New Section	Original Text (copied to each relevant section & relevant text retained)	Proposed Text	Discussion
5.4 Safety Case			
5.4.1 General Description	The manufacturer shall provide a safety case that affirms and provides evidence to demonstrate 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. This shall include the safety concept, which describes the intended use, the operating environment, the interactions with humans, sub-systems and components, control strategies, 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. The safety case shall be in the form of ~~also includes a~~ structured argumentation ~~demonstration~~ supported by evidence, including validation tests. The safety case	The manufacturer shall provide a safety case that affirms and provides evidence to demonstrate 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. This shall include the safety concept, which describes the intended use, the operating environment, the interactions with humans, sub-systems and components, control strategies, 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. The safety case shall be in the form of structured argumentation supported by evidence, including validation tests. The safety case shall also include the	

	shall also include the demonstration of credibility and suitability of test tools used in generating evidence and the processes for reinforcing ADS safety throughout the life of the system~~, that the ADS will be free from unreasonable risk.~~	demonstration of credibility and suitability of test tools used in generating evidence and the processes for reinforcing ADS safety throughout the life of the system	
5.4.2 Safety Concept			
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 components & interactions	(a) Inventory of components A list shall be provided, including all the units 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: (i) Perception and objects detection including mapping and	The manufacturer shall provide documentation listing the components in the ADS ~~systems~~ and their link to the function of each ADS feature~~function~~ which shall include: [a, b, c]	

	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). (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 (sensor range, placement, actuator performance)	~~A description shall be provided which gives a clear explanation of all the functions including control strategies of the ADS and the methods employed to perform the dynamic driving tasks within the ODD and the boundaries under which the ADS is designed to operate, including~~ a statement of the mechanism(s) by which control is exercised. ~~aA list of all input and sensed variables shall beis provided and the working range of these defined, along with a description of how each variable affects system behaviour. A list of all output variables which are controlled by the ADS shall be provided and an explanation given, in each case, of whether the control is direct or via another vehicle system. The~~	A description of the physical capabilities of the system shall be provided. This shall include: a) [d] b) The nominal range, placement and coverage area of each sensor c) The nominal capabilities of control actuators	

	~~range of control exercised on each variable shall be defined.~~ (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		

	(e) ADS specifications: (i) Description of ADS specifications in nominal~~, critical, and failure~~ situations, acceptance criteria and the demonstration of compliance with those criteria; ~~(ii) List of applied regulations, codes, and standards~~ [specifications related to performance of sensors, processors, actuators etc.)		
- Redundancies	(e) ADS specifications: (i) Description of ADS specifications in nominal, critical, and failure situations, acceptance criteria and the demonstration of compliance with those criteria; ~~(ii) List of applied regulations, codes, and standards~~ ~~The safety concept element of the safety case shall provide an explanation of the~~ design provisions built into the ADS to ensure functional and operational safety. Possible design provisions	Identification of redundant components, relationships and interconnections.	

Commented [RJM(1]: There is another section on failures - this one is focused on identifying which systems are redundant in the diagrams - perhaps better integrated in Listing of components & interactions

	in the ADS include: (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; (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 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). If the chosen provision selects a second (back-up) 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 back-up checking features shall be explained and the resulting limits of back-up~~		

	~~effectiveness defined. If the chosen provision selects the removal of an automated driving 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~~		
- Inputs & outputs, ranges & limits	~~A description shall be provided which gives a clear explanation of all the functions including control strategies of the ADS and the methods employed to perform the dynamic driving tasks within the ODD and the boundaries under which the ADS is designed to operate, including a statement of the mechanism(s) by which control is exercised. a~~A list of all input and sensed variables shall be~~is~~ provided and the working range of these defined, along with a description of how each variable affects system behaviour. A list of all output variables which are controlled by the ADS shall be provided and an explanation given, in each case,	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 system behaviour. A list of all output variables which are controlled by the ADS shall be provided and an explanation given, in each case, of whether the control is direct or via another vehicle system. The range of control exercised on each variable shall be defined.	

	of whether the control is direct or via another vehicle system. The range of control exercised on each variable shall be defined. (e) ADS specifications: (i) Description of ADS specifications in nominal, critical, and failure situations, acceptance criteria and the demonstration of compliance with those criteria; ~~(ii) List of applied regulations, codes, and standards~~		
5.4.2.1.2 Identification of hazards - risk & severity			
- Using process in SMS	The safety assessment approach shall include a top- down (from possible hazard to design) and bottom-up approach (from design to possible hazards). The safety assessment may be based on a Failure Mode and Effect Analysis (FMEA), a Fault Tree Analysis (FTA), a System-Theoretic Process Analysis (STPA) or any similar process appropriate to system functional and operational safety provided the	The manufacturer shall demonstrate how the hazard identification processes in their SMS have been applied to the ADS ~~System~~. [Check what is in SMS – do we need to list the possible types & ask for justification of appropriateness?]	

Commented [RJM(2]: Open Issue - Need to reference specific items in SMS which are relevant to this section and augment if needed based on original text.

	appropriateness of this process is demonstrated.		
- Known & Unknown combinations	The safety assessment approach shall include a top- down (from possible hazard to design) and bottom-up approach (from design to possible hazards). The safety assessment may be based on a Failure Mode and Effect Analysis (FMEA), a Fault Tree Analysis (FTA), a System-Theoretic Process Analysis (STPA) or any similar process appropriate to system functional and operational safety provided the appropriateness of this process is demonstrated.	[Check SMS]	
- Assessment of risks	[Text may be needed – check SMS]		
- Cybersecurity	(f) Maintenance and repair interface; protection against unauthorized access: ~~(i) The ADS shall provide an interface for the purposes of maintenance and repair by authorized persons;~~ (ii) The ADS shall be designed to protect against unauthorized access to and modification of the ADS functions; (iii) The	[May need to point to UN R155 & augment with f]	

Commented [RJM(4]: Open Issue - Add text accordingly - check with SMS section for starting point

Commented [RJM(3]: The intent here is to understand what is known/unknown about hazards, risks and severity

Commented [RJM(5]: Open Item - Text to define how risks are assessed after they are identified SMS may have some content

Commented [RJM(6]: Open item - Need additional cybersecurity measures/requirements - CS/OTA may be starting point

	measures ensuring protection from unauthorized access shall be provided in alignment with engineering best practices.		
- Physical Security	(g) Reasonably foreseeable misuse by the driver (if applicable) ~~(e.g., the use of a driver availability recognition system and an explanation on how the availability criteria were established), mistakes or misunderstanding by the driver if applicable (e.g., unintentional override) and~~ intentional tampering of the ADS.	[New text needed potential starting point: The ADS shall be designed to protect against unauthorized access to and modification of the ADS functions]O	
5.4.2.1.3 System update management			
- Process for monitoring performance, updating claims, arguments and evidence (as per sms)	[Discussion on how to tackle software updates required]	[open item – some reference in SMS to check and include]	
- Process for validating and distributing new software releases	(f) Maintenance and repair interface; protection against unauthorized access: (i) The ADS shall provide an interface for the purposes of maintenance and repair by authorized persons~~; (ii) The ADS shall be designed to protect against unauthorized access to and modification of the~~	[may need to reference UN R156~~5~~ & augment with f – check SMS section]	

Formatted: Font: 10 pt

Formatted: List Paragraph

Commented [RJM(7]: Open Item - Issues with Physical security, misuse, abuse, use as weapons, unauthorised entry etc.

Commented [RJM(8]: Open Item - Monitoring and update of Safety Case based on deployed performance

Commented [RJM(9]: Open item - How to manage software update and deployment process and potential impacts on safety case/evidence and traceability

	~~ADS functions; (iii) The measures ensuring protection from unauthorized access shall be provided in alignment with engineering best practices.~~		
5.4.2.2 Feature-Level		The requirements in this section shall apply to each feature o~~f~~f the ADS ~~system~~	
5.4.2.2.1 Summary of intended use	The safety case provided by the ADS manufacturer shall include a description of the ADS configuration and the intended uses and limitations on the use of its features which gives a simple explanation of the operational characteristics of the ADS and ADS features	The safety case provided by the ADS manufacturer shall include a description of the ADS configuration and the intended uses and limitations on the use of its features which gives a simple explanation of the operational characteristics of the ADS feature.	
5.4.2.2.2 Operational Design Domain (ODD)			
- Operating Environment	Operational Design Domain (e.g., road speed limits, road type and roadway characteristics, country, environment, road conditions, etc.) and including the ODD conditions and boundaries of each ADS feature in measurable and/or verifiable terms;	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 each element is measured, verified and any linked/dependent	

	~~A description shall be provided which gives a clear explanation of all the functions including control strategies of the ADS and the methods employed to perform~~ the dynamic driving tasks within the ODD and the boundaries under which the ADS is designed to operate~~, including a statement of the mechanism(s) by which control is exercised. aA list of all input and sensed variables shall beis provided and the working range of these defined, along with a description of how each variable affects system behaviour. A list of all output variables which are controlled by the ADS shall be provided and an explanation given, in each case, of whether the control is direct or via another vehicle system. The range of control exercised on each variable shall be defined.~~	variables. This shall include at least the following characteristics: - Road speed limits - Road type and roadway characteristics - Jurisdictions of operation - Any geographic limitations - Environment - Road conditions	
- Intended area of operation	~~A description shall be provided which gives a clear explanation of all the functions including control strategies of the ADS and the methods employed to perform the~~	The manufacturer shall specify the intended area of operation of the ADS feature.	

	~~dynamic driving tasks within the ODD and~~ the boundaries under which the ADS is designed to operate~~, including a statement of the mechanism(s) by which control is exercised. aA list of all input and sensed variables shall beis provided and the working range of these defined, along with a description of how each variable affects system behaviour. A list of all output variables which are controlled by the ADS shall be provided and an explanation given, in each case, of whether the control is direct or via another vehicle system. The range of control exercised on each variable shall be defined.~~		
- Conditions for activating & deactivating (incl fallback)	~~A description shall be provided which gives a clear explanation of all the functions including control strategies of the ADS and the methods employed to perform~~ the dynamic driving tasks within the ODD and the boundaries under which the ADS is designed to operate~~, including a statement of the mechanism(s) by which control is exercised. aA list of all~~	The manufacturer shall document~~state~~: - the conditions that must be present to permit activation ~~required to activate~~ of the feature - the conditions t~~hat~~o trigger a fallback response	

	~~input and sensed variables shall beis provided and the working range of these defined, along with a description of how each variable affects system behaviour. A list of all output variables which are controlled by the ADS shall be provided and an explanation given, in each case, of whether the control is direct or via another vehicle system. The range of control exercised on each variable shall be defined.~~	- the conditions ~~required~~ that must be present to permit deactiv~~at~~ation~~e~~ of the feature - the conditions which may prompt the user to voluntarily take back control, if applicable	
5.4.2.2.3 ~~Human~~ ADS Interactions			
- Identification of users and possible interactions	Interactions with other road users; Interaction with the driver (if relevant) including the transition of control procedures, ADS notifications and fallback user responses; Supervision centre (if relevant);	The manufacturer shall identify possible internal and/or external interactions with users including: - Other road users - Animals - The driver(if relevant) including the transition of control procedures, ADS notifications and fallback user responses - Remote assistant or operator (if relevant)	

Commented [RJM(10]: [End of 2024-09-24 meeting here]

Commented [RJM(11]: Open Item - Text should include not just identification but how this interaction will take place

Commented [RJM(12]: There may be some overlap here with DDT or user Section

Formatted: Highlight

Commented [RJM(14R13]: EU uses Remote Intervention Operator

Formatted: Highlight

- Methods of activating and deactivating	The method of activating, overriding, or deactivating the ADS by any or all of: the ADS user (where relevant), the human supervision centre (where relevant), passengers (where relevant) or other road users (where relevant).	The manufacturer shall describe the methods of activating, overriding, or deactivating the ADS by any or all of: the ADS user (where relevant), the ~~human supervision centre.~~ remote assistant or operator (where relevant), passengers (where relevant) or other road users (where relevant).	
5.4.2.2.4 ADS Functions & Control Strategies			
- In-operation hazard identification & avoidance	Basic performance (e.g. Object and Event Detection and Response (OEDR), etc.); Interactions with other road users; A description shall be provided which gives a clear explanation of ~~all the functions including~~ control strategies ~~of the ADS~~ and the methods employed to perform the dynamic driving tasks ~~within the ODD and the boundaries under which the ADS is designed to operate, including a statement of~~	The manufacturer shall describe how the ADS features detect, identify, and respond to hazards including: - control strategies and methods employed while performing the dynamic driving task - design provisions for functional and operational safety - hazard avoidance and mitigation - management of unknown hazardous scenarios	

Commented [RJM(15]: [to do after London meeting] Combine with hazard identification section above

	~~the mechanism(s) by which control is exercised. aA list of all input and sensed variables shall beis provided and the working range of these defined, along with a description of how each variable affects system behaviour. A list of all output variables which are controlled by the ADS shall be provided and an explanation given, in each case, of whether the control is direct or via another vehicle system. The range of control exercised on each variable shall be defined.~~ The safety concept element of the safety case shall provide an explanation of the design provisions built into the ADS to ensure functional and operational safety. ~~Possible design provisions in the ADS include: (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; (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 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). If the chosen provision selects a second (back-up) 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 back-up checking features shall be explained and the resulting limits of back-up effectiveness defined. If the chosen provision selects the removal of an automated driving 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~~ The documentation shall be supported by an analysis which shows how the ADS will behave to mitigate or avoid hazards which can have a bearing on the safety of the ADS vehicle user(s) and other road users. It shall show how unknown hazardous scenarios will be managed ~~by the manufacturer to keep the residual risk level under control. The chosen analytical approach(es) shall be established by the manufacturer and made available for assessment to the relevant authority before market introduction~~.		
- Minimal Risk Condition (definition, possibilities/scenarios)	Main conditions for achievement of a minimal risk condition;	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 conditions, foreseeable exit, sudden exit	[New text required – requirements may exist in DDT section but may not capture all elements]		
- Fault identification, diagnostic, fallback/minimal risk condition in failure conditions, reduced performance modes	(e) ADS specifications: (i) Description of ADS specifications in ~~nominal, critical, and~~ failure situations, acceptance criteria and the demonstration of compliance with those criteria~~; (ii) List of applied regulations, codes, and standards~~ ~~The safety concept element of the safety case shall provide an explanation of the design provisions built into the ADS to ensure functional and operational safety. Possible design provisions in the ADS include:~~ (a) Fallback (or fail safe) operation using a	The manufacturer shall describe how the ADS features respond 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; (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	

Commented [RJM(16]: Link with DDT section as well

	partial system; (b) Redundancy using separate systems; (c) A list of the potential faults identifiable by the diagnostic system(s) of the ADS; (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 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). If the chosen provision selects a second (back -up) 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 back -up checking features shall be explained and the resulting limits of back -up effectiveness defined. If the chosen provision selects the	failure). The resulting ADS 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). If the chosen provision selects a second (back -up) 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 back -up checking features shall be explained and the resulting limits of back -up effectiveness defined. If the chosen provision selects the removal of an automated driving 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	

Commented [RJM(17]: Modify accordingly to what is defined

	removal of an automated driving function, it shall be done in compliance with the relevant provisions of this regulation. In this case, all the corresponding output control signals associated with this function shall also be inhibited		
5.4.3 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	The safety case shall include arguments and evidence supporting the implementation of the safety concept that is understandable and logical and cover all the different functions of the ADS. ~~The documentation shall also demonstrate that validation measures are robust enough to demonstrate safety (e.g., reasonable coverage of chosen scenarios as part of the validation methodology chosen) and have been completed.~~	The safety case shall include claims, arguments and evidence ~~supporting the implementation of the safety concept~~ that is understandable, ~~and~~ logical and that demonstrate ~~-~~ that the requirements in each of following items are met:~~cover~~: ~~all the different functions of the ADS.~~ - Absence of unreasonable risk to ADS user(s) and other road users - DDT requirements - User requirements - Monitoring requirements - Safety Concept	

support which requirements	The documentation shall provide evidence that the vehicle is free from unreasonable risks to the ADS vehicle user(s) and other road users in the operational design domain. ~~This [may/shall] be achieved through: (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 [or] (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.~~ The safety case shall provide documentation sufficient to allow the relevant authority to verify through assessment of the case and possible testing by the	- [Cybersecurity] - [DSSAD] - Test environment 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 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	

Formatted: List Paragraph

Formatted: List Paragraph, Outline numbered + Level: 1 + Numbering Style: Bullet + Aligned at: 0.25" + Indent at: 0.5"

	authority that the manufacturer has successfully implemented the safety concept applicable to the ADS. The documentation shall itemizes the parameters being monitored on the vehicle and shall set out evidence supporting the argument that applicable safety requirements have been met. This documentation shall also describe the measures in place to ensure the ADS is free from unreasonable risks to the ADS user(s) and other road users when the performance of the ADS is affected by environmental conditions (e.g., climatic, temperature, dust ingress, water ingress, ice packing)	required above and the claims that demonstrate the requirement is met	
- Statement of Assumptions	[New text required]	The manufacturer shall state relevant assumptions it has made in relation to claims, arguments and evidence.	
- Lifecycle validity	[This is alluded to in SMS and in monitoring may be some existing text to reference]		

Commented [RJM(18): End of Session on 4 Oct 2024

- Test tools used for producing evidence have been validated
  - Claims for validity with supporting arguments and evidence
  - Credibility assessment
	(d) Inspection of the documentation that demonstrates the validation/verification plans and results including appropriate acceptance criteria. It shall include testing appropriate for validation, for example, Hardware in the Loop (HIL) testing, vehicle on-road operational testing, testing with real end users, or any other testing appropriate for validation/verification. ~~. The auditor/assessor shall perform an assessment of the physical testing (proving ground and/or public road) environment and shall assess the documentation of the virtual tool chain provided by the manufacturer. The auditor/assessor [may decide to carry out/shall oversee] tests of the complete integrated tool to assess the credibility of the virtual tool chain.~~ The documentation provided shall demonstrate adherence to and be in the form prescribed in [Annex 5] or explain the basis for any deviation from the principles set out in [Annex 5]. ~~Results of validation and verification~~	The safety case shall include claims, supported by argumentation and evidence that any simulation tools used for the generation of evidence have been assessed as per the credibility requirements in [section].	

Formatted: Highlight

	~~[may/shall] be assessed by analysing coverage of the different tests and setting minimal coverage thresholds for various metrics.~~		
5.4.3.2 Claims			
- Provide claim that a specific goal/requirement is met - Provide a summary table identifying which claims support which requirements	The safety case shall provide documentation sufficient to allow the relevant authority to verify through assessment of the case and possible testing by the authority that the manufacturer has successfully implemented the safety concept applicable to the ADS. ~~The documentation shall itemizes the parameters being monitored on the vehicle and shall set out evidence supporting the argument that applicable safety requirements have been met. This documentation shall also describe the measures in place to ensure the ADS is free from unreasonable risks to the ADS user(s) and other road users when the performance of the ADS is affected by environmental conditions (e.g., climatic,~~	The claims shall be detailed enough to allow an authority to verify that the target requirement has been met. The manufacturer may create multiple sub-claims related to claims, arguments, or evidence where a broader claim may not be sufficient or where additional justification is warranted as long as said sub-claims and their relationships are included in the summary documents.	

	~~temperature, dust ingress, water ingress, ice packing)~~		
- Use of sub-claims permitted	[new text required]		
5.4.3.3 Argumentation			
- Analysis supporting claim, providing contextual information how/why claim met	~~The safety case shall provide documentation sufficient to allow the relevant authority to verify through assessment of the case and possible testing by the authority that the manufacturer has successfully implemented the safety concept applicable to the ADS.~~ The documentation shall itemizes the parameters being monitored on the vehicle and shall set out evidence supporting the argument that applicable safety requirements have been met. ~~This documentation shall also describe the measures in place to ensure the ADS is free from unreasonable risks to the ADS user(s) and other road users when the performance of the ADS is affected by environmental conditions (e.g., climatic,~~	Each argument supporting a claim shall provide contextual information and supporting information why a claim is met.	

	~~temperature, dust ingress, water ingress, ice packing)~~		
- Scenario Approach	~~The documentation shall provide evidence that the vehicle is free from unreasonable risks to the ADS vehicle user(s) and other road users in the operational design domain. This [may/shall] be achieved through: (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 [or]~~ (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.	The argumentation shall include analysis of evidence demonstrating that the claim is met including: a) ~~Overall v~~Validation targets (i.e., validation acceptance criteria) supported by validation results provided it is demonstrated that those validation methods are robust enough and/or ~~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~~ b) A scenario-specific approach provided it is demonstrated that the scenarios provide reasonable coverage of	

Commented [RJM(19]: This may not be applicable to every requirement

		the ODD ~~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.~~ Any comparisons drawn between the performance of an ADS feature and that of a manually driven vehicle shall be restricted to data gathered in the same ODD and operating conditions.	
- ODD Coverage	~~The safety case shall include arguments and evidence supporting the implementation of the safety concept that is understandable and logical and cover all the different functions of the ADS.~~ The documentation shall also demonstrate that validation measures are robust enough to demonstrate safety (e.g., reasonable coverage of chosen scenarios as part of the	[combined above]	

Commented [RJM(20]: This may not be applicable to every requirement

	validation methodology chosen) and have been completed. ~~The documentation shall provide evidence that the vehicle is free from unreasonable risks to the ADS vehicle user(s) and other road users in the operational design domain. This [may/shall] be achieved through:~~ (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 [or] (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.		
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)	(d) Inspection of the documentation that demonstrates the validation/verification plans and results including appropriate acceptance criteria. It shall include testing appropriate for validation, for example, Hardware in the Loop (HIL) testing, vehicle on-road operational testing, testing with real end users, or any other testing appropriate for validation/verification. ~~The auditor/assessor shall perform an assessment of the physical testing (proving ground and/or public road) environment and shall assess the documentation of the virtual tool chain provided by the manufacturer. The auditor/assessor [may decide to carry out/shall oversee] tests of the complete integrated tool to assess the credibility of the virtual tool chain. The documentation provided shall demonstrate adherence to and be in the form prescribed in [Annex 5] or explain the basis for any deviation from the principles set out in [Annex 5].~~ Results of validation and verification	Testing results may be presented individually or on aggregate and shall include appropriate acceptance criteria. Each piece of testing evidence shall include enough information or be recorded in such a way that it may be reproduced upon request (e.g. same software/hardware versions, same tool versions, same scenario, same parameters etc.). The manufacturer is required to facilitate access and execution of the necessary tools and analysis software upon request by the authority for the purpose of reproducing this evidence.	

	[may/shall] be assessed by analysing coverage of the different tests and setting minimal coverage thresholds for various metrics.		
- Supporting materials	[new text required]	Evidence other than testing (e.g. source code, engineering drawings, photographs, required documentation, etc.) may be used where appropriate.	

Cross-reference table

Original Paragraph	Inserted into
5.4.1.1 intended use	5.4.2.2.1 Summary of intended use
5.4.1.1 a) ODD	5.4.2.2.2 Operating Environment
5.4.1.1 b) Basic performance	5.4.2.2.4 In-operating hazard identification & avoidance
5.4.1.1 c) Interaction with other road users	5.4.2.2.3 Identification of users and interactions 5.4.2.2.4 In-operating hazard identification & avoidance
5.4.1.1 d) Minimal Risk Condition	5.4.2.2.4 Minimal risk condition
5.4.1.1 e) Interaction with driver	5.4.2.2.3 Identification of users and interactions
5.4.1.1 f) Supervision centre	5.4.2.2.3 Identification of users and interactions
5.4.1.1 g) Activating/deactivating	5.4.2.2.3 Methods of activating and deactivating
5.4.2.1 functions/control strategies	5.4.2.1.1 Physical Capabilities 5.4.2.1.1 Inputs & outputs, ranges & limits 5.4.2.2.2 Operating Environment 5.4.2.2.2 Intended area of operation 5.4.2.2.2 Conditions for activating & deactivating 5.4.2.2.4 In-operating hazard identification & avoidance
5.4.3 a) Inventory of components	5.4.2.1.1 Listing of components & interactions
5.4.3 b) Functions of the units	5.4.2.1.1 Listing of components & interactions
5.4.3 c) Identification of units	5.4.2.1.1 Listing of components & interactions
5.4.3 d) Installation of sensing system components	5.4.2.1.1 Physical Capabilities
5.4.3 e) ADS Specifications	5.4.2.1.1 Physical Capabilities 5.4.2.1.1 Redundancies 5.4.2.1.1 Inputs & outputs, ranges & limits 5.4.2.2.4 Fault Identification, diagnostic …
5.4.3 f) Maintenance & Repair	5.4.2.1.2 Cybersecurity 5.4.2.1.3 Process for validating and distributing new software releases
5.4.4.1 Safety Case	5.4.1
5.4.4.2 Design provisions for funct op safety	5.4.2.1.1 Redundancies 5.4.2.2.4 In-operating hazard identification & avoidance 5.4.2.2.4 Fault Identification, diagnostic …
5.4.4.3 Mitigation/avoidance of hazards	5.4.2.2.4 In-operating hazard identification & avoidance
5.4.4.4 a) – Moved to Assessment	

5.4.4.4 b) – Moved to Assessment	
5.4.4.4 c) Hazard analysis	5.4.2.1.2 – Using processes in SMS 5.4.2.1.2 – Known & Unknown (Risk & severity) combinations
5.4.4.4 d) Verification/validation plan	5.4.3.1 Validation of test tools 5.4.3.4 Test results
5.4.4.5 List of hazards	5.4.2.1.2 Known & Unknown (Risk & severity) combinations 5.4.2.1.2 Assessment of risks 5.4.2.1.2 Cybersecurity
5.4.4.6 Implementation of safety concept and validation methods	5.4.3.1 Safety Case/argument/evidence 5.4.3.3 ODD coverage
5.4.4.7 Free from unreasonable risk	5.4.3.1 Safety Case/argument/evidence 5.4.3.3 Scenario approach 5.4.4.7 ODD coverage
5.4.4.8	5.4.3.1 Safety Case/argument/evidence 5.4.3.2 generation of claims 5.4.3.3 Analysis of claims
5.4.4.9 – moved information to users	