Submitted by the experts from Canada

Document FRAV-02-08 (p1/4 pages)
2nd FRAV session, 14-15 January 2020
Agenda item 6.4.

Based on FRAV-01-13-Rev1, FRAV-01-07 and FRAV-01-09

Some requirements apply to different levels of system sophistication.

SAFETY ELEMENTS	INDUSTRY UNDERSTANDING OF REQUIREMENTS	POSSIBLE FUNCTIONAL REQUIREMENTS BASED ON CANADA SAFETY ASSESSMENT (FRAV-01-07) AND FRAV-01-09
SYSTEM SAFETY	1. Ensuring compliance with road traffic regulations. 2. Document about the road rules in scope of the application.	1. 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) 2. 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) 3. The system shall adapt to the driving conditions (reduce speed on wet/snowy/icy/gravel roads or due to visibility factors, road geometry) 4. The system shall anticipate possible collisions and act in a manner to reduce their possibility of occurrence 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) 6. If an update renders the system obsolete or otherwise no longer supported, it shall not permit activation
FAILSAFE RESPONSE	1. Description of MRM strategy (documentation) and physical demonstration 2. Description of driving take over functionality	7. The system shall anticipate a function crossing the ODD boundaries and seek to remain within the function’s ODD limits 8. 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 9. The system shall not cross and re-enter function ODD limits cyclically and shall seek other actions to minimize risks if this occurs 10. 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

SAFETY ELEMENTS	INDUSTRY UNDERSTANDING OF REQUIREMENTS	POSSIBLE FUNCTIONAL REQUIREMENTS BASED ON CANADA SAFETY ASSESSMENT (FRAV-01-07) AND FRAV-01-09
		11. The system shall be equipped with a monitoring system that can detect: faults, malfunctions or other abnormalities of system components and monitor system performance 12. 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.) 13. 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
HUMAN MACHINE INTERFACE (HMI)/ OPERATOR INFORMATION	1. Communication of Take-over request to the driver. 2. Communication of the system status to the driver. 3. Communication of malfunctions to the driver. 4. Communication of critical messages to the driver. 5. Recognition of MRM in operation by the driver. 6. Demonstration of activation/deactivation of AV mode. 7. Demonstration of driver availability (awareness, readiness and engagement) and override feature. 8. Demonstration of signaling features. Interaction with other road users.	14. The system shall have intuitive user controls and communications systems 15. The system HMI will clearly indicate if the system is active, available or disabled 16. If the vehicle has multiple systems with varying degrees of driver interaction, distinct symbols and activation methods shall be used to avoid mode confusion 17. The system Software and Hardware versions shall be accessible 18. The system shall clearly communicate: degraded operation, malfunctions, failures, required system maintenance, emergency conditions, ongoing minimal risk manoeuvres or take-over requests to the driver/occupants. 19. The system shall clearly communicate the need, and provide the driver sufficient time for take-over requests 20. 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 21. The system shall be able to execute emergency manoeuvres in an attempt to avoid imminent hazards 22. 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. In the case of a level 4+ system, a take-over request shall not be issued to a driver who is unavailable. 23. The system shall clearly communicate its intention to pedestrians, cyclists and other road users (e.g., turn signals, speed change, high beam flash, other external communication)

SAFETY ELEMENTS	INDUSTRY UNDERSTANDING OF REQUIREMENTS	POSSIBLE FUNCTIONAL REQUIREMENTS BASED ON CANADA SAFETY ASSESSMENT (FRAV-01-07) AND FRAV-01-09
OBJECT EVENT DETECTION AND RESPONSE (OEDR)	1. Ability to detect object/events reasonably expected in the OD. 2. Ability to respond to object/events reasonably expected in the OD.	24. The system shall be able to detect the roadway 25. The system shall be able to identify lane location (w/, w/o 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 classify static and dynamic objects in its defined field of view which are foreseeable in the OD (at minimum, it must classify: light vehicles, heavy vehicles, pedestrians, cyclists, motorcyclist, emergency vehicles, animals, traffic control devices, traffic signs …) 30. The system shall be able to recognize and respond to traffic control devices, traffic signs and infrastructure including the state of traffic control devices 31. The system shall be able to detect indications of object intent (e.g., turn signal, acceleration, location in lane, body position, eye glaze) 32. The system shall be able to predict the behaviour of detected objects and take appropriate action to reduce the risk of collisions 33. The system shall treat objects which cannot be classified with increased uncertainty 34. 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 take into consideration that other road users may not respect traffic laws 36. The system shall detect and respond appropriately to emergency service vehicles (e.g., yielding the right of way at intersections) 37. 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 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 manoeuvre without requiring hard braking of an oncoming vehicle

SAFETY ELEMENTS	INDUSTRY UNDERSTANDING OF REQUIREMENTS	POSSIBLE FUNCTIONAL REQUIREMENTS BASED ON CANADA SAFETY ASSESSMENT (FRAV-01-07) AND FRAV-01-09
OPERATIONAL DESIGN DOMAIN (ODD)	1. Definition/documentation of OD for the specific application and verification of the OD recognition. Description of functionalities available within the OD.	39. The system shall have a clearly defined ODD for each function with at minimum consideration for variables such as weather, road type, speed 40. The system shall be able to detect its OD 41. The system shall not allow activation of a function if the OD is outside the function's ODD
POST-CRASH AV BEHAVIOUR	1. Communication with operations centre, collision notification centres or use of other communication technologies, when the infrastructure is available. 2. Ensure the AV achieve a minimal safe-state immediately after being involved in a crash (e.g. fuel pump off, disengage electrical power, removing motive power, …).	42. 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 43. The system shall inform the occupants and contact emergency service providers, owners and/or operators 44. Prior to re-activation, the system shall conduct self-diagnostics to ensure it is capable of operation 45. Upon direction by emergency personnel or authorised user, the system, if able, shall move off the roadway