons for using that area of operation could be provided as reference (e.g. operational considerations, capability restrictions etc.) and an explanation for the existence of geographic limitations within the ODD definition could be included to clarify the reason for the use of those limitations (e.g. required local/regional approvals, local/regional traffic rules, etc.)

ODD definition standards/best practices:

- ISO 34503 (BSI/PAS 1883)

- AVSC00002202004

48. Paragraph 5.3.1.4.2 (GTR) / 7.3.1.4.2 (UNR) & 5.3.1.4.2.1 (GTR) / 7.3.1.4.2.1 (UNR)

Subject text:

5.3.1.4.2. / 7.3.1.4.2. The outlines shall include the components/functions of the ADS and other vehicle systems that are relevant to meeting the requirements of this Regulation.

5.3.1.4.2.1. / 7.3.1.4.2.1. The outlines shall show interconnections between the components/functions of the ADS and those components/functions and other systems via:

- (a) A circuit diagram for the electrical transmission links,
- (b) A piping diagram for pneumatic and/or hydraulic transmission equipment, and
- (c) A simplified diagrammatic layout for mechanical linkages.

Explanation:

In this context, other vehicle systems could include information that originates from outside the vehicle if they are used to meet the requirements of the regulation (e.g. certain information could be used to detect ODD boundaries such as weather reports, traffic reports, construction zones etc.)

The electrical transmission links could also capture methods for transmitting signals via electrical wire, fibre optics or wireless means. The manufacturer could decide to use a different type of diagram for these purposes as long as the information is present.

Additional information with regards to wireless links could be included (e.g. frequency, bandwidth, approx. range, link speed/capacity, resistance to interference/obstructions)

49. Paragraph 5.3.1.4.3 (GTR) / 7.3.1.4.3 (UNR)

Subject text:

The outlines shall include how the following functions and aspects are addressed:

- (a) Sensing and perception of events and objects,
- (b) Decision-making and planning,
- (c) Remote interactions and remote monitoring by a remote supervision centre (if applicable),
- (d) Information display/user interface,
- (e) The data storage system (e.g., Data Storage System for Automated Driving), and

(f) Redundancies of relevant components and/or connections.

Explanation:

The list consists of items to include for the outline in the safety concept. Some items included in this list might not be separate components or systems.

50. Paragraph 5.3.1.9 (GTR) / 7.3.1.9 (UNR) & 5.3.1.10 (GTR) / 7.3.1.10 (UNR)

Pr.

Medium

Subject text:

5.3.1.9. / 7.3.1.9. The system description shall indicate the categories of other road users with whom the ADS is designed to interact (e.g., pedestrians, cyclists, etc) and describe the nature of their interactions with the ADS.

5.3.1.10. / 7.3.1.10. The system description shall identify the ADS users with whom the ADS is designed to interact and describe the nature of their interactions with the ADS.

Relevant paragraphs:

2.21. "Other road user (ORU)" means any entity making use of publicly accessible road infrastructure.

4.1.2.4. / 6.1.2.4. The ADS shall detect and respond to objects and events relevant to its performance of the DDT.

4.1.2.7. / 6.1.2.7. The ADS shall interact safely with other road users.

4.1.2.8. / 6.1.2.8. The ADS shall avoid collisions with safety-relevant objects.

Explanation:

While the ADS Performance of DDT requirements set out appropriate interaction and collision avoidance rules for other road users, it does not require the manufacturer to explain what those interactions might be. The requirement in 5/7.3.1.9 attempt to bridge this gap by requiring the identification of road users categories the ADS can interact with and the nature of those interactions. The ADS could be designed with ways to communicate with other road users via light or sound. For example:

- The ADS could have light projections on the road to signal its intentions
- The ADS could use the vehicle horn to warn animals, pedestrians or other vehicles of its presence
- The ADS could be capable of indicating it is yielding to another vehicle or pedestrian via sound, symbol, light flashes or other methods.

Similarly, while the ADS requirements - Interactions between the ADS and its User(s) section set out appropriate interaction requirements with ADS users, it does not require the manufacturer to explain what those interactions might be nor which users are considered in the particular ADS design. The requirements in 5/7.3.1.10 attempt to bridge this gap by requiring the identification of the users and the nature of their interactions.

51. Paragraphs 5.3.1.4.3 b) (GTR) / 7.3.1.4.3 b) (UNR), 5.3.1.11 (GTR) / 7.3.1.11 (UNR) and 5.3.1.12 (GTR) / 7.3.1.12 (UNR), 5.3.1.16.1 c) (GTR) / 7.3.1.16.1 c) (UNR)

Pr. High

Subject Text:

5.3.1.4.3. / 7.3.1.4.3. The outlines shall include how the following functions and aspects are addressed:

(c) Remote supervision and remote monitoring by a remote supervision centre (if applicable),

5.3.1.11. / 7.3.1.11. If the ADS can request a remote intervention, the system description shall describe the nature and process for such interaction.

5.3.1.12. / 7.3.1.12. The system description shall describe the methods of activating,

overriding, or deactivating the ADS feature by any or all of: the ADS user (where relevant), remote intervention (where relevant), passengers (where relevant), or other road users (where relevant).

5.3.1.16.1 / 7.3.1.16.1 If a partial performance mode of operation is used under certain fault conditions (e.g. in case of severe failures), The manufacture shall describe:

(c) the warning strategy to the users/remote supervision centre (if applicable).

Explanation:

There were several discussions around the remote topic during the development of the regulations and the writing of the interpretation. It was clear that remote driving would not be possible in the current version of the regulation given it is a separate topic with wider implications. The text also intended to capture safety-relevant situations where there was input remotely rather than situations where a user requested non-safety relevant support/assistance.

The group reviewed existing definitions in SAE J3016-2021 (SAE/ISO PAS 22736:2021) and in EU 2022/1426 and the possibility of introducing new definitions but did not reach consensus.

For example:

- SAE J3016-2021 defines remote assistance but restricts it to humans and providing advice to the ADS, while the discussions saw the possibility of assistance by systems and humans and providing assistance to users and the ADS.
- EU 2022/1426 defines remote intervention operator linking to the EU2022/1426 definition of on-board operator, which deviates from the approach used in this regulation.

In this light, certain terms were used in the text to try and represent the understanding and move forward but which might not align exactly with the strict definitions/uses of those terms in other documents. Manufacturers might wish to use the concepts and terms in those other documents but should note the differences between their use/intent in those documents and in this regulation. Experts have noted that some of the standards are in the process of being updated and new ones created. The terms and definitions in those new documents could better reflect the intent of this regulation and might be used as reference in future iterations of the regulation.

Who/what is it?

The group discussed the possibility that the ADS might communicate remotely with a human or another system (e.g. a system with more powerful computation or additional information such as sensors mounted on infrastructure). The basic concept is that some exchange of information and/or an interaction occurs with an external source. *Use of "remote supervision centre"*

The group discussed the possibility of a centre, housing systems, humans or both intended to provide information remotely and/or monitor the status of vehicles or fleets. The current wording being used for this concept is "remote supervision centre" but was not intended to mean a centre that is restricted to supervision - it could house agents that monitor vehicles/fleets, assist the ADS/users or provide assistance upon request. Further, the ADS should not require "supervision" in the sense of "supervise" in J3016:2021 which is only intended for much less capable driver assistance systems.

Intervention or interaction?

The group had debates around using the terms "intervention" and "interaction", the intent was that the ADS (or a user) would request for remote "assistance" in certain situations leading to an interaction. However, not all interactions are of interest (i.e. only those that are safety-related) which are likely to be only interventions. However, intervention was not intended to have the meaning that a remote person be monitoring the ADS and decide to intervene, the initial request for intervention was intended to originate from the ADS (or its users). The document uses both terms in different places but generally the intent is the same – safety-relevant, ADS/user-initiated interactions with a remote entity.

The ADS should always be in control of the DDT, while it may ask for suggestions in how to resolve/navigate a difficult situation, it could decide to take a different course of action than suggested remotely in the interest of safety (or as the situation evolves).

[.

52. Paragraph 5.3.1.14 (GTR) / 7.3.1.14 (UNR)

Pr. Low

Subject Text :

The system description shall describe the range of end states constituting a mitigated risk condition that can be achieved by the ADS feature, including:

- (a) The conditions that might trigger an attempt to reach a mitigated risk condition,
- (b) The processes by which the ADS feature attempts to reach a mitigated risk condition, and
- (c) The evaluation of risk related to mitigated risk condition end states.

Relevant paragraphs:

2.15. “ADS fallback response” means a system-initiated deactivation procedure or an ADS-controlled procedure to place the vehicle in a mitigated risk condition (MRC).

2.20. “Mitigated Risk Condition (MRC)” means a stable and stopped state of the vehicle that reduces the risk of a crash.

4.1.3.3. / 6.1.3.3. In the event of a collision involving the ADS vehicle, if required to stop by applicable law, the ADS shall fall back to an MRC or bring the vehicle to a standstill as appropriate. During this process, the user may initiate deactivation of the ADS if the design of the ADS allows.

4.1.4.3. / 6.1.4.3 In response to a fault, the ADS shall either:

- (a) Execute a fallback response and prohibit activation of the impacted feature(s) if the fault prevents the ADS from performing the DDT in accordance with the requirements under paragraph 4/6.1., or
- (b) Adapt its performance of the DDT in accordance with the severity of the fault, provided the resulting performance complies with the requirements under paragraph 4/6.1.

4.1.4.4.1. / 6.1.4.4.1 The procedure for remote termination of an ADS performing the DDT shall include the capability to perform an ADS fallback response.

4.1.6. / 6.1.6. Fallbacks to a Mitigated Risk Condition (MRC)

4.1.6.1. / 6.1.6.1. For ADSF-2, the ADS fallback response shall be to place the vehicle in an MRC. The ADS feature may permit a user-initiated deactivation to interrupt the fallback to an MRC.

4.1.6.2. / 6.1.6.2. For ADSF-1, if it has not been possible to complete a system-initiated deactivation procedure, the ADS shall execute a fallback to an MRC. During the fallback to the MRC, the user may initiate the deactivation of the ADS.

4.1.6.3. / 6.1.6.3. Upon completion of an ADS fallback to an MRC, a user may be permitted to assume control of the vehicle.

Explanation:

While the ADS Performance of DDT requirements set out requirements when an MRC is required, they do not specify the process to achieve the MRC, its end state, nor do they capture other situations that could result in the vehicle attempting to reach an MRC.

It is expected that the conditions that might trigger an attempt to reach an MRC would include the situation in the above requirements but could include others that may be dependent on the system design.

The process to reach an MRC is likely to vary depending on the situation and system capabilities and the range of end states that can be achieved. The process for determining what MRC is appropriate for the situation, the risks involved in reaching the MRC and risks

once the MRC is achieved should be documented.

During the process to reach an MRC, it might be appropriate to communicate that the ADS is attempting to achieve an MRC (e.g. hazard lights, horn, V2X signals). MRC end states are expected to be fully stopped with parking brake applied (or other means to prevent vehicle rollaway) and could include activation of hazard lights.

Possible end state examples:

- Stop in lane (current lane, move to slowest lane)
- Stop on shoulder, emergency lane or bus lane
- Exit highway/main road or clear narrow sections (e.g. bridges) to stop in more appropriate location
- Navigate to nearest parking spot (on-road, rest stop, parking lot)

For ADSF-2 vehicles, the expectation would be that the MRC is more technologically involved than an ADSF-1 since the only fallback response of an ADSF-2 is achieving an MRC (while ADSF-1 can rely on a fallback user). (e.g. an ADSF-2 might exit a highway and stop at a rest stop or parking lot while an ADSF-1, if the fallback user does not respond, might only be capable of pulling over to the shoulder or stopping in lane)

The reason for initiating an MRC and the surrounding conditions will have an impact on what is possible – a failure or sudden ODD exit could need a very quick MRC while a situation where there is less risk (planned ODD exit) could allow the ADS to take more time to achieve an MRC.

The intent of an MRC is to limit risk and the risks of reaching the MRC should also be a consideration.

53. Paragraph 5.3.1.16 (GTR) / 7.3.1.16 (UNR)

Subject text:

5.3.1.16. / 7.3.1.16. The system description shall describe how the ADS feature responds to failure situations, including at least one or more following means (as applicable):

- (a) Fallback (or fail-safe) operation using a partial system.
- (b) Redundancy using separate systems.
- (c) Diversity of systems performing the same function.
- (d) Removal of some or all automated driving function(s).

5.3.1.16.1. / 7.3.1.16.1. If a partial performance mode of operation is used under certain fault conditions (e.g., in case of severe failures), the system description shall describe:

- (a) Conditions for activation of that mode (e.g., type of failure),
- (b) Resulting ADS feature behaviour and capabilities (e.g., achievement of a mitigated risk condition immediately), and
- (c) Warning strategy to the user/remote supervision centre (if applicable).

5.3.1.16.2. / 7.3.1.16.2. If a second (backup) or a diverse means to realize the performance of the dynamic driving task is used, the system description shall describe:

- (a) The principles of the change-over mechanism,
- (b) The logic and level of redundancy and any built-in checking features, and
- (c) The resulting limits of effectiveness.

5.3.1.16.3. / 7.3.1.16.3. If the chosen response to a system failure entails the removal of an ADS function, the system description shall describe how it is done in compliance with the relevant provisions of this regulation. It shall also describe how all the corresponding output control signals associated with this function are inhibited.

Relevant paragraphs:

2.23. "Failure" means the termination of an intended behaviour of a system or component due to fault manifestation.

2.24. "Fault" means an abnormal condition that can cause a system or component to fail.

4.1.4.1. / 6.1.4.1. *The requirements for DDT performance in nominal situations shall continue to apply during failure situations as far as is reasonably practicable under the specific circumstances with the aim of minimising overall safety risks.*

4.1.4.3. / 6.1.4.3. *In response to a fault, the ADS shall either:*

- (a) Execute a fallback response and prohibit activation of the impacted feature(s) if the fault prevents the ADS from performing the DDT in accordance with the requirements under paragraph 4/6.1., or*
- (b) Adapt its performance of the DDT in accordance with the severity of the fault, provided the resulting performance complies with the requirements under paragraph 4/6.1.*

Explanation:

While the ADS performance of DDT requirements set out requirements for performance in failure situations, the safety case seeks additional information to determine how the ADS responds to such failures. Section 5.3.1.16. / 7.3.1.16 refer to four means, which are not fully aligned with the 3 more detailed sub-paragraphs. This difference reflects a structural inconsistency rather than an additional obligation and may be considered for clarification in future regulatory iterations.

The listed means describe a possible approach for nomenclature and categorization. Manufacturers could use alternative nomenclature and categorization aligned with their failure management strategies. These strategies could yield different outcomes depending on the situation at hand (i.e. depending on system design, failure impact and risk assessment, the same means could result in fail-operation, fail-degraded, or fail-safe behaviour). A potential mapping is below:

- (a) Fallback (or fail-safe) operation using a partial system.
 - a. This could be consistent with the intent of *.3.1.16.3 if the currently active feature requires the use of those functions and must execute a fallback
 - i. fail-safe
- (b) Redundancy using separate systems.
 - a. Depending on the capabilities of the separate system and assessed risk, this could result in a system that:
 - i. fails operational (could be consistent with the intent of *.3.16.2) or
 - ii. fails degraded (could be consistent with the intent of *.3.16.1 and/or *.3.16.2)
- (c) Diversity of systems performing the same function.
 - a. Depending on the capabilities of the diverse systems and assessed risk, this could result in a system that:
 - i. fails operational (could be consistent with the intent of *.3.16.2) or
 - ii. fails degraded (could be consistent with the intent of *.3.16.1 and/or *.3.16.2)
- (d) Removal of some or all automated driving function(s).
 - a. This could be consistent with the intent of *.3.1.16.3 if the currently active feature can continue without those functions
 - i. fail operational (does not impact current active feature) or
 - ii. fail degraded

Depending on how the system is impacted by the fault/failure and the requirements from 4.1.4.3. / 6.1.4.3, the following information could be provided, where relevant:

1. Fallback (or fail-safe) operation using a partial system – This could describe a fault which prevents the ADS feature from performing the DDT in accordance with the requirements of 4/6.1 resulting in a fallback response & prevention of feature from activation 4.1.4.3/6.1.4.3 a)
 - a. A description of types of failures that could lead to this situation and how the ADS responds to the failure situation
2. Fail-Degraded – This could describe a fault for which the ADS can adapt its performance of the DDT in accordance with the severity of the fault (4.1.4.3 / 6.1.4.3 b). The ADS DDT Performance requirements (4/6.1) can still be met with defined performance limits (e.g. lower operating speed, limitations on road types , avoiding certain intersections/manoeuvres etc.)

- a. Describe what failures lead to performance limits (conditions for activation) and what those limits might be (ADS behaviour and capabilities) and how the transition between full operation and degraded operation occurs (change over mechanism)
 - b. The adapted performance (partial performance mode) might have been considered when defining the ODD boundaries (e.g. reduced visibility leading to lower operating speed).
 - c. Describe the warning strategies & intended warning recipients
3. Fail-Operational – The could describe a failure that does not cause any reduction of DDT performance (i.e. “fail operational” due to redundancy or design)
- a. A description of what types of failures could lead to this situation (conditions for activation), how the ADS responds to the failure situation (change over mechanism) and any resulting limits of effectiveness of the ADS or its remaining redundancies.
 - b. The manufacturer could describe any warning strategies and longer-term mitigation measures (e.g. schedule maintenance to repair/replace component within an appropriate interval) as part of, or alongside built-in checking features

54. Paragraph 5.3.2.6 (GTR) / 7.3.2.6 (UNR)

Pr. Medium

Subject Text:

The safety concept shall describe the conditions that the automated driving 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 as described pursuant to paragraph 5.3.1.3. of this Regulation.

Explanation:

The main objective of this paragraph is to compare the ODD (design – defined in 5/7.3.1.3) with the expected operating conditions (also known as target operating domain) which might not be identical. (e.g. the ODD could be divided highway with no pedestrian access, but it is expected that pedestrians might be encountered in the case of a vehicle breakdown or emergency). This requirement is intended to demonstrate that the manufacturer has identified the expected operating conditions, identified any gaps between the ODD and those conditions, and can justify within its safety case that there are no unreasonable risks due to those gaps.

The expected operating conditions should have been identified via safety and/or engineering processes and the ODD properly defined considering those conditions to avoid unnecessary risks or ODD exits for conditions that are expected with a certain frequency.

The wording is intended to exclude consideration for very unlikely events (e.g. space debris falling) but include events that are expected even if in relatively low frequency (e.g. animal crossing the roadway)

55. Paragraph 5.3.2.7 (GTR) / 7.3.2.7 (UNR) & 5.3.2.9 (GTR) / 7.3.2.9 (UNR) & 5.3.2.10 (GTR) / 7.3.2.10 (UNR)

Pr. Medium

Subject text:

5.3.2.7 / 7.3.2.7 The safety concept shall describe measures or strategies, where applicable, implemented to:

- (a) Prevent or mitigate abuse, misuse, and errors by occupants that could affect safe performance of the DDT (e.g., occupants attempting to access driving controls),
- (b) Prevent, mitigate, or deter harm to occupants caused by external sources (e.g., unauthorised persons attempting to access a vehicle with occupants), and
- (c) Prevent, mitigate, or deter abuse and misuse of the vehicle or its systems from external sources. (e.g., objects placed on vehicles during operation, attempts to damage a vehicle).

5.3.2.9 / 7.3.2.9 The safety concept shall include a list of safety risks to passengers (e.g., safety belts not fastened, passengers not seated) and a description of how they are managed for all passengers while an ADS feature is active.

5.3.2.10 / 7.3.2.10. The safety concept shall describe the strategies in place to avoid operating the vehicle when the general working condition of the vehicle is not satisfactory (e.g., condition of tyres, brakes, lighting, status of external loads, steering). These strategies may include technological solutions, physical inspections or other relevant solutions.

Explanation:

These paragraphs are aimed at tasks that a driver would normally perform but which must now be managed either by the ADS or some other means.

Clarification of abuse, misuse and errors for 5/7.3.2.7

- Errors – action (or lack of action) by the user without intention to cause harm (e.g. pressing a wrong button, believing the ADS feature is still active after deactivation, attempting to override the system by using inappropriate means due to lack of understanding)
- Abuse – action (or lack of action) by the users with intent to circumvent protections or cause harm (e.g. trying to bypass gaze monitoring through use of a mask, attempt to bypass physical barriers around driving controls, causing damage to a vehicle, placing objects in front/on the vehicle to stop it from functioning)
- Misuse – action (or lack of action) by the users to use the system in an unintended way (e.g. ignoring system initiated deactivations in order to finish watching a movie while the vehicle achieves an MRC, holding onto the vehicle to be towed while on a skateboard)

Potential examples of measures or strategies for 5/7.3.2.7

- Dedicated controls for ADS
- Disabling driving controls
- Installing physical barriers around driving controls
- Making noise/light (honking horn, loudspeaker, alarm, hazard lights, high beams)
- Locking doors
- Calling emergency services/remote supervision centre

Potential examples of measures or strategies for 5/7.3.2.9 (see also 4/6.3.7)

- Potential safety risks (non-exhaustive):
 - o occupants are not seated or wearing seat belts (depending on vehicle design)
 - o doors are not closed
 - o capacity of vehicle is exceeded (weight, passenger limit)
- Potential ways to manage (as appropriate):
 - o Detection sensors (weight, door, seat belt, seat position, cabin camera)
 - o Attendant intervention (in-vehicle, at stops, remote)
 - o Warning strategies (labels, audio, visual indicators)

Potential examples of considerations and strategies for 5/7.3.2.10 (see also 4/6.3.7)

- Potential considerations (non-exhaustive)
 - o Brake/tire wear/wheel alignment
 - o Fluid levels
 - o Lamps operational
 - o Trailer coupling / loads secured
 - o Body/window damage
 - o Sensor occlusion (dirt/ice/snow)
 - o Vehicle component malfunctions (steering, speedometer, vibrations/noise)
- Potential strategies (as appropriate):
 - o Periodic inspections (before dispatch/at stops)
 - o Sensors (weight, camera, wear, fluid)
 - o Vehicle attendant / verified by driver prior to activating ADS
 - o Design strategies (e.g. sensors cleared by wipers/washer fluid/defroster)

56. Paragraph 5.3.2.8 (GTR) / 7.3.2.8 (UNR)

Subject text:

The safety concept shall describe strategies to limit sudden ODD exits and frequent activation and deactivation situations.

Relevant paragraphs:

4.1.5.1. / 6.1.5.1. *The ADS shall recognise the conditions and boundaries of the ODD of its feature(s).*

4.1.5.4. / 6.1.5.4. *The ADS shall execute a fallback response when one or more ODD conditions of the feature in use are no longer met.*

4.1.5.5. / 6.1.5.5. *The ADS shall be able to anticipate and safely respond to foreseeable exits from the ODD of each feature.*

Explanation:

As there is risk in performing a fallback response (whether transition to driver or achieving an MRC) and that an ODD exit requires a fallback response, the ADS should have strategies to reduce the overall risk to the extent possible when operating in situations near the boundaries of the ODD. The ADS is required to recognise the conditions and boundaries of its ODD and anticipate foreseeable exits.

This requirement seeks to understand the strategies used to reduce the possibility of:

- Sudden ODD exits - this is intended to describe situations that cause an ODD exit with no time to warn a fallback user the transition is coming, or to adjust operating parameters to avoid the exit. (e.g. sudden heavy rain, unanticipated construction zone/road closure/collision ahead)

○ Potential strategies

- monitor weather forecasts for upcoming conditions that may be outside the ODD
- limit operation on certain roadways during certain times of day/events.
- monitor roadway status information

- Frequent activation and deactivation situations (i.e. operating very near the boundaries of the ODD ; e.g. there is an ODD exit but the user can almost immediately reactivate the system, after activation, the system shortly has another ODD exit)

○ Potential strategies

- hysteresis
- only allowing activation of feature if well within ODD limits

57. Paragraph 5.3.3.1 (GTR) / 7.3.3.1 (UNR)

Pr. High

Subject text:

5.3.3.1. / 7.3.3.1. The safety case shall include a series of claims for each of which there must be at least one supporting argument.

5.3.3.1.1. / 7.3.3.1.1. Each argument shall be supported by at least one piece of evidence.

5.3.3.1.2. / 7.3.3.1.2. Each claim, argument, and piece of evidence shall be uniquely labelled but may be used more than once (i.e., a piece of evidence may support more than one argument).

Relevant paragraphs:

2.32. *“Safety case” means structured documentation that provides a compelling, comprehensible, and valid case that the ADS meets the relevant ADS requirements of this regulation and is free from unreasonable risks to the ADS vehicle user(s) and other road*

users.

2.32.1. “Argument” means a written explanation within a safety case that captures the logical connections between a claim and the evidence for achievement of that claim.

2.32.2. “Claim” means a verifiable statement within a safety case.

2.32.3. “Evidence” means material pertinent to demonstrating the validity of a claim, such as physical test results, simulation results, analyses with supporting data, etc.

Explanation:

The safety case is composed of a series of claims supported by arguments and evidence. The manufacturer could use different notations, concepts or terminology as long as the safety case explains how it corresponds to claims, arguments and evidence and that an appropriate mapping to the requirements of the regulation can be described (e.g. ISO/IEC/IEEE 15026-2). There are several ways to approach documenting claims, arguments and evidence the examples given below is not the only possible approach.

Example 1: (ADS meets the relevant ADS requirements of this regulation)

- Claim C-001: The ADS can detect and respond safely to faults
 - o Subclaim SC-001: The ADS detects faults, malfunctions and abnormalities that compromise its capability to perform the DDT within the ODD (req. 4/6.1.4.2)
 - Argument A-001: Analysis was made to determine which components/systems could impact the performance of the DDT if they exhibit a fault, malfunctions or abnormality (E-001). An algorithm is used to detect such faults (E-005) and is installed in such a way that it can monitor those components (E-004). A test procedure was created to simulate a fault in a component (E-002). The test procedure was run multiple times to generate faults on different components and all tests resulted in a positive detection and appropriate action taken (E-003).
 - Evidence E-001: Analysis determining which components/systems could impact the performance of the DDT if they exhibit a fault, malfunction or abnormality
 - Evidence E-002: Testing procedure to generate faults, malfunctions and abnormalities in a component
 - Evidence E-003: Test results showing algorithm can detect faults, malfunctions and abnormalities when tested as per testing procedure (E-002) & results in a fallback response
 - Evidence E-004: Diagram/schematic showing where fault detection algorithm is installed and its connections with monitored components
 - Evidence E-005: Description of how the algorithm functions, assumptions and capabilities
 - o Subclaim SC-002: In response to a fault the ADS executes a fallback response (req. 4/6.1.4.3)
 - Argument A-002: When the detection algorithm detects a fault, malfunction or abnormality (see SC-001), a fallback response is triggered (E-006). No adaptation in performance is used. The effectiveness of the detection algorithm is confirmed by running testing procedure (E-002) with results (E-003).
 - Evidence E-002: Testing procedure to generate faults, malfunctions and abnormalities in a component
 - Evidence E-003: Test results showing algorithm can detect faults, malfunctions and abnormalities when tested as per testing procedure (E-002) & results in a fallback response
 - Evidence E-006: Description of how a fallback is triggered when algorithm (E-005) detects a fault, malfunction or abnormality.

Example 2: (ADS is free from unreasonable risks.)

- Claim C-002: The acceptance criterion provides an appropriate means to evaluate risk
 - o Subclaim SC-003: The acceptance criterion is predicated upon appropriate

- performance indicators
 - Argument A-003: The performance indicators selected are in line with state of the art risk assessment metrics
 - Evidence E-007: Procedure that outlines use of metrics
 - Evidence E-008: Testing results that show implementation of metrics
 - Subclaim SC-004: The acceptance criterion leverages appropriate benchmarks
 - Argument A-004: The benchmarks selected are in line with state of the art benchmarks
 - Evidence E-009: Procedure that outlines use of benchmarks specific to the ODD and use-case
 - Evidence E-010: Testing results that show implementation of metrics compared to benchmarks
 - Subclaim SC-005: The methodology provides credible evidence that the stated acceptance criterion is appropriately evaluated and supports the determination of absence of unreasonable risk
 - Subclaim SC-006: The methodology provides appropriate coverage
 - Argument A-005: The methodology provides adequate coverage according to a taxonomy (known unsafe) and includes feedback mechanism for the discovery of unknown unsafe
 - Evidence E-011: Taxonomy
 - Evidence E-012: Coverage report of Taxonomy
 - Evidence E-013: Feedback process for discovery
 - Evidence E-014: Log of newly discovered unsafe events
 - Subclaim SC-007: The methodology provides credible evidence
 - Argument A-006: The methodology uses robust and conservative methods, including qualified tools, which results in outputs of adequate fidelity and confidence.
 - Evidence E-015: Statistical method to calculate conservativeness
 - Evidence E-016: Conservativeness report
 - Evidence E-017: Process and training for using tools
 - Evidence E-018: Tool qualification report
 - Evidence E-019: Tool training report

Potential references:

- NASA System Safety Handbook (NASA/SP-2014-612)
- GSN Community Standard
- Safety case notations: alternatives for the non-graphically inclined? – C.M. Holloway

58. Paragraph 5.3.3.7 (GTR) / 7.3.3.7 (UNR)

(ADS-17)

Subject text:

Each requirement defined under paragraphs 5/7.3.3.2, 5/7.3.3.4, 5/7.3.3.6., and as may be defined by the manufacturer shall have at least a claim

Relevant paragraphs:

5.3.3.2. / 7.3.3.2 *The claims, arguments, and evidence shall be understandable, logical, correct, and robust and shall demonstrate that:*

- (a) *The ADS is free of unreasonable risk to ADS user(s) and other road users and*
- (b) *The ADS meets the applicable requirements of this regulation in each of the following areas:*
 - (i) *Performance of the DDT (paragraph 4/6.1.).*
 - (ii) *User interactions (paragraph 4/6.2), except for the user information requirements under*

paragraph 4/6.2.5., and
(iii) Other requirements (paragraph 4/6.3.),

5.3.3.4. / 7.3.3.4 The claims, arguments, and evidence shall describe how the SMS processes (section 5/7.1) have been applied to manage ADS safety throughout the lifecycle of the system.

5.3.3.6. / 7.3.3.6 The claims, arguments, and evidence shall demonstrate that the approach to testing is suitable for the demonstration of the safety case and the compliance with performance/functional requirements.

Explanation:

The claims, arguments and evidence presented in the safety case needs to demonstrate that:

1. the ADS meets the requirements of the regulation and
2. that it is free of unreasonable risks

To demonstrate it meets the requirements, there should be at least one claim (or subclaim) that presents argumentation and evidence that each requirement is met. The applicable requirements are:

- section 4/6 as described in 5/7.3.3.2 b),
- identified through the application of SMS process as described in 5/7.3.3.4, and,
- suitability of testing approaches as described in 5/7.3.3.6

To demonstrate that the ADS is free of unreasonable risk, the manufacturer might have claims beyond those set out in the requirements of this regulation. There should be at least one claim (or subclaim) that presents argumentation and evidence that the ADS is free of unreasonable risks.

59. Paragraph 5.3.3.9 (GTR) / 7.3.3.9 (UNR)

Pr. Low

Subject text:

Evidence supporting argumentation shall consist of test results or analysis (e.g., system layout and schematics, photographs, required documentation, etc.) as appropriate.

Relevant paragraphs:

2.32.3. "Evidence" means material pertinent to demonstrating the validity of a claim, such as physical test results, simulation results, analyses with supporting data, etc.

Explanation:

Evidence supporting a claim is not restricted to testing results. It could include any supporting documentation the manufacturer believes supports its argumentation that the claim is met. The evidence should be relevant to the claim as explained in the argumentation rather than a series of unrelated documents without explanation. Examples of possible non-testing evidence:

- Testing procedures/protocols
- Diagrams / schematics
- Code
- Photographs / video
- Certificates
- Analysis information
- Research studies/publications
- Internal standards
- Reviews / inspections

G. Section [6.3 (GTR) / 8.3(UNR)] – Assessment of the safety case

59. Paragraph 6.3.1.4 b) (GTR) / 8.3.1.4 b) (UNR)

(ADS-17)

Subject text:

(GTR) The assessment shall review the manufacturer's safety case for robustness to verify that at least the following criteria have been met:

(b) The integrity level used for development, verification, and validation of the ADS and its features is appropriate to reduce the risk below the unreasonable risk threshold,

(UNR) The approval authority or its designated technical service shall review the manufacturer's safety case for robustness to verify that at least the following criteria have been met:

(b) The integrity level used for development, verification, and validation of the ADS and its features is appropriate to reduce the risk below the unreasonable risk threshold,

Explanation:

The intent of this paragraph is to verify that the level of robustness and integrity documented in the safety case for the development, verification, and validation of the ADS and its features is appropriate to reduce the risk below the unreasonable risk threshold. This includes documenting the confidence/rigor of the tools, processes and testing used during the development, verification and validation stages in claims that are supported by arguments and evidence.

The intent is not to require that integrity levels be defined, but rather to verify that the development, verification and validation processes used are appropriate and proportional to the risks that have been identified.

For example: In the ISO 26262 approach - Automotive Safety Integrity Level (ASIL):

- Risk is based on severity, exposure and likelihood
- ASIL is based on severity, exposure and controllability.

Higher ASIL levels indicate that a higher degree of rigor was applied and would be appropriate for the elements with highest degrees of risk.

In this context, the requirement tries to verify that the tools, methods or tests results meet the level of integrity as deemed necessary for the system in development. The rationale for the acceptable level of accuracy, confidence or repeatability needs to be documented in claims and supported by evidence.
