Submitted by the expert from the European Commission

Document FRAV-02-06
2nd FRAV session, 14-15 January 2020
Agenda item 6.4.

The list of safety elements is preliminary and derived from a review of the guidelines and policies issued by Contracting Parties. The list is aligned with the principles of the revised UN Framework Document on Automated / Autonomous Vehicles

	Industry safety elements	Industry understanding of the FD requirements	Possible functional requirements based on EU guidelines and framework document text	Remarks
a.	**SYSTEM SAFETY**	**Demonstration that the AV should be free of unreasonable safety risks for the driver and other road users.**	**When in the automated mode, the automated/autonomous vehicle (AV) should be free of unreasonable safety risks to the driver and other road users and ensure compliance with road traffic regulations**	
	Dynamic behaviour in road traffic (The AV should be free of unreasonable safety risks to the driver and other road users)	Ensuring compliance with road traffic regulations.	1. When in the automated driving mode ("Operational Domain"-OD), 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 OD. 2. When in the automated driving mode, the vehicle shall not cause any traffic collision that are rationally foreseenable and preventable. Any avoidable accident shall be avoided, 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. 7 . 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. 8. The vehicle shall be able to keep a safe distance with other vehicles in front, exhibit caution in occluded areas, leave time and space for others in lateral maneuvers, be cautious with right-of-ways and if a traffic collision can be safely avoided without causing another it shall be avoided. 3. When in the automated driving mode, the vehicle shall, as far as possible, have a predictable and careful behaviour and shall allow an appropriate interaction with other road users (e.g. obey to orders by authorities or communication with other road users when needed).	
	Adherence to rules of the road (Federal and local laws) (The AV should ensure compliance with road traffic regulations)	Document about the road rules in scope of the application.	4. When in the automated driving mode ("Operational Domain"-OD), the automated vehicle shall drive in accordance with the traffic rules unless the only way to avoid an accident is to not respect the traffic rules(harm) or in presence of conflicting rules.	
b.	**FAILSAFE RESPONSE**	**Ability to detect when the conditions of the OD are not met anymore. Ability to transition automatically to a Minimal Risk condition upon failure detection.**	**The AV should be able to detect its failures or when the conditions for the [ODD/OD] are not met anymore. In such a case the vehicle should be able to transition automatically (minimum risk manoeuvre) to a minimal risk condition.**	
	Minimal Risk Manœuvre (In such a case the vehicle should be able to transition automatically (minimum risk manoeuvre) to a minimal risk condition.)	Description of MRM strategy (documentation) and physical demonstration	20. 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. 20a. A minimum risk manoeuvre shall be perfomed in case of shock in the best possible way, according to vehicle operational status and current situation. 20. The minimum risk manoeuvre shall lead to a vehicle stop. 22. 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.	
	Take over of DDT (if required, based on level of automation)	Description of driving take over functionality	22. 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 repond to the take over request, the vehicle shall be stopped in parking mode and the AD mode shall be desactivated.	Would fit better under HMI,Description of the take over procedure is covered under HMI section
	Understanding the system limits and boundaries (The AV should be able to detect its failures or when the conditions for the [ODD/OD] are not met anymore)	-	10. The system shall detect when it is difficult to continue in the automated driving mode, for instance when reaching the boundaries of the OD or in case of failure.	

c.	**Human Machine Interface (HMI) /Operator information**	**AV should include driver engagement monitoring in case where driver could be involved in the driving task to assess their awareness and readiness to perform full driving task. The vehicle should request the driver to hand over the driving tasks in case that the driver needs to resume control of the vehicle. Interaction with other road users.**	**The 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. The vehicle should request the driver to hand over the driving tasks in case that the driver needs to regain a proper control of the vehicle. In addition, automated vehicle should allow interaction with other road users (e.g. by means of external HMI on operational status of the vehicle, etc.)**	
	Take-Over request (The vehicle should request the driver to hand over the driving tasks in case that the driver needs to regain a proper control of the vehicle.)	Communication of Take-over request to the driver.	16. The system may request the driver to take over with a sufficient lead time in particular when -the driver overrides the system or -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. " 17.The system shall give sufficient leadtime 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. 18. The system shall be designed to enable the driver to clearly recognize the take over request from the system. 19. 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. 19a. 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). 19b. When the driver takes over after a system request, the system shall give back control to the driver with a vehicle confirguration maximizing driver controlability (e.g. wipers ON in case of rain, headlamps ON by night). 19c. Non-driving activities allowed in the AD mode shall be consistent with the available delay for the driver to takeover after a system request. 15. 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.	
	System Status	Communication of the system status to the driver.	12. The vehicle shall always inform the driver (or person responsible for operation) or passengers about the operational status (operational, failure, etc.) of the system in an unambiguous manner. In case of cohabitation on a single vehicle of several driving modes with different delegation levels, the enecssary measures shall be taken to control driver mode confusion risks. 14a. Non driving activities allowed in the AD mode and available through the vehicle system shall be available in the AD mode only and be interrupted with a specific HMI, when the vehicle request the driver to takeover or when the driver takes control on her/his own.	
	Malfunction	Communication of malfunctions to the driver.	covered by line 12	
	Communication of Critical Messages	Communication of critical messages to the driver.	covered by line 12	
	Minimum Risk Manoeuvre in operation	Recognition of MRM in operation by the driver.	status covered by line 12, decsirption of MRM in line 7	
	Automated mode active	Demonstration of activation/deactivation of AV mode.	11. The activation of the automated driving mode shall only be possible when the conditions of the OD are met. +line 12	
	Driver availability and override possibility (if required, based on level of automation) (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)	Demonstration of driver availability (awareness, readiness and engagement) and override feature.	13. 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 predjudice to national traffic rules). 14. 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. It 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. 11a. 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).The system may however momentarily delay deactivation (and may include a driver take over request if there is a driver) when an immediate human deactivation could compromise safety. 20b. During the whole MRM, the driver can take over in usual way. 15. 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.	Would propose to split between driver availibility and override
	Signalling driving intentions to other road users (In addition, automated vehicle should allow interaction with other road users (e.g. by means of external HMI on operational status of the vehicle, etc.)	Demonstration of signaling features. Interaction with other road users.	21. Other road users shall be informed that the vehicle is performing a minimum risk manoeuvre in accordance with applicable traffic rules (e.g. hazard lights, brake lights, turning indicators).	

d.	**OBJECT EVENT DETECTION AND RESPONSE (OEDR)**		**The AV shall be able to detect and respond to object/events that may be reasonably expected in the [ODD/OD]**	
	Response to scenarios and recognition of the OEDR (The AV shall be able to detect and respond to object/events that may be reasonably expected in the [ODD/OD])	Ability to detect object/events reasonably expected in the OD.	6. An automated driving system shall recognize whether or not the situation is within the set OD, and operate only in that OD.	Not clear why 2 different lines
	Scenario Recognition (Object and Event Detection) (The AV shall be able to detect object/events that may be reasonably expected in the [ODD/OD])	Ability to respond to object/events reasonably expected in the OD.	7. The system shall be safe by design to cope with any situation within the OD (environment perception capabilities, ability to take right decisions and perform the right dynamic driving tasks and allow interaction with other road users) without continuous supervision by the driver. 8. In particular, the vehicle shall be able to keep a safe distance with other vehicles in front, exibit caution in occluded areas, leave time and space for others in lateral maneuvers, be cautious with right-of-ways and if an accident can be safely avoided without causing another it shall be avoided.	
e.	**OPERATIONAL DESIGN DOMAIN (ODD)**		**For the assessment of the vehicle safety, the vehicle manufacturers should document the OD available on their vehicles and the functionality of the vehicle within the prescribed OD. The OD should describe the specific conditions under which the automated vehicle is intended to drive in the automated mode. The OD should include the following information at a minimum: roadway types; geographic area; speed range; environmental conditions (weather as well as day/night time); and other domain constraints.**	
	Operational Domain setting and recognition (roadway types, geographic area, speed range, environmental conditions, other domain constraints)	Definition/documentation of OD for the specific application and verification of the OD recognition. Description of functionalities available within the OD.	6. An automated driving system shall recognize whether or not the situation is within the set OD, and operate only in that OD. 5. The manufacturer shall declare to the type-approval authority the scope of the automated driving mode (so called operational domain(s) (OD)) where and when the automated driving system is designed to operate. This shall include at a minimum: · Road conditions (motorways/expressways, general roads, number of lanes, existence of lane marks, roads dedicated to automated driving vehicles, etc.) · Geographical area (urban and mountainous areas, Geofence setting, etc.) · Environmental conditions (weather, night-time limitations, etc.) · Speed range · Other conditions that must be fulfilled for the safe operation in the driving mode. 9. The OD shall be set in a way that it allows the driver to take over safely from the automated system (i.e. only take over requests in low risk situations) and in compliance with the relevant traffic rules. 11. The activation of the automated driving mode shall only be possible when the conditions of the OD are met.	

Submitted by the expert from the European Commission

Document FRAV-02-06
2nd FRAV session, 14-15 January 2020
Agenda item 6.4.

f. **VALIDATION FOR SYSTEM SAFETY**		**Vehicle manufacturers should demonstrate a robust design and validation process based on a systems-engineering approach with the goal of designing automated driving systems free of unreasonable safety risks and ensuring compliance with road traffic regulations and the principles listed in this document. Design and validation methods should include a hazard analysis and safety risk assessment for Automated Driving System (ADS), for the OEDR, but also for the overall vehicle design into which it is being integrated and when applicable, for the broader transportation ecosystem. Design and validation methods should demonstrate the behavioural competencies an Automated/autonomous vehicle would be expected to perform during a normal operation, the performance during crash avoidance situations and the performance of fall back strategies. Test approaches may include a combination of simulation, test track and on road testing.**
Design & Validation (best practices, design principles, standards)	Demonstration of a robust design and validation process based on system-engineering approach, including hazard analysis and safety risk assessment.	31. The Type-approval authority shall assess that the manufacturer has put in place a robust design and validation process of the automated system with the goal to ensure that the vehicle complies with these guidelines, particularly that it will not cause accidents and will provide safe take over requests and minimum risk manoeuvresThe type-approval authority shall make a finding of safety equivalence based on the manufacturer's safety evaluation report documenting testing, validation, and assessment (see Annex).
Risk Analysis & Mitigation (Failures, Inadequate Control)	Description of Risk Analisys and Failure modes mitigation functions.	32. The manufacturer shall in particular demonstrate that it has conducted a hazard and safety risk analysis for the automated system, its integration in the overall vehicle design and the broader transportation ecosystem and put in place adequate design and redundancy to cope with these risk and hazards (safety concept).
Performance in critical/complex situations (includes response to priority vehicles)	Ability to detect conditions outside the OD.	33. Systems shall in particular be designed to cope with risks that could impact safety critical functionality due to cyber-attacks and failure (functional safety) but also potential inadequate control, undesirable control actions, driver misuse and inadequate interaction with other road users (operational safety). Relevant demonstration methods include ISO 26262 for functional safety[3] and a system-theoretic process analysis (STPA)for operational safety or an equivalent method such as draft ISO PAS 21448.
Vehicle behaviour predictability	How the vehicle behave with respect the sorrounding environment and other vehicles / road traffic elements.	30. Automated vehicles, their systems, components and technical units shall comply to the largest extent with the existing EU Safety Regulations listed in Annex IV to Directive 2007/46/EC, unless they are incompatible with the purpose of the automated vehicles.
Testing Methods	Description of Testing methods for AV validation.	34. All design decisions shall be tested, validated and verified by the manufacturer as individual subsystem and as part of the entire vehicle architecture. 35. The type-approval authorities or the technical services acting on their behalf shall make a finding of safety equivalence based on the manufacturer's safety evaluation report documenting testing, validation, and assessment methods listed above. OEM shall set up a catalog of senarios, including misuse, to be used for safety argumentation during design and verification/validation process(for decision making scenarios). - The type-approval authorities shall verify that the hazard and safety risk analysis is designed to cover all types of system failures and driving hazards for the system concerned, and to assess their criticity. -They shall assess that the logical chart of responses to risk (e.g. redundancy, manoeuvers) covers the range of identified system failures and driving hazards. -They shall ensure that the human – machine interactions have been properly assessed, based on a relevant set of tests and users. -The manufacturer shall demonstrate with its internal validation process leads to an overall acceptable level or residual risk. It shall demonstrate that any accident avoidable by designed has been addressed. The 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. -They shall carry out a minimum number of tests to verify that the vehicle subject to the exemption operates safely from the functional and operational safety point of view considering on one hand the most critical failure and driving scenarios, and on the other hand, the carefulness and understandability of operation by other road users in non critical scenarios. They shall ensure that there is a transparent method of measuring the operational/run-time performance of the system. The minimum number of tests should include false negative and false positive test scenarios. Simulation method may be used, subject to their validation the approval authorities/technical services in accordance with the procedure for virtual testing in Directive 2007/46/EC or Regulation 858/2018. Field experience shall be taken into account to continuously improve safety. 36. The type-approval authorities or the technical services acting on their behalf shall have access to the system to carry out the vehicle safety assessment. 37. The type-approval authority or/and the technical services acting on its behalf shall have the necessary competences, certifications and training to carry out the vehicle safety assessment and tests listed above.

g.	**CYBER SECURITY**	**Protection against cyber-attacks in accordance with established best practices for cyber vehicle physical systems.**	**The AVe should be protected against cyber-attacks in accordance with established best practices for cyber vehicle physical systems. Vehicles manufacturers shall demonstrate how they incorporated vehicle cybersecurity considerations into ADSs, including all actions, changes, design choices, analyses and associated testing, and ensure that data is traceable within a robust document version control environment.**	
	Risk Analysis & Mitigation Strategies (Cyberattack events)	Demonstration of Cybersecurity considerations including actions, changes, design choices, analyses and associated testing.	28. The Vehicle shall be designed to protect the vehicle against automated vehicle hacking using state of the art techniques[2] and comply with EU data protection legislation. This includes risk assessment by the manufacturer, design measures and adequate processes to avoid, mitigate and react to cyber attacks. [2] See for instance the most recent requirements on cybersecurity by the UN (WP.29) or other organizations (SAE J3061 and ISO/SAE21434).	
	Incident Management	Demonstration of Cybersecurity considerations including actions, changes, design choices, analyses and associated testing.		
	Documentation Strategies/Changes/Testing	Ensure data traceability within a robust document version control environment.		
h.	**SOFTWARE UPDATES**			
	Software/System update process	Ensuring system updated occur as needed in a safe way and provided for after-market repairs and modifications.	29. Vehicle manufacturers shall take measures such as those related to updating of software, etc., installed in automated vehicles necessary to ensure in-use cybersecurity **and safety** over its lifetime.	Software updates for safety needs also to taken into account by FRAV
i.	**EVENT DATA RECORDER (EDR) and DATA STORAGE SYSTEM FOR AUTOMATED DRIVING VEHICLES (DSSAD)**	**Collection of necessary data related to the system status, occurrence of malfunctions, degradations or failures.**		
	Protocol/data elements	Typology and format of data to be collected.	26. The on-board device shall be able to store data in a secured manner, comply with EU data protection legislation and be protected against manipulation. It shall also allow the access by relevant national authorities. 27. More specific requirements for data recording devices (recording time, retention time, for what purposes data is used, standardized access, how to handle personal information, etc.) may be developed on the basis of the experience gained.	
	Access to Data	Access to the data collected to help establish the cause of a crash and the status of the ADS and the status of the driver, when required.	24. This data collected shall allow to assign liability in case of accident and shall allow to assess if the driver or the vehicle properly reacted to the situation. It shall at least include the operation status of the automated driving system, state of the driver, information on surrounding, control information of the vehicle.	
	Recording Interval/Recording capacity	Recording of necessary data collected.	23. Automated vehicles should be equipped with an on-board device that records the operational status of the automated driving system and the status of the driver to determine who was driving during an accident. 25. The on-board device shall be able to cope with a vehicle crash (similar to ecall e.g resistance to heavy accelearation and fire).	
j.	**VEHICLE MAINTENANCE AND INSPECTION**			
	Inspections/Repair/Modifications processes	Ensure safety of in-use vehicles.		In use safety is an important aspect to be considered by FRAV
	Maintenance of existing level of crashworthiness (for vehicles carrying occupants)	Encourage availability of documentation to facilitate the maintenance and repair of ADs after a crash, including equipment and processes identification to ensure safe operation after repair.		
	Vehicle state monitoring			
k.	**CONSUMER EDUCATION AND TRAINING**	**Training and development of employee, dealer, distributor and consumers.**		
	Training programmes			
	User (Driver/Passenger) information	Consumer Information, automated system manual.	38. Vehicle manufacturers shall inform automated vehicle users of the following points using easy-to-understand materials, etc., and take measures to make them understandable: · Operational conditions of the system, scope of OD, vehicle behaviour in the OD and functional limitations · Means to deactivate the automated driving mode · Driver’s tasks and responsibility (such as the need for the driver to take over driving when the system cannot continue driving for level 3 vehicles) · Possible action to take other than driving according to the performance of the system and its operation status (for level 3 vehicles) · Information related to indications by HMI (whether or not the automated driving system is operating, etc.) · User behaviour to adopted in case of urgency · Behaviours of the vehicle when a problem has occurred to the system · Need to conduct proper maintenance (inspection) and software update of in-use automated vehicles.	
	System Operational Domain/Limits			
	System Prescribed Use			
l.	**CRASHWORTHINESS AND COMPATIBILITY**			
m.	**POST-CRASH AV BEHAVIOUR**			
	Collision notification to occupants and operations centres	Communication with operations centre, collision notification centres or use of other communication technologies, when the infrastructure is available.		
	Achieve a minimal risk-state	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, ...).	11b. After a shock while driving (e.g. frontal collision with airbag triggering), the vehicle shall come to a stop and inhibit the AD mode reactication until proper operation has been verified.	