Concordance of FRAV Stakeholder Input with the Proposed Discussion Topics in Document FRAV-08-09

This document supplements the FRAV leadership proposal for FRAV discussion topics regarding safety requirements for Automated Driving Systems. This document is based upon documents FRAV-03-07, FRAV-05-06, FRAV-06-04, FRAV-06-07, FRAV-06-10, FRAV-06-11, FRAV-07-08, FRAV-07-09, FRAV-08-06, and FRAV-08-07.

Proposed Topics	References
Overall Level of Safety The ADS performance should be consistent with human driving behaviors while avoiding human recognition, decision, and performance errors and the introduction of new risks.	9. The nominal operation of the ADS shall result in equal or safer performance than a human driver. i.e. achieve a neutral or positive risk balance.] 10. The overall safety target shall be at least as good as manual driving, i.e. P (accident with fatalities) < 10-8 /h and P (accident with light or severe injuries) <10-7/h. FRAV-07-08: • The nominal operation of the ADS shall result in equal or safer performance than a competent and careful human driver.
1. ADS should drive safely.	
1.1. The ADS should perform the entire Dynamic Driving Task.	J3016 8. When in automated driving mode, the automated vehicle drives and shall replace the driver for all the driving tasks for all the situations which can be reasonably expected in the ODD. 23. The ADS shall prioritize actions that will maintain the safe flow of traffic and prevent collisions with other road users and objects. 30. The system shall be able to detect indications of object intent (e.g., turn signal, acceleration, location in lane, body position, eye glaze) 36. The system sensors shall be capable of detecting objects within the lane in front of the vehicle up to at least the minimal braking distance required for the vehicle to come to a full stop 42. The automated driving system shall execute longitudinal and lateral maneuvers in response to objects and events within its operational design domain without causing damage, injury, or death where preventable.

1.1.1. The ADS should control the longitudinal and lateral motion of the vehicle.	J3016 36. The system sensors shall be capable of detecting objects within the lane in front of the vehicle up to at least the minimal braking distance required for the vehicle to come to a full stop 37. The system shall not allow a lane change unless the rear sensors are capable of detecting objects to the immediate sides and in both rear adjacent lanes at a distance that would allow the maneuver without requiring hard braking of an oncoming vehicle 42. The automated driving system shall execute longitudinal and lateral maneuvers in response to objects and events within its operational design domain without causing damage, injury, or death where preventable. 43. The vehicle shall be able to keep a safe distance with other vehicles in front. 45. The vehicle shall leave time and space for others in lateral maneuvers
1.1.2. The ADS should recognize the ODD conditions and boundaries of the ODD of its feature(s).	J3016 2. The vehicle shall demonstrate adequate mitigation of risks (e.g. approaching ODD boundaries) 24. The system shall be able to detect the roadway 25. The system shall be able to identify lane location with and without lane markings 26. The system shall be able to detect and identify lane markings 27. The system shall be able to detect objects in its defined field of view 28. The system shall be able to estimate the speed and heading of objects 29. The system shall be able to recognize and respond to traffic control devices, traffic signs and infrastructure including the state of traffic control devices 39. The ADS must be capable of identifying when conditions defining the ODD are met and predicting when they will no longer be met. 40. The automated driving system shall detect and respond to conditions within its operating environment that indicate the approach of boundaries of its operational design domain 41. The automated driving system shall detect and respond to its ODD boundary conditions before exiting the ODD 50. The automated driving system shall execute a safe fallback response when the conditions defined for its operational design domain are not present.

	53. The vehicle manufacturer shall define the operational design condition under which the automated driving system is designed to be activated, operated and deactivated 132. The system shall anticipate a function crossing the ODD boundaries and seek to remain within the function's ODD limits

1.1.3. The ADS should detect, recognize, classify, and prepare to respond to objects and events in the traffic environment.	30. The system shall be able to detect indications of object intent (e.g., turn signal, acceleration, location in lane, body position, eye gaze) 31. The system shall be able to predict the behavior of detected objects and take appropriate action to reduce the risk of collisions 33. The system shall be able to recognize and react to service providers with responsibilities to direct traffic (e.g., police, construction worker) 35. The system shall detect and respond appropriately to emergency service vehicles (e.g., yielding the right of way at intersections) 36. The system sensors shall be capable of detecting objects within the lane in front of the vehicle up to at least the minimal braking distance required for the vehicle to come to a full stop 38. The automated driving system shall detect conditions within its operating environment that fall outside the boundaries of its operational design domain. 49. When in the automated driving mode, the vehicle shall allow an appropriate interaction with other road users (e.g. obey to orders by authorities or communication with other road users when needed). 108. The vehicle shall automatically initiate a fallback response or fallback response sequence in response to detection of conditions outside its operational design domain 110. Upon crossing the function ODD limits, the system shall take action to minimize risks (e.g., re-enter function ODD limits, revert to minimal risk condition, transition to driver, emergency manoeuvre) and notify the occupants the ODD boundary has been crossed 111. The system shall not cross and re-enter function ODD limits cyclically and shall seek other actions to minimize risks if this occurs

1.2. The ADS should respect traffic rules.	18. The Automated Driving System (ADS) shall have predictable behavior 19. The System shall behave in a way that maintains the safe flow of traffic and is predictable to other road users and "comfortable" to occupants (following distance, lane centering, gradual acceleration/braking/steering, proper signaling) 20. The vehicle shall comply with all applicable road traffic laws except in cases where compliance would conflict with safety 21. The System must comply with the traffic rules but may temporarily bend these rules (during an emergency, uncommon or edge case situation), if such actions reduce safety risks or are required for the safe flow of traffic (e.g., crossing a double centre line to go around an obstacle) 22. The ADS shall drive in accordance with the traffic rules. 35. The system shall detect and respond appropriately to emergency service vehicles (e.g., yielding the right of way at intersections) 43. The vehicle shall be able to keep a safe distance with other vehicles in front. 46. The vehicle shall be cautious with right-of-ways 48. When in the automated driving mode, the vehicle shall, as far as possible, have a predictable and careful behaviour 49. When in the automated driving mode, the vehicle shall allow an appropriate interaction with other road users (e.g. obey to orders by authorities or communication with other road users when needed).

1.3. The ADS should interact safely with other road users.	19. The System shall behave in a way that maintains the safe flow of traffic and is predictable to other road users and "comfortable" to occupants (following distance, lane centering, gradual acceleration/braking/steering, proper signaling) 35. The system shall detect and respond appropriately to emergency service vehicles (e.g., yielding the right of way at intersections) 49. When in the automated driving mode, the vehicle shall allow an appropriate interaction with other road users (e.g. obey to orders by authorities or communication with other road users when needed). 72. The vehicle shall also be designed to minimize potential effects of errors from the vehicles' users, inside and outside of the vehicle, and of other road users. 74. The ADS shall communicate critical messages to vehicle's users and other road users when needed. 95. The vehicle shall signal to other road users 96. Intentions to undertake dynamic driving tasks 97. The system shall clearly communicate its intentions to pedestrians, cyclists and other road users (e.g., turn signals, speed change, high beam flash, other external communication 98. When needed, communication with other road users shall provide sufficient information about the vehicle's status and intention. 99. The system shall communicate the initiation of a minimal risk maneuver FRAV-06-11: • The ADS shall react on other vehicles wrong behavior with the best collision avoidance/mitigation strategy possible using state of the art technology.

1.4. The ADS should adapt its behavior in line with safety risks.	1. The Automated Driving System (ADS) shall react to unforeseen situations in a way that minimizes risk. 3. The vehicle shall demonstrate safe driving behavior 5. The system shall minimize the risks to vulnerable road users (VRU) in the case of an imminent collision (e.g., hit vehicle instead of VRU) 14. The system shall adapt to the driving conditions (reduce speed on wet/snowy/icy/gravel roads or due to visibility factors, road geometry) 15. The system shall anticipate possible collisions and act in a manner to reduce their possibility of occurrence 19. The System shall behave in a way that maintains the safe flow of traffic and is predictable to other road users and "comfortable" to occupants (following distance, lane centering, gradual acceleration/braking/steering, proper signaling) 23. The ADS shall prioritize actions that will maintain the safe flow of traffic and prevent collisions with other road users and objects. 31. The system shall be able to predict the behavior of detected objects and take appropriate action to reduce the risk of collisions 32. The system shall treat objects which cannot be classified with increased uncertainty 34. The system shall take into consideration that other road users may not respect traffic laws 38. The automated driving system shall detect conditions within its operating environment that fall outside the boundaries of its operational design domain. 42. The automated driving system shall execute longitudinal and lateral maneuvers in response to objects and events within its operational design domain without causing damage, injury, or death where preventable. 44. The vehicle shall exhibit caution in occluded areas 45. The vehicle shall leave time and space for others in lateral maneuvers 46. The vehicle shall be cautious with right-of-ways 48. When in the automated driving mode, the vehicle shall, as far as possible, have a predictable and careful behaviour 49. When in the automated driving mode, the vehicle shall allow an appropriate interaction with other road users (e.g. obey to orders by authorities or communication with other road users when needed).

1.5. The ADS behavior should not be the critical factor in the cause of a collision.	National Motor Vehicle Crash Causation Survey, NHTSA, DOT HS 811 059, July 2008 6. The vehicle in automated mode shall not cause any traffic collision that are rationally [reasonably] foreseeable and preventable. 7. Any avoidable accident shall be avoided. 13. The vehicle shall respond to reasonably foreseeable conditions within its operating environment without causing an event resulting in [destruction of property,] injury or death 15. The system shall anticipate possible collisions and act in a manner to reduce their possibility of occurrence 16. The Automated Driving System (ADS) shall not cause any traffic accidents that are reasonably foreseeable and preventable. 23. The ADS shall prioritize actions that will maintain the safe flow of traffic and prevent collisions with other road users and objects. 31. The system shall be able to predict the behavior of detected objects and take appropriate action to reduce the risk of collisions 36. The system sensors shall be capable of detecting objects within the lane in front of the vehicle up to at least the minimal braking distance required for the vehicle to come to a full stop 37. The system shall not allow a lane change unless the rear sensors are capable of detecting objects to the immediate sides and in both rear adjacent lanes at a distance that would allow the maneuver without requiring hard braking of an oncoming vehicle 42. The automated driving system shall execute longitudinal and lateral maneuvers in response to objects and events within its operational design domain without causing damage, injury, or death where preventable. 43. The vehicle shall be able to keep a safe distance with other vehicles in front. 47. If a traffic collision can be safely avoided without causing another it shall be avoided 48. When in the automated driving mode, the vehicle shall, as far as possible, have a predictable and careful behaviour FRAV-06-11: • The ADS shall not cause a collision due to its own driving behavior. • The ADS should prevent collisions with other road users and objects.
1.5. The ADS should adapt its behavior to the	17. The vehicle shall not disrupt the normal flow of traffic 18. The Automated Driving System (ADS) shall have predictable behavior

surrounding traffic conditions.	19. The System shall behave in a way that maintains the safe flow of traffic and is predictable to other road users and "comfortable" to occupants (following distance, lane centering, gradual acceleration/braking/steering, proper signaling) 23. The ADS shall prioritize actions that will maintain the safe flow of traffic and prevent collisions with other road users and objects. 31. The system shall be able to predict the behavior of detected objects and take appropriate action to reduce the risk of collisions 35. The system shall detect and respond appropriately to emergency service vehicles (e.g., yielding the right of way at intersections) 43. The vehicle shall be able to keep a safe distance with other vehicles in front. 46. The vehicle shall be cautious with right-of-ways 48. When in the automated driving mode, the vehicle shall, as far as possible, have a predictable and careful behaviour 72. The vehicle shall also be designed to minimize potential effects of errors from the vehicles' users, inside and outside of the vehicle, and of other road users.

1.6. The ADS behavior should not be the critical factor in the cause of a collision.	National Motor Vehicle Crash Causation Survey, NHTSA, DOT HS 811 059, July 2008 6. The vehicle in automated mode shall not cause any traffic collision that are rationally [reasonably] foreseeable and preventable. 7. Any avoidable accident shall be avoided. 13. The vehicle shall respond to reasonably foreseeable conditions within its operating environment without causing an event resulting in [destruction of property,] injury or death 15. The system shall anticipate possible collisions and act in a manner to reduce their possibility of occurrence 16. The Automated Driving System (ADS) shall not cause any traffic accidents that are reasonably foreseeable and preventable. 23. The ADS shall prioritize actions that will maintain the safe flow of traffic and prevent collisions with other road users and objects. 31. The system shall be able to predict the behavior of detected objects and take appropriate action to reduce the risk of collisions 36. The system sensors shall be capable of detecting objects within the lane in front of the vehicle up to at least the minimal braking distance required for the vehicle to come to a full stop 37. The system shall not allow a lane change unless the rear sensors are capable of detecting objects to the immediate sides and in both rear adjacent lanes at a distance that would allow the maneuver without requiring hard braking of an oncoming vehicle 42. The automated driving system shall execute longitudinal and lateral maneuvers in response to objects and events within its operational design domain without causing damage, injury, or death where preventable. 43. The vehicle shall be able to keep a safe distance with other vehicles in front. 47. If a traffic collision can be safely avoided without causing another it shall be avoided 48. When in the automated driving mode, the vehicle shall, as far as possible, have a predictable and careful behaviour

2. ADS should interact safely with the driver.	
General principles	4. The vehicle shall demonstrate good Human Machine Interface 69. The system shall have intuitive user controls and communications systems.
2.1. Activation of an ADS feature should only be possible when the conditions of its ODD have been met.	11. Activation and use of the vehicle in automated mode shall only be possible within the boundaries of the automated driving system's operational design domain. 39. The ADS must be capable of identifying when conditions defining the ODD are met and predicting when they will no longer be met. 52. The activation of the ADS shall only be possible when the conditions of the ODD are met.
2.2. The ADS should signal when conditions indicate a probable ODD exit.	40. The automated driving system shall detect and respond to conditions within its operating environment that indicate the approach of boundaries of its operational design domain 41. The automated driving system shall detect and respond to its ODD boundary conditions before exiting the ODD
2.3. The user should be permitted to override the ADS to assume full control over the vehicle.	54. When the driver takes over control on his own (manual deactivation/override), the system shall not disturb the driver take over by inappropriate action (e.g. by switching off light by night). 55. Means shall be provided to humans (driver or if no driver, passenger or operation control center) to deactivate or override immediately the automated mode in an easy manner (deliberate action). 56. The system may momentarily delay deactivation (and may include a driver take over request if there is a driver) when an immediate human deactivation could compromise safety. 57. Means shall be provided to the user to deactivate or override the ADS in an easy manner. 62. Demonstration of driver availability (awareness, readiness and engagement) and override feature 116. The system may request the driver to take over with a sufficient lead time in particular when the driver overrides the system

2.4.	The ADS should safely manage transitions of full control to the user.	50. The automated driving system shall execute a safe fallback response when the conditions defined for its operational design domain are not present.
		54. When the driver takes over control on his own (manual deactivation/override), the system shall not disturb the driver take over by inappropriate action (e.g. by switching off light by night).
		56. The system may momentarily delay deactivation (and may include a driver take over request if there is a driver) when an immediate human deactivation could compromise safety.
		89. The system shall clearly communicate the need, and provide the driver sufficient time for take-over requests
		100. Non-driving activities allowed in the AD mode shall be consistent with the available delay for the driver to takeover after a system request.
		114. The system shall be capable of transferring control back to the user in a safe manner.
		116. The system may request the driver to take over with a sufficient lead time in particular when the driver overrides the system
		117. The system may request the driver to take over with a sufficient lead time in particular when the system determines that it is difficult to continue automated driving mode, such as when the situation becomes outside the OD, or when a problem has occurred to the automated vehicle.
		118. The system shall give sufficient lead time to the driver to take over and shall remain in the automated driving mode as long as the driver has not taken over, and/or will otherwise transfer to a minimum risk manoeuvre.
		120. The system shall be designed to enable the driver to clearly recognize the takeover request from the system.
		122. When the driver takes over after a system request, the system shall give back control to the driver with a vehicle configuration maximizing driver controllability (e.g. wipers ON in case of rain, headlamps ON by night).
		125. Fallback strategies shall take into account that users may be inattentive, drowsy, or otherwise impaired, and shall therefore be implemented in a manner that will facilitate safe operation and minimize erratic driving behaviour.
		(FRAV-06-10 Netherlands)
		• Design with mental model in mind
		• Harmonized HMI for ADS
		  ○ Transparent
		  ○ Support (monitor) correct level of engagement
		  ○ Simplicity
		  ○ Salient
		• Harmonized states for transition of control
		  ○ Also for multiple features
		• Driver engagement is gradual (not binary)
		• Advice for harmonized driver training to WP1/IGEAD

2.4.1. Prior to a transition of control to the user, the ADS should verify the availability of the user to assume control.	61. Vehicles equipped with automated driving systems that may require driver intervention (e.g., transition demand) shall detect if the driver is available to take over the driving task by continuously monitoring the driver. 62. Demonstration of driver availability (awareness, readiness and engagement) and override feature 63. If the system shall monitor the take-over-ready driver, in the case of a level 3 system, the driver must remain available for system operation. 64. In the case of a level 4+ system, a take-over request shall not be issued to a driver who is unavailable. 65. If the system is designed to request the driver to take over under some circumstances, the system shall monitor whether the driver is ready to take over driving from the system. 66. The system shall ensure through appropriate design (e.g. driver monitoring system) and warnings that the driver remains available to respond to take over request and prevent any foreseeable and preventable misuse by the driver in the OD. 67. When the ADS is active it shall be capable of determining the user's status. 68. If the system is designed to request and enable the user to take over control under some circumstances, the ADS shall ensure through appropriate design and warnings that the user remains available to respond to the takeover request. 85. The system shall clearly communicate take-over requests to the driver/occupants. 88. Communication of Take-over request to the driver. 89. The system shall clearly communicate the need, and provide the driver sufficient time for take-over requests 91. Status of driver availability 92. Driver availability and override possibility (if required, based on level of automation) 93. AV should include driver engagement monitoring in cases where drivers could be involved (e.g. take over requests) in the driving task to assess driver awareness and readiness to perform the full driving task 125. Fallback strategies shall take into account that users may be inattentive, drowsy, or otherwise impaired, and shall therefore be implemented in a manner that will facilitate safe operation and minimize erratic driving behaviour.
2.4.2. Pursuant to a transition, the ADS should verify full control of the vehicle by the user prior to deactivation.	60. The ADS deactivation shall only be performed when it has been verified that the user has taken over control. 102. If applicable, activities other than driving that are provided by the ADS to the user once the ADS is activated shall be automatically suspended as soon as the ADS issues a transition demand or is deactivated. 115. The system shall be able to determine whether or not the user has taken over. 118. The system shall give sufficient lead time to the driver to take over and shall remain in the automated driving mode as long as the driver has not taken over, and/or will otherwise transfer to a minimum risk manoeuvre. 119. The ADS shall remain active as long as the vehicle's user has not taken over, or the ADS has reached a Minimal Risk Condition (MRC). 121. The system shall be able to determine whether or not the driver has taken over. This verification shall at least include a criterion on vehicle lateral control by the driver unless the vehicle is already stopped.

2.5.	The ADS should tolerate user input errors.	58. The ADS may momentarily delay deactivation if safety is compromised by the immediate input of the user. 59. When necessary the ADS shall protect the vehicle control against inadvertent or undeliberate [unintentional] user intervention. 66. The system shall ensure through appropriate design (e.g. driver monitoring system) and warnings that the driver remains available to respond to take over request and prevent any foreseeable and preventable misuse by the driver in the OD. 72. The vehicle shall also be designed to minimize potential effects of errors from the vehicles' users, inside and outside of the vehicle, and of other road users.

2.6.	The ADS should provide feedback to the user on its operational status.	66. The system shall ensure through appropriate design (e.g. driver monitoring system) and warnings that the driver remains available to respond to take over request and prevent any foreseeable and preventable misuse by the driver in the OD. 68. If the system is designed to request and enable the user to take over control under some circumstances, the ADS shall ensure through appropriate design and warnings that the user remains available to respond to the takeover request. 70. If the vehicle has multiple systems with varying degrees of driver interaction, distinct symbols and activation methods shall be used to avoid mode confusion 71. The mode concept shall be designed in a way that minimizes mode confusion at the user and system level. 74. The ADS shall communicate critical messages to vehicle's users and other road users when needed. 75. Status of the automated driving system 76. Communication of the system status to the driver 77. The system HMI will clearly indicate if the system is active, available or disabled 78. The ADS shall clearly inform user about the operational status (operational, failure, etc.) in an unambiguous manner. 79. The ADS shall communicate the system availability status 80. Communication of malfunctions to the driver 81. The system shall clearly communicate degraded operation, malfunctions, failures to the driver/occupants. 82. The system shall clearly communicate required system maintenance to the driver/occupants. 83. The system shall clearly communicate emergency conditions to the driver/occupants. 84. The system shall clearly communicate ongoing minimal risk manoeuvres to the driver/occupants. 85. The system shall clearly communicate take-over requests to the driver/occupants. 87. Communication of critical messages to the driver 88. Communication of Take-over request to the driver. 89. The system shall clearly communicate the need, and provide the driver sufficient time for take-over requests 91. Status of driver availability 92. Driver availability and override possibility (if required, based on level of automation) 99. The system shall communicate the initiation of a minimal risk maneuver 110. Upon crossing the function ODD limits, the system shall take action to minimize risks (e.g., re-enter function ODD limits, revert to minimal risk condition, transition to driver, emergency manoeuvre) and notify the occupants the ODD boundary has been crossed 120. The system shall be designed to enable the driver to clearly recognize the takeover request from the system. (FRAV-06-10 Netherlands) • Design with mental model in mind

	• Harmonized HMI for ADS

2.7.	The ADS should warn the user of failures to fulfill user roles and responsibilities.	66. The system shall ensure through appropriate design (e.g. driver monitoring system) and warnings that the driver remains available to respond to take over request and prevent any foreseeable and preventable misuse by the driver in the OD. 68. If the system is designed to request and enable the user to take over control under some circumstances, the ADS shall ensure through appropriate design and warnings that the user remains available to respond to the takeover request. 70. If the vehicle has multiple systems with varying degrees of driver interaction, distinct symbols and activation methods shall be used to avoid mode confusion 71. The mode concept shall be designed in a way that minimizes mode confusion at the user and system level. 73. Information shall be available to the vehicle's user that clearly defines their responsibilities, the procedures to comply with a takeover requests, and possible consequences if they do not comply. 101. The driver shall be made aware of the use and the limits of the automated driving mode, as well as which tasks other than driving may be enabled by the system for the driver (This is only about the technical capability of the system and without prejudice to national traffic rules).
2.8.	The user should be provided with information regarding user roles and responsibilities for the safe use of the ADS.	73. Information shall be available to the vehicle's user that clearly defines their responsibilities, the procedures to comply with a takeover requests, and possible consequences if they do not comply. 101. The driver shall be made aware of the use and the limits of the automated driving mode, as well as which tasks other than driving may be enabled by the system for the driver (This is only about the technical capability of the system and without prejudice to national traffic rules).

3. ADS should manage safety-critical situations.	
3.1. The ADS should recognize and respond to road safety agents.	49. When in the automated driving mode, the vehicle shall allow an appropriate interaction with other road users (e.g. obey to orders by authorities or communication with other road users when needed). 35. The system shall detect and respond appropriately to emergency service vehicles (e.g., yielding the right of way at intersections) 94. The system shall communicate with occupants, authorities, owners, operators or first responders after an abnormality/fault is detected, after a collision or after otherwise manoeuvred to a minimal risk condition.
3.2. The ADS should mitigate the effects of road hazards.	17. The vehicle shall not disrupt the normal flow of traffic 72. The vehicle shall also be designed to minimize potential effects of errors from the vehicles' users, inside and outside of the vehicle, and of other road users. 51. The automated driving system shall execute an emergency response when conditions for the execution of a safe fallback response are not present. 133. The system shall be able to execute emergency manoeuvres in an attempt to avoid imminent hazards FRAV-06-11: • The ADS shall react on other vehicles wrong behavior with the best collision avoidance/mitigation strategy possible using state of the art technology.

3.3. The ADS should execute a Minimal Risk Maneuver (MRM) as conditions warrant.	50. The automated driving system shall execute a safe fallback response when the conditions defined for its operational design domain are not present. 51. The automated driving system shall execute an emergency response when conditions for the execution of a safe fallback response are not present. 105. The ADS shall be equipped with appropriate technical measures that continuously monitor system performance, perform fault detection and hazard analysis, signal any detected malfunctions that affect the system performance, and ultimately take corrective actions or revert to a minimal risk condition when needed. 113. The system shall take appropriate measures when a system abnormality/fault is detected in order to reduce risk (degraded mode, limp mode, revert to minimal risk condition etc.) 123. When the system detects that it is difficult to continue in the automated driving mode, it shall be able to transfer to a minimal risk condition (with or without take over request) through a minimal risk manoeuvre. 126. The system shall be able to, at minimum, bring the vehicle to a gradual stop if the driver has not taken over the driving task after the provided take-over time. 127. A minimum risk manoeuvre shall be performed in case of shock in the best possible way, according to vehicle operational status and current situation. 129. The minimum risk manoeuvre shall lead to a vehicle stop. 128. During the whole MRM, the driver can take over in usual way. 130. The Minimum Risk Manoeuvre (MRM) shall comply with traffic rules. MRM settings for automated vehicles may include measures to stay in or change the lane while warning to the surrounding and automatically stop the vehicle in a safe manner on the side of the road.
3.3.1. In the absence of a fallback-ready user, the ADS should fall back directly to an MRM.	64. In the case of a level 4+ system, a take-over request shall not be issued to a driver who is unavailable. 105. The ADS shall be equipped with appropriate technical measures that continuously monitor system performance, perform fault detection and hazard analysis, signal any detected malfunctions that affect the system performance, and ultimately take corrective actions or revert to a minimal risk condition when needed. 124. The Minimal Risk Manoeuvre (MRM) shall be capable of achieving an MRC when a given trip cannot or should not be completed for example in case of a failure in the ADS or other vehicle systems.

3.4.2. The ADS should execute an MRM in the event of a failure in the transition of full control to the user.	125. Fallback strategies shall take into account that users may be inattentive, drowsy, or otherwise impaired, and shall therefore be implemented in a manner that will facilitate safe operation and minimize erratic driving behaviour.
3.4.3 *Pursuant to an MRM, the ADS should place the vehicle in a Minimal Risk Condition prior to deactivation.*	109. Fallback responses shall only be initiated when conditions permit their completion. 112. The system shall have appropriate redundancies that allow it to, at minimum, execute an emergency stop in the case of any system failure or emergency 119. The ADS shall remain active as long as the vehicle's user has not taken over, or the ADS has reached a Minimal Risk Condition (MRC). 131. The driver may be asked to take over at the end of the minimum risk manoeuvre (e.g. to park on the side of the road in case of level 3 lane keeping system). If the driver does not respond to the takeover request, the vehicle shall be stopped in parking mode and the AD mode shall be deactivated.
3.5. The ADS should signal an MRM.	83. The system shall clearly communicate emergency conditions to the driver/occupants. 84. The system shall clearly communicate ongoing minimal risk manoeuvres to the driver/occupants. 90. Recognition of MRM in operation by the driver 94. The system shall communicate with occupants, authorities, owners, operators or first responders after an abnormality/fault is detected, after a collision or after otherwise manoeuvred to a minimal risk condition. 99. The system shall communicate the initiation of a minimal risk maneuver 135. The system shall inform the occupants and contact emergency service providers, owners and/or operators
3.6. ADS vehicles that may operate without a user-in-charge should provide means for occupant communication with a remote operator.	103. For vehicles designed to operate only with no driver (e.g. driverless shuttles), a communication function shall be provided to send an emergency notification to an operation control centre. A camera and voice communication device shall be provided in the vehicle so that an operation control centre can monitor the situation inside the vehicle. 104. For ADS designed to operate with no driver present in the vehicle e.g. driverless shuttles, an audio and visual communication channel shall be provided to exchange emergency notifications.
3.7. The ADS should safely manage short-duration transitions between ODD.	110. Upon crossing the function ODD limits, the system shall take action to minimize risks (e.g., re-enter function ODD limits, revert to minimal risk condition, transition to driver, emergency manoeuvre) and notify the occupants the ODD boundary has been crossed

	111. The system shall not cross and re-enter function ODD limits cyclically and shall seek other actions to minimize risks if this occurs
3.8. Upon completion of an MRM, the user may be permitted to assume control of the vehicle.	131. The driver may be asked to take over at the end of the minimum risk manoeuvre (e.g. to park on the side of the road in case of level 3 lane keeping system). If the driver does not respond to the takeover request, the vehicle shall be stopped in parking mode and the AD mode shall be deactivated.
3.9. Pursuant to a collision, the ADS should stop the vehicle and deactivate.	134. Following a collision, the vehicle shall be brought to a complete stop to the best capabilities of the system and shall be brought to a minimal-risk state 136. Prior to re-activation, the system shall conduct self-diagnostics to ensure it is capable of operation 137. Upon direction by emergency personnel or authorised user, the system, if able, shall move off the roadway 138. After detection of a first significant shock while driving (e.g. frontal collision with airbags triggering or lateral collision during an insertion), the vehicle shall inhibit AD mode reactivation until proper operation has been verified 139. After detection of a first significant shock while driving (e.g. frontal collision with airbags triggering or lateral collision during an insertion), the vehicle shall immediately attempt to achieve a safe state in the best possible way, according to vehicle operational status and current situation 140. Post-crash, the ADS may also request the user to takeover vehicle control if vehicle and current situation are sufficiently controllable.

4. ADS should safely manage failure modes.	
4.1. The ADS should detect system malfunctions and abnormalities.	86. The system shall be equipped with a monitoring system that can detect: faults, malfunctions or other abnormalities of system components and monitor system performance. 105. The ADS shall be equipped with appropriate technical measures that continuously monitor system performance, perform fault detection and hazard analysis, signal any detected malfunctions that affect the system performance, and ultimately take corrective actions or revert to a minimal risk condition when needed. 113. The system shall take appropriate measures when a system abnormality/fault is detected in order to reduce risk (degraded mode, limp mode, revert to minimal risk condition etc.)
4.2. The ADS should execute a safe fallback response upon detection of a failure that prevents performance of a portion of the DDT.	J3016 (an ADS is no longer an ADS if it cannot perform the entire DDT). 106. The ADS should be designed, to the extent practicable, to function predictably, controllably, and safely in the presence of faults and failures affecting the system performance. 107. In case of failure impacting the safety of the ADS, an appropriate control strategy shall be in place as long as the failure exists. 112. The system shall have appropriate redundancies that allow it to, at minimum, execute an emergency stop in the case of any system failure or emergency 113. The system shall take appropriate measures when a system abnormality/fault is detected in order to reduce risk (degraded mode, limp mode, revert to minimal risk condition etc.) 117. The system may request the driver to take over with a sufficient lead time in particular when the system determines that it is difficult to continue automated driving mode, such as when the situation becomes outside the OD, or when a problem has occurred to the automated vehicle.

4.3. Provided a failure does not compromise ADS performance of the entire DDT, the ADS should respond safely to the presence of a fault in the system.	106. The ADS should be designed, to the extent practicable, to function predictably, controllably, and safely in the presence of faults and failures affecting the system performance. 107. In case of failure impacting the safety of the ADS, an appropriate control strategy shall be in place as long as the failure exists. 113. The system shall take appropriate measures when a system abnormality/fault is detected in order to reduce risk (degraded mode, limp mode, revert to minimal risk condition etc.)
4.4. The ADS should signal faults and resulting operational status.	78. The ADS shall clearly inform user about the operational status (operational, failure, etc.) in an unambiguous manner. 80. Communication of malfunctions to the driver 81. The system shall clearly communicate degraded operation, malfunctions, failures to the driver/occupants. 94. The system shall communicate with occupants, authorities, owners, operators or first responders after an abnormality/fault is detected, after a collision or after otherwise manoeuvred to a minimal risk condition.

5. ADS should ensure a safe operational state.	
5.1. The ADS should be permanently disabled in the event of obsolescence.	12. If an update renders the system obsolete or otherwise no longer supported, it shall not permit activation
5.2. Pursuant to a collision and/or a failure detected in DDT-related functions, ADS activation should not be possible until the safe operational state of the ADS has been verified.	136. Prior to re-activation, the system shall conduct self-diagnostics to ensure it is capable of operation 138. After detection of a first significant shock while driving (e.g. frontal collision with airbags triggering or lateral collision during an insertion), the vehicle shall inhibit AD mode reactivation until proper operation has been verified
5.3. The ADS should signal required system maintenance to the user.	82. The system shall clearly communicate required system maintenance to the driver/occupants. 141. Any safety related failures regarding the roadworthiness of the ADS shall be systematically reported to the vehicle user.
5.4. The ADS should be accessible for the purposes of maintenance and repair to authorized persons.	142. The system Software and Hardware versions shall be accessible