§6.3. Safety case

Green means no change to the text (including no numbering change)

Blue means an editorial proposal.

Orange means an open issue or substantive proposal for amendment.

6.	Manufacturer requirements				
6.3.	Safety case				
6.3.1.	Safety concept				
		6.3.1.1.	The safety case shall include documentation of the safety concept of the ADS and its feature(s).		Add a provision to require documentation of the safety concept with the checklist of items in the following paragraphs.
6.3.1.1.	The safety case shall describe each component of the ADS and any other vehicle systems that are relevant to meeting the requirements of this regulation.	6.3.1.2.	The safety **concept** shall describe the components of the ADS and of any other vehicle systems that are relevant to satisfying the requirements of this Regulation.		
6.3.1.1.1.	The description shall include an ~~outline~~ schematic of the ADS illustrating the equipment distribution and the interconnections among the components and systems.	6.3.1.3.	**The safety concept** shall include a schematic illustrating the equipment distribution and the interconnections among the components and systems.		A schematic, by definition, is an abstract representation, so “outline” is redundant. To communicate the level of detail, it might be useful to consider alternate wording for “illustrating” (e.g., summarizing, overviewing, highlighting,…).
6.3.1.1.2.	The outline shall include how the following elements are addressed:	6.3.1.3.1.	The **schematic** shall illustrate how the following elements are addressed:		
	(a) Perception and objects detection including mapping and positioning,		(a) Perception and detection of objects (including mapping and positioning),		Proposal for clarity and grammar.

(b) Characterisation of decision-making,		
(c) Remote supervision and remote monitoring by a remote supervision centre (if applicable),		*Flagged for review: In the absence of "remote" definitions and in consideration of previous IWG discussions, the IWG should decide whether to retain this provision (and if yes, then definitions for "remote supervision", "remote monitoring", and "remote supervision centre").*
(d) Information display/user interface,		
(e) The data storage system (e.g., DSSAD),	(e) Data Storage System for Automated Driving, and	Sec: We expect DSSAD requirements from the EDR/DSSAD IWG. Subsection 5.3. (Other requirements) will require ADS vehicles to be equipped with a DSSAD. Sec: List should include "and" on the next-to-last item.
(f) Redundancies of components and/or connections.		
6.3.1.2. The safety case shall outline the function of each component of the ADS.	6.3.1.4. The safety **concept** shall outline the function of each component of the ADS.	Establishes the requirement for "the outline".
6.3.1.2.1. The outline shall show the signals linking each function with other components or with other vehicle systems. This may be provided by a labelled block diagram or other schematic, or by a description aided by such a diagram.	6.3.1.4.1. The outline shall show the signals linking each function with other components or with other vehicle systems.	Renumbering and consistent use of "the outline" for clarity.
	6.3.1.4.2. The outline may be provided by a labelled block diagram or other schematic, or by a description aided by such a diagram.	
6.3.1.2.5. Priorities of signals on multiplexed data paths shall be stated wherever	6.3.1.4.3. The prioritisation of signals on multiplexed data paths shall be stated	"may" is used for permissions; "can" is used to indicate that something is possible.

	priority may be an issue affecting performance or safety.		wherever priority can affect performance or safety.	
6.3.1.2.2.	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.	6.3.1.4.3.	The outline shall show interconnections within the ADS via:	Flow: The concept has an outline and the outline shows the items.
			(a) A circuit diagram for the electric transmission links,	*"Electric" or "electrical"?*
			(b) A piping diagram for pneumatic and/or hydraulic transmission equipment, and	
			(c) A simplified diagrammatic layout for mechanical linkages.	*Isn't a "simplified diagrammatic layout" a "schematic"?*
6.3.1.2.3.	The transmission links both to and from other systems shall be shown.	6.3.1.4.4.	The outline shall show any transmission links to and from other systems.	Clarity and flow.
6.3.1.2.4.	There shall be a clear correspondence between transmission links and the signals carried between components and systems.			*What does "clear correspondence" mean here? 6.3.1.4.1. introduces the requirements to outline the signals. Are the "interconnections" in 6.3.1.4.3. synonymous with "transmission links"? Or does "transmission links" only refer to para. 6.3.1.4.4. (i.e., the links to and from other systems)?*
6.3.1.2.5.	Priorities of signals on multiplexed data paths shall be stated wherever priority may be an issue affecting performance or safety.			Moved to be together with other paragraphs on showing signals in the outline (above). Provide outline with signals showing prioritisation of signals where multiplexed.
6.3.1.3.	Each component shall be clearly and unambiguously identifiable (e.g. by marking for hardware, and by marking or software identification for software content).			*What level of the section is this referring to? Is the identification of each component done in the description of the safety concept or in the schematic or in the outline of the transmission/signal links?*
6.3.1.3.1.	This will provide a clear method for identifying the hardware and software in the associated documentation.			

6.3.1.3.2.	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.			*This is a requirement for the software management process, not for the documentation of the safety concept.*
6.3.1.3.3.	Where functions are combined within a single control unit or within a single computer, but shown in multiple blocks in the diagram, then for clarity and ease of explanation, only a single hardware identification marking shall be used.	6.3.1.3.3.	A single hardware marking shall be applied to functions combined within a single control unit or computer regardless of whether the functions are shown in multiple blocks in the diagram.	What are “multiple blocks”?
6.3.1.3.3.1.	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.			
6.3.1.4.	The manufacturer shall provide information regarding the installation options that will be employed for the individual components that comprise the sensing system.			
6.3.1.4.1.	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.			
6.3.1.4.2.	The information shall also include installation specifications that are			

	critical to the ADS's performance such as tolerances on installation angle.		
6.3.1.4.3.	Any changes to the individual components of the sensing system, or the installation options, shall be updated in the documentation.		
6.3.1.5.	A list of all input and sensed variables shall be provided and the working range of these defined, along with a description of how each variable is linked to the control functions of the ADS and potential impacts on system behaviour. This shall include the nominal range, and coverage area of each sensor.		
6.3.1.6.	A list of all of the ADS output variables shall be provided and an explanation given, in each case, of whether the output directly controls the vehicle or is processed via another vehicle system. The range of control exercised on each variable shall be defined as well as the nominal capabilities of control actuators.		
6.3.1.7.	The manufacturer shall demonstrate how their SMS processes for functional and operational safety with regards to risk identification, risk analysis, risk evaluation, risk treatment (including acceptance) and keeping the risk assessments up to date have been applied to the ADS according to [section 6.1.2 Risk Management and section 6.1.3 ADS Design and Development].	China	Propose to delete: The relevant requirement has been already specified in the paragraph 6.3.2.4. ("The manufacturer shall demonstrate through the safety case that the application of the SMS is suitable for managing ADS safety throughout the lifecycle of the system in accordance with 6.1."). Not necessary to duplicate in the safety concept.

6.3.1.7.1	Any operational risk identified in the ADS shall, where appropriate, have mitigations implemented. The ADS manufacturer shall then be able to show the link between the overall risk management process, the mitigations, and the resulting operational risks.		
6.3.1.8.	The manufacturer shall describe how the ADS features detect, identify, and respond to hazards, including the following:		
	(a) Detection and identification of hazards,		
	(b) Design provisions for functional and operational safety (e.g. redundancies),		
	(c) An analysis which shows how the ADS will behave (e.g. control strategies) to mitigate or avoid hazards which can have a bearing on the safety of the ADS vehicle user(s) and other road users, and		
	(d) An analysis that shows how unknown hazardous scenarios will be managed.		
6.3.1.9.	The manufacturer shall describe measures taken to assure the cybersecurity of the ADS and the analysis performed to identify and disposition likely security threats. Where UN R 155 applies, the manufacturer shall describe how the ADS meets the requirements of that regulation.		

6.3.1.10.	The manufacturer shall document measures it has implemented to prevent or deter abuse or misuse of the ADS or its occupants which may normally be performed by a driver. (e.g. unauthorised persons attempting to access a vehicle with occupants, occupant attempting to access driving controls, objects placed on vehicles during operation, attempts to damage a vehicle).		
6.3.1.11.	[Software updates & Safety Case updates as per 6.1.5.2]		OPI: Use of text from Workshop for UNR - 7. Modifications and extension of approval of the vehicle type
6.3.1.12.	The manufacturer shall demonstrate that software updates are validated and confirmed in accordance with SMS section [6.1.5.7] [UNR156].		
6.3.1.13.	The manufacturer shall describe the following aspects of the data storage system:		
	(a) Storage location and crash survivability,		
	(b) Data recorded during vehicle operation and occurrences,		
	(c) Data security and protection against unauthorized access or use, and		
	(d) Means and tools to carry out authorized access to data.		
6.3.1.14.	The safety case provided by the ADS manufacturer shall include a description of each ADS feature		

	configuration including ADS functions applicable to that specific feature, the intended uses and limitations on the use of the feature which gives a simple explanation of its operational characteristics.		
6.3.1.15.	The manufacturer shall document how it has defined the Operational Design Domain for the ADS feature and the boundaries within which it is designed to operate. The manufacturer shall document how the ADS determines the presence/absence of the conditions and any linked/dependent conditions (e.g. reduced speed in icy weather). This shall include at least the following characteristics:		
	(a) Intended area of operation (i.e. Jurisdictions, geographic limitations, etc.)		
	(b) Roadway characteristics (i.e. road type, road conditions, speed limit, etc.)		
	(c) Environmental conditions (i.e. Weather, illumination, etc.)		
	(d) Dynamic elements (i.e. kinds of other road users, etc.)		
		(e) Vehicle status	China
		(f) ADS user's status	China
6.3.1.16.	The manufacturer shall describe the conditions that the driving automation system is reasonably likely to encounter on its trip(s), including, but		

	not limited to, environmental and geographical conditions, and/or the presence or absence of certain traffic or roadway characteristics, and explain how those expected conditions compare to the ODD of the ADS.		
6.3.1.17.	The manufacturer will explain the type of use(s) for which the ADS is intended, such as personal car ownership, urban taxi fleet, goods transportation, highway use, etc.		
6.3.1.18.	The manufacturer shall document:		
	(a) The conditions that must be present to permit activation of the feature,		
	(b) The conditions that trigger a fallback response,		
	(c) The conditions that must be present to permit deactivation of the feature, and		
	(d) The conditions which may prompt the user to voluntarily take back control, if applicable.		
6.3.1.19.	The manufacturer shall identify the other road users with whom it is designed to interact.		
6.3.1.20.	The manufacturer shall identify the ADS users, including remote users with whom it is designed to interact and describe the nature of their interaction with the ADS, distinguishing those who provide remote assistance from those, if any, who perform remote driving.		

6.3.1.21.	The manufacturer shall describe the methods of activating, overriding, or deactivating the ADS feature by any or all of: the ADS user (where relevant), the remote assistant or operator (where relevant), passengers (where relevant) or other road users (where relevant).		
6.3.1.22.	The manufacturer shall describe the range of end states constituting a mitigated risk condition that can be achieved by the ADS feature. This shall include:		
	(a) The conditions which may 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.		
6.3.1.23.	The manufacturer shall describe how the ADS detects and responds to approaching and crossing of ODD boundaries. This shall include strategies to limit sudden ODD exits and frequent activation/deactivation situations.		
6.3.1.24.	The manufacturer shall describe how the ADS feature responds to failure situations, including:		
	(a) Fallback (or fail safe) operation using a partial system,		

	(b) Redundancy using separate systems,		
	(c) A list of the potential faults identifiable by the diagnostic system(s) of the ADS feature,		
	(d) Removal of some or all automated driving function(s),		
	(e) Failure of a vehicle system or component other than the ADS that precludes the ADS from performing the DDT.		
6.3.1.25.	If a partial performance mode of operation is used under certain fault conditions (e.g. in case of severe failures), The manufacture shall describe:		
	(a) the conditions for activation of that mode (e.g. type of failure),		
	(b) the resulting ADS feature behaviour and capabilities (e.g. achievement of a minimal risk condition immediately), and		
	(c) the warning strategy to the driver/remote supervision centre (if applicable).		
6.3.1.26.	If a second (backup) means to realize the performance of the dynamic driving task is used, the manufacturer shall describe:		
	(a) the principles of the change-over mechanism,		

	(b) the logic and level of redundancy and any built-in backup checking features,		
	(c) the resulting limits of backup effectiveness.		
6.3.1.27.	If the chosen provision selects the removal of an ADS function, it shall be done in compliance with the relevant provisions of this regulation. In this case, all the corresponding output control signals associated with this function shall also be inhibited.		
6.3.1.28.	The safety case shall demonstrate that suitable and documented processes have been used to derive behavioural competencies and scenarios that are ODD-relevant and relevant to the ADS safety concept.		Pending consensus with Test Environment OPI.
6.3.1.28.1.	The methodology in the Annex [X] is a suitable process to derive behavioural competencies.		Pending consensus with Test Environment OPI.
6.3.1.29.	The safety case shall demonstrate that processes to identify and generate scenarios:		Pending consensus with Test Environment OPI.
	(a) covers the appropriate nominal, critical and failure scenarios,		
	(b) takes into account data driven, knowledge driven and stochastic approaches to systematically identify hazardous events and other occurrences used to develop scenarios,		

	(c) consider ODD restrictions that are consistent with real world operations OR properly consider scenario elements (especially dynamic elements) that are representative of existing traffic conditions consistent with the ODD,		If all items in list required, then add “and”.
	(d) properly maps and characterizes the behaviours of all the elements included in the scenarios		
6.3.1.29.1.	The safety case shall demonstrate that the set of scenarios resulting from the scenario generation and identification process is suitable for demonstrating ADS safety and to cover the space of reasonably foreseeable situations and conditions that the ADS will encounter during its real-world operations. In particular the set of scenarios selected as evidence to support the ADS safety case includes at least:		
	(a) a sufficient number of scenarios reaching ODD limits,		Add “and”?
	(b) reasonably foreseeable scenarios that are not deemed to be preventable by the ADS (e.g. related to unsafe behaviours by other road users or to inappropriate infrastructural elements).		
6.3.1.29.2.	The methodology in the Annex [XX] is a suitable process to generate scenarios		This is not a requirement. Propose to delete. Method for generating scenarios inherent in analysis of

	that cover reasonably foreseeable situations and conditions.		ODD so should be covered by paired provisions in SMS, safety case, and test environment.
6.3.1.29.3.	The safety case shall demonstrate that appropriate sampling techniques to select the parameters for the logical and concrete scenarios have been used.		
6.3.1.30.	The manufacturer shall provide the following information as part of its safety case:		
	(a) Validation/verification plans including appropriate acceptance criteria,		
	(b) Analysis of coverage of the different tests and setting minimal ODD coverage thresholds for various metrics and includes ODD boundaries [reference to DDT Annex],		
	(c) Validation/verification results including evidence that the Validation targets (i.e., validation acceptance criteria) are met,		
	(d) Evidence that the scenarios tested provide reasonable coverage of the ODD,		
	(e) How it has applied the testing processes it has documented under sectionas per 6.2 of this rule in the context of the ADS covered by the safety case],		
	(f) An explanation of how the scenario selection process is reasonably designed to provide		

	reasonable coverage of the ODD and its boundaries, and		
	(g) Any comparisons drawn between the performance of an ADS feature and that of a manually driven vehicle reflect comparable vehicle categories (e.g. category M1 or category 1-1) and situations.		
6.3.1.31.	The manufacturer shall state how it has determined that the acceptance criteria it has used in its safety case is deemed to be sufficient, including:		
	(a) Identification of metrics used in evaluating the safety case,		
	(b) Justification of the chosen acceptance criteria for those metrics, and		
	(c) The scoring/evaluation of the evidence in generating metrics.		
6.3.2.	Claims, Arguments and Evidence of the Safety case		
6.3.2.1.	The safety case shall be composed of a series of claims for each of which there must be at least one supporting argument.		
6.3.2.1.1.	Each argument shall be supported by at least one piece of evidence.		
6.3.2.1.2.	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).		
6.3.2.2.	The safety case shall include claims, arguments and evidence that are understandable, logical, correct and robust and that demonstrate that:		
	(a) the ADS is free of unreasonable risk to ADS user(s) and other road users and		
	(b) the ADS meets applicable requirements of this regulation in each of following areas:		
	(i) DDT requirements (5.1)		
	(ii) User Interactions (5.2), except for the user information requirements of 5.2.5.		
	(iii) Other Requirements (5.3)		
6.3.2.3.	The manufacturer shall provide the following summary information with regards to its safety case:		
	(a) A summary identifying the relationships between claims and their supporting argument and evidence, and		
	(b) A summary identifying each regulatory requirement noted above and the claims that demonstrate the requirement is met.		
6.3.2.4.	The manufacturer shall demonstrate through the safety case that the	See China comment @ 6.3.1.7.	Sec: This seems to have the timing backwards. The approval of the SMS comes before approval of the

	application of the SMS is suitable for managing ADS safety throughout the lifecycle of the system in accordance with 6.1.			safety case. The outcomes of SMS application should be reflected in the safety case. In other words, an SMS process identifies and mitigates risks. These risks and mitigations are explained in the safety concept and the claim that the mitigations are effective is proven by the evidence.
6.3.2.5.	The manufacturer shall demonstrate through the safety case its ability to monitor the ADS over its lifetime in accordance with the requirement listed in 6.1.5.1-6.1.5.8	6.3.2.5.		
6.3.2.6.	The manufacturer shall state relevant assumptions it has made in relation to claims, arguments and evidence.			
6.3.2.7.	The manufacturer shall demonstrate that the credibility of the simulation toolchain in accordance with6.2 and that the credibility of physical testing used for the generation of evidence with regards to safety have been assessed.	6.3.2.7.	The manufacturer shall demonstrate that the credibility of the simulation toolchain in accordance with" X" [Credibility section] and that the suitability of physical testing used for the generation of evidence with regards to safety have been assessed.	China: Consistent with the description in 4.2.3.1 d). For physical testing, suitability may be more appropriate than credibility. (4.2.3.1 d) Demonstration of credibility and suitability of test tools used in generating evidence)
6.3.2.7.1.	The manufacturer shall demonstrate that the approach to testing is suitable for the demonstration of the safety case and the compliance with performance/functional requirements.			
6.3.2.8.	There shall be at least one claim for each goal or regulatory requirement.			
6.3.2.8.1.	The manufacturer may create multiple sub-claims for a claim, where a broader claim may not be sufficient or where additional justification is warranted as long as said sub-claims are sequenced			

	logically and their relationships are included in the summary documents.			
6.3.2.9.	Each argument supporting a claim shall provide contextual information and supporting information that explains how a claim is met based on an appropriate set of evidence.			
6.3.2.10.	Evidence supporting argumentation shall consist of test results or analysis (e.g. source code, engineering drawings, photographs, required documentation etc.) as appropriate.	China	Propose to delete: "source code", "engineering drawings" are know-how relevant, it's not appropriate to be indicated as examples in the regulation. "required documentation" is too broad, less value as an example.	
6.3.2.10.1.	Testing results may be provided individually or on aggregate and shall include appropriate acceptance criteria.			
6.3.2.10.2.	Each test shall include enough information or be recorded in such a way that it may be reproduced upon request (e.g. same software/hardware versions, same tool versions, same scenario, same parameters etc.).			
6.3.2.10.3.	The manufacturer shall facilitate access and execution of the necessary tools and analysis software upon request by the authority for the purpose of reproducing this evidence as part of the approval process or during compliance verification.			
6.3.2.11.	As part of the manufacturer’s demonstration of compliance to [6.1.6.8 b)], the manufacturer shall review its safety case prior to certification/approval and is			

	encouraged do so during the development process.		
6.3.2.11.1.	The reviewer(s) shall be independent, meaning that they are free from conditions that would threaten their ability to review the Safety Case without bias.		
6.3.2.11.2.	The reviewer(s) may be internal or external to the manufacturer.		
6.3.2.11.3.	The review shall be documented, available for inspection and include:		
	(a) Qualifications of the reviewer/ review team,		
	(b) Date/period of review, version of: the safety case, tools and ADS reviewed,		
	(c) Methods used to review the Safety Case,		
	(d) Listing of any evidence repeated/reproduced,		If the review shall include all these items, then this item must include “and”.
	(e) Identified gaps, questions or areas of lower confidence or unknowns		
6.3.2.11.4.	Following each review, and after a time of the manufacturer’s choice but before assessment of compliance, the manufacturer shall include in their review documentation the steps taken to remediate or improve upon any findings (e.g. release notes).		