E. [JR1]Section [5.3(GTR) / 7.3 (UNR)] – Safety Case[2]

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) Intended area of operation (e.g., jurisdictions, 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).[JR3]

Explanation:

The manufacturer may 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[4]. The four categories in the regulation are expected to be broken down several levels to appropriately define the operating domain.

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

The boundaries[5][JR6] of each condition refer to the limits of attribute values beyond which the ADS is outside its ODD (e.g. the ADS feature may 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** to determine if the current operating conditions[7] 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 may or may not include geographic limitations (sometimes referred to as a geo-fence). Unlike other ODD conditions (e.g., road configuration, weather conditions), geographic limitations are generally not related to the ADS feature's capabilities. Often such limitations reflect a manufacturer's choice of where to operate in light of either available vehicle supply or operational support capacity, or they may reflect the boundary of an area of permissible operation approved by a government authority.

For example, an ADS feature may 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 may choose to operate the system in just one geographic area, either due to limited vehicle availability or the need to obtain government approval in other geographic areas.

Removal or modifications of such geographic limitations would not on their own require modification to the applicable safety case, assuming all other ODD conditions are the same in the old and new areas of operation. However, a modification of geographic limitations in

the ODD 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 would likely require an amendment to the safety case demonstrating the ADS's ability to comply with those different local/regional/national rules in the new geographic areas. Similarly, a single ODD could be substantiated in many locations, that is all of these locations fit the ODD definition and bounds. It is also possible that a new location falls within the existing ODD bounds and therefore deployment in that location does not require modification to the ODD, rather confirmation. For clarity, an explanation for the existence of geographic limitations could be included with the ODD definition to clarify the reason for the use of those limitations (e.g. required local/regional approvals, local/regional traffic rules, operational considerations, capability restrictions etc.)[JR8][JR9]

ODD definition standards/best practices:

- ISO 34503 (BSI/PAS 1883)
- AVSC00002202004

48. 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).[JR10][JR11]

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 may be. The ADS may 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 may be nor which users are considered in the particular ADS design.

49. 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) *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),[JR12][JR13]

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).

Explanation:

[Remote monitoring does not provide the ADS with any tactical or operational DDT support.**]**

[Remote intervention provides the ADS with tactical DDT support but does not provide operational DDT support. Remote driving (tactical and operational DDT) is not in scope of the regulation.**]**

[A remote supervision centre is intended to describe a facility that could include the capabilities for remote monitoring and/or remote interventions.**]**

Remote monitoring can provide strategic information (e.g. a customer is waiting for pickup at this location) to the ADS (i.e. a dispatch centre), it could facilitate interaction with users (i.e. customer support) or call for emergency services/roadside assistance.

Remote intervention (which is referred to as "remote assistance" in SAE J3016)[14] could[JR15] be requested **by the ADS** when the ADS is faced with a difficult/ambiguous situation. The ADS may communicate information relevant to the problematic situation and/or present several potential courses of action **(e.g. by proposing a trajectory)**. The remote intervention provides support but does not undertake the DDT directly. The ADS remains in control of tactical and operation DDT functions- and fallback response, and can refuse a suggested course of action if it deems it unsafe (e.g. the situation evolves).

Remote interventions allow for a more rapid resolution of issues. They could potentially be performed by a human or software (e.g. a system with more powerful computation or additional information). It could be thought of as a 2nd opinion on how to navigate a difficult situation. e.g. – There are some traffic cones around an area, but it is unclear if the correct path around is to one side or the other.

e.g. – There is an unknown object/interaction/situation, and it is unclear how to navigate it

50. 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 4.1., 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 4.1.

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.[JR16]

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 may 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 may be appropriate to communicate 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 may exit a highway and stop at a rest stop or parking lot while an ADSF-1 may 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 may need a very quick MRC while a situation where there is less risk (planned ODD exit) may 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.

51. Paragraph 5.3.1.16 (GTR) / 7.3.1.16 (UNR) ~~[17]~~

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):

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 4.1., 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 4.1.

Explanation:

While the ADS Performance of DDT requirements set out requirements for performance in failure situations, additional information is required to determine how risks in these situations have been addressed. Three possibilities are considered:

1. Fail-Safe - The failure prevents the ADS feature from performing the DDT (Fallback response & prevent feature from activating) (5/7.3.1.16.3)
    a. Describe what types of failures could lead to this situation and how the situation might be handled
2. Fail-Degraded - The failure requires limiting the performance of the ADS, but ADS DDT Performance requirements can still be met with those performance limits (e.g. lower operating speed, limiting road types that can be used, avoiding certain intersections/manoeuvres etc.) (5/7.3.1.16.1)
    a. Describe what failures lead to performance limits and what those limits may be and how the transition between full operation and degraded operation occurs
    b. Note that certain partial performance modes may have already been considered depending on how the ODD was defined (e.g. fault causing lower visibility leading to lower operating speed). Other partial performance modes should be explained including what types of failures can lead to partial performance modes, and how the ADS feature performance or capabilities are impacted. [JR18][JR19]
3. Fail-Operational - The failure does not cause any reduction of performance (i.e. “fail operational” due to redundancy or design) (5/7.3.1.16.2)
    a. Describe what failures would not cause any performance reduction and how the system may react to detecting such a failure (e.g. switch over to a redundant component)

b. How those failures might be dealt with in longer-term (e.g. schedule maintenance to repair/replace component)[JR20]

c. Additional information may be required to understand why a failure would not lead to degraded operation or prevent a feature from operating. (e.g. redundant components exist, failure does not impact DDT performance etc.)

~~51.~~52. Paragraph 5.3.2.~~9~~7 (GTR) / 7.3.2.~~9~~7 (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 may not be identical. (e.g. the ODD may be divided highway with no pedestrian access, but it is expected that pedestrians may be encountered in the case of a vehicle breakdown or emergency).

The expected operating conditions should have been identified via safety and/or engineering processes and the ODD properly defined considering those conditions to avoid 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 expected even if in relatively low frequency (e.g. animal crossing the roadway)

Reasonably likely but infrequent or low risk expected conditions may be outside the ODD leading to a fallback response. However, expected conditions with higher frequency or risk profiles that are outside a feature's ODD might indicate that the feature cannot safely operate in that environment.

~~52.~~53. Paragraph 5.3.2.8~~10~~ (GTR) / 7.3.2.8~~10~~ (UNR) *Pr. Medium*

Subject text:

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).

Explanation:

This is intended to encompass strategies that may be taken to prevent/avoid/mitigate situations which would normally be handled by a driver. e.g.

- 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

54. Paragraph 5.3.2.9 (GTR) / 7.3.2.9 (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) the ADS should have strategies to limit ODD exits to the extent possible.
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
  - (e.g. monitor weather forecasts for upcoming conditions that may be outside the ODD; limit operation on certain roadways during certain times of day/events).
- Frequent activation and deactivation situations (i.e. operating very near the boundaries of the ODD)
  - (e.g. hysteresis; only allowing activation of feature if well within ODD limits **and only** **[21]**[JR22]**triggering a fallback if a sustained ODD exit has been detected**)[JR23]

~~53.~~55. 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 ***process documentation,*** *[24][JR25]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.

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

- Claim C-001: The ADS can detect and respond safely to faults
  - 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
    - 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-005). No adaptation in performance is used. This 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
    - 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 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 evaluation 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

56. Paragraph 5.3.3.7 (GTR) / 7.3.3.7 (UNR) ***(ADS-17)*****[26]**

Subject text:

Each requirement defined under paragraphs 5.3.3.2, 5.3.3.4, 5.3.3.6., 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[27].

Explanation:

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 main requirements for the ADS 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 may 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.

~~54.~~57. 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

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.
For example: In the ISO 26262 approach - Automotive Safety Integrity Level (ASIL):
- Risk is based on severity, exposure and likelihood
- ASIL is based on hazard severity, exposure and controllability.

In this case, we would be interested in verifying that the ASIL is appropriate for the hazards and risks that have been identified.

In this context, it would also apply to the tools, methods or tests results. The rationale for the acceptable level of accuracy, confidence or repeatability needs to be documented in claims and supported by evidence.