Proposals for Interpretation Documents for UN Regulation No. 157 - Automated Lane Keeping Systems (ALKS)

Submitted by the experts of the European Commission

Introduction

The present manuscript is intended to support the interpretation of the United Nation Regulation 157 (R157 in the following), specifically for what concerns requirements related to the preparation of the Information Document as from Annex 4.

According to R157 Annex 4, prior to the granting of an authorisation for market distribution, the applicant shall be required to submit a detailed demonstration of safety, which shall be reviewed and assessed by the regulatory body in accordance with clearly defined procedures.

The applicant shall be required to submit or make available to the relevant authority all information that is specified or requested in the applicable Regulation. This information is typically presented in the form of an Information Document (ID) as mandated by the applicable legislative requirements.

The requirements to be considered in preparing the ID depend on the regulatory regime adopted by the Country, which may affect the scope and depth of the information presented in the document. In order to have a common framework of information, the following paragraphs provide guidance on the format and content of the ID to be submitted by the candidate[1] for type approval purposes (hereinafter referred to as *Guide*). The Guide is aimed at both manufacturers and regulatory bodies.

Even if the format of the Guide is applicable to any automated driving system, the content is intended primarily for automated vehicles performing the dynamic driving task (DDT) without any human intervention, including the transition from the automatic to the human driver. Finally, the actual contents of the ID depend on the specific type and design of the vehicle considered.

The Guide is divided into two parts, Part A introducing general concepts and aspects that are relevant in defining general safety principles, and Part B providing guidance on the preparation of the Information Document.

[1] The term ‘Candidate’ refers to (a) the ‘Applicant’ (manufacturer/operator/…), (b) the ‘Subject of consideration’ (can be vehicle, can be System...) and (c) the ‘Modifications’ (if applicable, e.g., as is the case with a series vehicle (‘subject of consideration’) which is retrofitted with L4 functions).

A. General Considerations

1. Preamble

1.1. The common understanding of basic general concepts and aspects is fundamental for a constructive interaction between the stakeholders involved in the evaluation of Automated Driving System (ADS) safety by sharing the same terminology and definitions, thus simplifying and speeding up the dialogue and harmonising evaluations.

1.2. Part A of this document concerns the introduction of general concepts and aspects that are relevant in defining the details of the content of the ID reported in Part B. Part A establishes the necessary common understanding concerning those general concepts and aspects.

1.3. The target group of this document includes at least the applicant (e.g., producers/assemblers, importers, sellers), regulatory authorities and support organisations performing independent verification. In addition, Part A can be considered as a reference glossary to be used for any other purpose concerning safety of ADS.

2. Definitions

2.1. Safety of any activity is a general concept requiring specific definitions to establish a common framework and understanding. The following definitions apply to the content of the Guide.

2.2. Automated/Autonomous Vehicle

Vehicle equipped with systems capable, in specific conditions, to perform the Dynamic Driving Task without human/driver intervention.

2.3. Dynamic Driving Task (DDT)

The whole set of real-time functions required to operate a vehicle in on-road traffic.

2.4. System

Set of components, which interact according to a design, in which an element of the system can be another system, called a sub-system.

Examples are mechanical systems, electrical systems and instrumentation and control systems.

2.5. The Automated Driving System (ADS) (also referred to as “the System”)

The system with its electronic control system(s) and all the other relevant systems that provide the Automated Driving Function.

This also includes any transmission links to or from other systems that are outside the scope of this Regulation that have an impact on the Automated Driving Function.

2.6. Automated Driving Function

A function of the ADS that can perform the DDT of the vehicle.

2.7. Operational Design Domain (ODD)

The set of specific operating conditions (e.g., environmental, geographic, temporal, traffic, infrastructure, speed range, weather and any other conditions) within the boundaries set by the regulations under which the automated driving system is designed to operate without any intervention by the driver.

2.8. Accident

The occurrence of fault or emergency conditions.

An accident occurs when:

- A fundamental safety system fails, and the related functions are no more performed.
- Occurrence of conditions not included in the normal operation that cause emergency actions to be actuated.

Note that an accident is not necessarily associate to a damage. An accident is characterised by conditions not included in the set of normal conditions and that can potentially generate a damage. However, safety systems can prevent or mitigate the damage.

2.9. Emergency Systems

Systems only devoted to work in accident conditions to prevent the evolution of an accident in more sever conditions or to mitigate the accident consequence.

The intervention of those systems can be capable to turn the accident conditions into normal operation conditions. In this case, they are switched off. If a normal operation cannot be recovered, the emergency systems will lead the vehicle to safe conditions and emergency systems will remain into operation.

2.10. Safety

Ensuring proper operating conditions for prevention of accidents and mitigation of accident consequences.

The protection is related to the vehicle occupants and other road users and items (as other vehicles, structures and objects) present along the road.

2.11. Safety Concept

High level concept embedded in the ADS to assure that all possible conditions have been considered and the systems implemented perform the intended functions.

This means that, for a set of expected situations, dedicated systems and/or procedures are provided so that the ADS can prevent accidents or mitigate accident consequences under faults and non-fault conditions.

2.12. Safety Analysis

Evaluation of the potential accidents' occurrence associated with the operation of a vehicle or the conduct of an activity.

This typically includes the occurrence of conditions leading to an accident, the reaction of the system to prevent the accident, the evolution of the accident if prevention fails, the response of the systems (including emergency systems) in accident conditions and finally the consequences of the accident considering any mitigation effects. Special analytical techniques (e.g., a computer code) are used.

Note that the formal safety analysis is the main part of the overall safety assessment; that is, it is part of the systematic process that is carried out throughout the design process (and throughout the lifetime of the vehicle or the activity) to ensure that all the relevant safety requirements are met by the proposed (or actual) design.

Safety analysis is often used interchangeably with safety assessment or accident analysis. However, when the distinction is important, safety analysis is a documented process for the study of safety that is done performing a number of accidents analysis, and safety assessment is a documented process for the evaluation and judgment of safety level, for example, evaluation of the magnitude of hazards, evaluation of the performance of safety

measures and judgement of their adequacy, or quantification of the overall impact or safety of a vehicle or activity.

2.13. Assessment

The process, and the result, of analysing systematically and evaluating the compliance with requirements.

Assessment is typically related to activities carried out to determine whether requirements are met, and processes are adequate and effective.

Assessment should be distinguished from analysis. Assessment is aimed at providing information that forms the basis of a decision on whether something is satisfactory or not. Many kinds of tools can be used to perform analyses. Hence an assessment may include several analyses.

2.14. Safety Assessment

The process, and the result, of analysing systematically and evaluating protection and safety measures associated with a given activity.

Safety assessment is carried out throughout the design process and throughout the lifetime of the vehicle.

Safety assessment includes, but is not limited to, the formal safety analysis; that is, it includes the formalised evaluation of the potential accidents associated with the operation of a vehicle.

Stages in the lifetime of a vehicle to be considered in a safety assessment include:

a. ODD definition.

b. Vehicle design and development, including both software and hardware.

c. Vehicle manufacturing.

d. Testing.

e. Type approval of the vehicle.

f. Operation of the vehicle.

g. Modification of the vehicle design or operation.

h. Periodic technical inspection

i. Changes in ownership or management of the vehicle.

j. Decommissioning of the vehicle.

k. Life extension of the ADS beyond its original design life.

2.15. Safety System

System important to safety, provided to prevent the occurrence or to limit the consequences of faults and emergency conditions. The safety systems perform safety functions.

Safety systems consist of the protection system (active and passive), the safety actuation systems and the safety system support features.

Components of safety systems may be provided solely to perform safety functions or may perform both safety functions in defined operational states and non-safety functions in other operational states (e.g., the braking system used in normal operation might be the same used in emergency conditions).

Emergency systems are designed to work in accidental conditions and are generally actuated only when those conditions occur.

2.16. Safety Related System

Every system (also support systems) that is necessary to perform safety functions is safety related and should be considered as part of the safety system.

Some components part of the safety systems can be used in other non-safety systems (e.g., normal operation system) providing that priority is given to the safety functions.

Safety related systems are also all the systems to inform all other road users of the intended manoeuvres of the vehicle (turning, stopping starting etc.)

2.17. Safety Function

A specific purpose that must be accomplished to ensure the safety of the vehicle, or action to prevent or to mitigate the consequences of accident/emergency conditions (see Figure 1).

2.18. Fundamental Safety Function

A fundamental safety function fulfils a safety objective (see Figure 1).

A fundamental safety function is necessary for the use of the ADS: the ADS cannot be activated if a fundamental safety function cannot be performed. If it is included in the design, when minor safety functions are not operable, the vehicle could be used imposing some specific limitations (e.g., reducing the maximum speed) or redefining the operational conditions of use of the vehicle. The failure of the systems performing fundamental safety functions implies the immediate stop of the vehicle also if all normal operations systems are properly working.

Redundancy of the systems performing fundamental safety functions is typically applied.

2.19. Safety Feature

Safety feature is how the safety function is applied.

As an example, the function to safely avoid the collision of the vehicle with an obstacle in emergency conditions can be performed adopting different approaches: by emergency breaking, by an evasive manoeuvre, or by a combination of both options.

The selected approach to perform the safety function follows different specific technical requirements (see Figure 1).

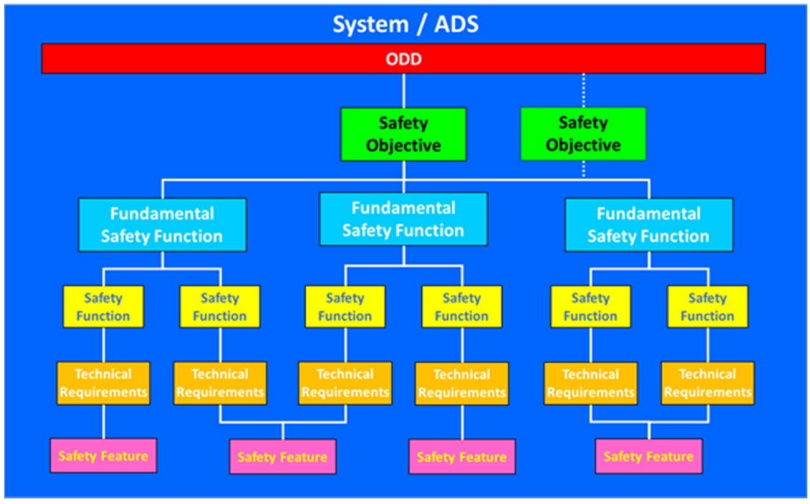

Figure 1 – Relation among safety objective/s, fundamental safety function/s, safety function/s, safety requirements and safety feature/s in a vehicle system or ADS.

2.20. Safety Objectives

Safety objectives are specific criteria adopted in the demonstration of safety.

Currently, they are selected by the producer of the ADS based on high level safety principles defined by the Regulation.

Those criteria could be qualitative, but typically, they are quantitative and are used for comparison with the safety performances to judge the acceptability of the ADS safety level. Those criteria can be based on different approaches selected by the producer of the ADS and are taken into account in the design of ADS.

The adoption of a specific approach to define the safety objectives also implies that the demonstration of the selected approach and of the methods used to prove compliance with the criteria are also validated for that purpose and accepted by the regulatory body.

2.21. Normal Operation and Normal Operating Conditions

Normal operation is the operation within specified operational limits and conditions to perform the designed activity.

In the Guide, specific conditions refer only to those of transportation within specified static and kinematic limits. In this framework, elements like acceleration, breaking actions, speeds etc. are considered. All the other aspects (e.g., comfortable seats, entertainment devices, interior conditions) are outside the scope of the present Guide.

The objective of normal operation is that dangerous conditions are avoided as much as possible while remaining inside specific range of variation of the dynamic solicitations (i.e., within operational limits). An example is provided by the smooth speed reduction as a consequence of the deceleration of the leading vehicles. Decelerations below a0 are considered as normal operation whereas emergency operation are above such limit, with a0 being the threshold value identified by the legislation in force.

When the ADS manages the vehicle keeping the set of identified dynamic variables within specific ranges of variation, the vehicle is in Normal Conditions and the systems are in Normal Operation. A stationary vehicle in a safe state without system failures is also considered as being in Normal Conditions.

An ADS meant to drive the vehicle in normal conditions will be equipped with different systems, each devoted to managing different features and/or functions, as for example (not exhaustive list):

1. To keep a safe distance with the surrounding vehicles avoiding sudden braking or acceleration.
2. To keep the correct lane without sudden lateral corrections.
3. To perform a lane change to take-over an obstacle detected by the sensors with the correct timing, avoiding excessive side speeds or abrupt braking.
4. To adapt the speed to road geometry and conditions, weather and traffic conditions avoiding abrupt accelerating or braking or excessive speed.
5. To respect general and local traffic rules and limits.

The driver support can be included as part of normal operations. In this case, all the conditions consistent with the driver capabilities shall be specified on the ODD. However, diver actions should never be included as a safety option.

2.22. Emergency Operation and Emergency Operating Conditions

The emergency operation is actuated when a deviation from normal operation occurs (failure of normal operation systems) or due to the occurrence of events requiring prompt action to mitigate adverse consequences on human health or property damage.

Notwithstanding the ADS is aimed to keep the vehicle within the Normal Operation, interventions causing the dynamic parameters to fall outside the normal operation thresholds are likely to occur due to external (e.g., interaction with other road users) or internal factors (e.g., failure of a critical component of a relevant system). The latter condition may cause the vehicle to perform a safe stop, in a fast way but without any sharp action, while the former implies the logic that determines the system intervention based on more stringent limiting parameters. In such conditions, the primary ADS aim is to prevent or to mitigate the harm to the passengers and other road users, as well as damage of items. In both cases, the vehicle is in Emergency Conditions and the systems are performing Emergency Operation.

Some examples of actions under Emergency Operation are:

1. Sharp braking action to avoid collision with obstacles that could not be avoided with normal braking.
2. In case of unavoidable exit from the road due to loss of grip, asymmetric braking configuration mode and abrupt steering procedures to allow the vehicle to exit from the less dangerous side.
3. Abrupt intervention of the braking and steering system that could be necessary in case of damage to a tire.

The above definition of Normal and Emergency Conditions and Operation have a conceptual and operational relevance because the hardware and software devoted to the Normal and Emergency have different requirements and are subjected to different operative processes of validation and assessment. The clear definition of the Normal and Emergency definitions makes possible the consequent standardisation of the procedures and methods for validation and assessment.

Figure 2 shows the simplified scheme of the elements relevant to Normal and Emergency Conditions and Operation definition. Normal Conditions are the necessary conditions taking place to perform Normal Operation as defined in ODD. The main target activities of the ADS constitute the set of Normal Operations. When Normal Conditions are not taking place, the ADS cannot perform Normal Operation and some actions by the ADS are necessary to guarantee a safe control and management of the situation. The systems devoted to this aim are the Emergency Systems. The Emergency systems perform emergency actions to bring back in normal conditions or, if it is not possible, to assure and to keep a safe state.

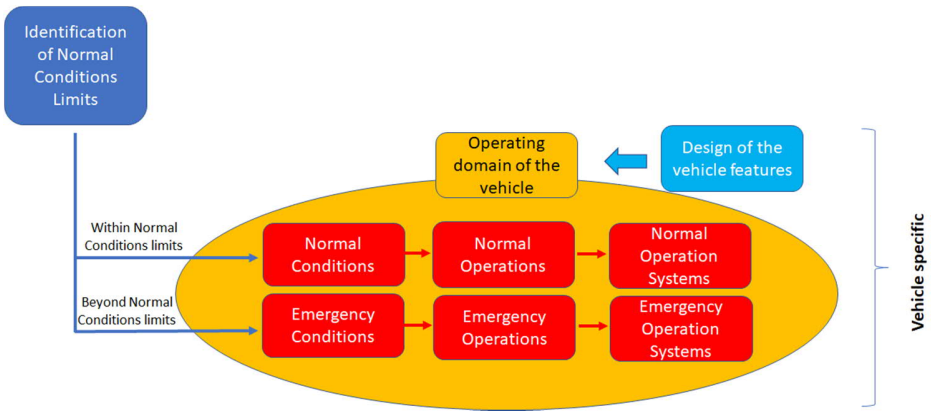

Figure 2 - Simplified scheme of the elements relevant to Normal and Emergency Conditions and Operation definition.

2.23. Safety Assessment Process

The safety assessment process is a methodology to evaluate ADS functions and the design of systems performing these functions, to determine that the associated hazards for those functions have been properly addressed. The safety assessment process is qualitative and can be quantitative.

The Safety assessment process includes the evaluation of:

a. Systems identification

   i. Specification of the Normal and Emergency Conditions of the vehicle.

   ii. Identification and categorisation of the systems and safety systems the vehicle is equipped with, with specific reference to the different intervention requirements under Normal and Emergency Conditions.

   iii. Selection of the systems required to perform the intended operations under different conditions.

b. Response of the system called in to operation

   i. Evaluation of the effects and consequences of the intervention of the systems.

c. Assessment of the reliability and capacity that the selected system is capable to perform the intended operations.

Safety assessment should address all the conditions of the vehicle and all the implemented systems.

When the above-mentioned aspects are well identified and defined, the safety assessment process can be subdivided in two main steps:

Step 1 Selection of the Conditions, Operations and Systems for both Normal and Emergency Conditions to be included in the analysis. It is necessary to ensure that all the foreseeable conditions and occurrences have been considered, the related operations and the necessary systems have been identified. The safety verification process is performed at this level.

Step 2 Proving that Conditions, Operations and Systems selected at Step 1 comply with the specific requirements. It is necessary to demonstrate the effectiveness of the relevant systems to perform the intended functions. The safety validation process is performed at this level.

Figure 3 summarises the most relevant aspects of the Safety Concept and presents the main elements of safety assessment process. For emergency aspects (second rows of red boxes) the possible expected conditions are identified, analysed, and actuated systems are selected. This phase constitutes the first safety level (first row of blue boxes). The assessment of the selected systems effects in the selected conditions constitutes the second level of safety evaluation (last blue box).

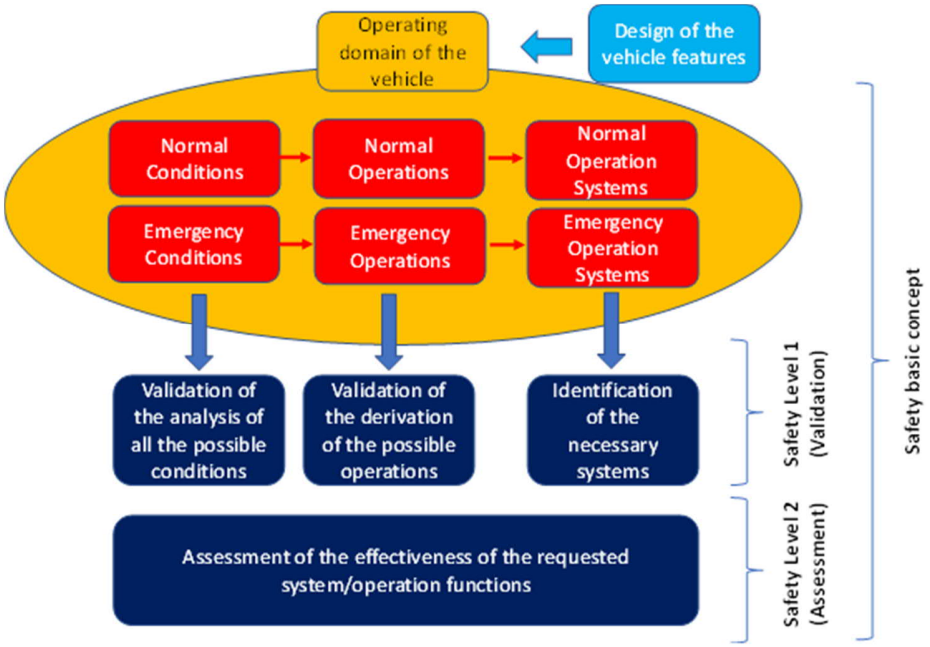

Figure 3 - Most relevant aspects of the Safety Concept.

3. Fundamental Principles

3.1. The vision and the associated key safety aspects, as identified within the WP29 Framework Document on automated/autonomous vehicles[2] and the EC Guidelines on the approval of automated vehicles through the exemption procedure[3], are here briefly described concerning their intent and purpose.

3.1. Safety Vision

3.1.1. Automated vehicles have the potential of improving road transport from many viewpoints, including mitigation of its negative externalities (such as effects of car accidents) and promoting social inclusion. The first prerequisite to achieve these improvements is that vehicles placed on the market can guarantee a high level of performance. The following safety vision established by WP.29 aims at the delivery of safe and secure road vehicles

3.1.2. *"The level of safety to be ensured by automated/autonomous vehicles implies that "an automated/autonomous vehicle shall not cause any non-tolerable risk", meaning that automated/autonomous vehicle systems, under their automated mode ([ODD/OD]), shall not cause any traffic accidents resulting in injury or death that are reasonably foreseeable and preventable."*

3.2. Key Safety Aspects

3.2.1. EC Guidelines on the approval of automated vehicles through the exemption procedure and the WP29 Framework document on automated/autonomous vehicles define a

[2] www.unece.org/fileadmin/DAM/trans/doc/2019/wp29/ECE-TRANS-WP29-2019-34-rev.1e.pdf
[3] ec.europa.eu/growth/content/guidelines-exemption-procedure-eu-approval-automated-vehicles_en

series of elements that must be addressed to evaluate the vehicle safety. Those elements can be considered as key safety aspects, which shall be addressed in the appropriate sections of the ID. Reference shall be made to the latest revisions of the two reference documents mentioned above. Compliance with all key safety aspects shall be demonstrated by the manufacturers in the ID. The key safety aspects are as follows:

a. *System Safety*: When in automated mode, the automated/autonomous vehicle should be free of unreasonable safety risks to the driver and other road users and ensure compliance with road traffic regulations.

b. *Failsafe Response*: The automated/autonomous vehicles 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.

c. *Human Machine Interface (HMI) / Operator information*: The automated/autonomous vehicles 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 the driver needs to regain proper control of the vehicle. In addition, automated vehicles should allow interaction with other road users (e.g., by means of external HMI on operational status of the vehicle, etc.)

d. *Object Event Detection and Response (OEDR)*: The automated/autonomous vehicles shall be able to detect and respond to object/events that may be reasonably expected in the [ODD/OD].

e. *Operational [Design] Domain (O[D]D) (automated mode)*: 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.

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 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.

g. *Cybersecurity*: The automated/autonomous vehicle 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.

h. *Software Updates*: Vehicle manufacturers should ensure system updates occur as needed in a safe and secured way and provide for after-market repairs and modifications as needed.

i. *Event Data Recorder (EDR) and Data Storage System for Automated Driving vehicles (DSSAD)*: The automated/autonomous vehicles should have the function that collects and records the necessary data related to the system status, occurrence of malfunctions, degradations or failures in a way that can be used to establish the cause of any crash and to identify the status of the automated/autonomous driving system and the status of the driver.

j. *Vehicle maintenance and inspection*: Vehicle safety of in-use vehicles should be ensured through measures such as related to maintenance and the inspection of automated vehicles etc. Additionally, vehicle manufacturers are encouraged to have documentation available that facilitates the maintenance and repair of ADSs after a crash. Such documentation would likely identify the equipment and the processes necessary to ensure safe operation of the automated/autonomous vehicle after repair.

k. *Consumer Education and Training*: Vehicle manufacturers should develop, document and maintain employee, dealer, distributor, and consumer education and training programs to address the anticipated differences in the use and operation of automated vehicles from those of conventional vehicles.

l. *Crashworthiness and Compatibility*

m. *Post-crash AV behaviour*: Automated/autonomous vehicles should be able to return to a safe state immediately after being involved in a crash. Things such as shutting off the fuel pump, removing motive power, moving the vehicle to a safe position off the roadway, disengaging electrical power and other relevant actions should be considered. A communication with an operations canter, collision notification canter, or vehicle communications technology should be used.

3.2.2. The safety principles are applicable, as relevant, throughout the entire lifetime of the vehicles including back-fits and updates. They provide the basis for requirements and measures for the protection of people and property against risks deriving from automated driving.

3.2.3. It is recommended to refer to the latest revision of the applicable regulation, to ensure that no modifications have been issued to the safety vision and key safety aspects.

B. The Information Document

1. Preamble

1.1. The ID shall report the safety assessment in sufficient level of details to demonstrate the safety, to support the conclusions reached and to provide an adequate input to independent verification and regulatory review.

1.2. While the ID itself should be sufficiently comprehensive for the above purposes, there may be other documents, which are used as supporting information to regulatory review. Similar rules to those established for the ID should apply to all documentation intended for submission to the regulatory body.

1.3. Sensitive information included in the ID and supporting reports, the unauthorised disclosure of which could compromise proprietary and vehicle security, should be identified. Such information should be protected in accordance with guidance on information security in force.

1.4. In the following, the expected approval process is reported, and the sections and contents of the ID are described.

2. Expected Approval Process

2.1. The ID is an integral part of the communication between the applicant and the regulatory body, and it forms an important part of the basis for certification of an automated vehicle as a precondition for its safe operation. A multiple stage approach should be established to subdivide the application into basic elements so as to streamline the process:

a. *Stage 1 - Audit report of manufacturer development processes*: should be issued before or at the beginning of the development phase. It includes the description of all relevant ADS development processes of the manufacturer. It ensures that the manufacturer has the capabilities to develop products applying the best industrial practices. It confirms that the management system set in place is reasonable and effective. The qualification of the manufacturers' employees, suppliers, subcontractors and any third parties taking part in the ADS development as well as quality of their product is covered by this audit report. This report should include demonstration that the manufacturer has the capabilities and knowledge to develop safe and secure products, which can operate flawlessly on public roads. This audit report stands for its own and needs to be updated or re-audited in regular intervals.

b. *Stage 2 - Preliminary Information Document (PID)*: should be issued at the beginning of or during the development phase of a new product. The subject of this assessment is the ADS itself. This document lays down how the ADS is being developed according to the state of the art and to the manufacturers own processes as described in Stage 1. It gives a detailed view of the functional safety, Safety of the Intended Functionality (SOTIF) and Security concept and description of how the safety objectives are being met. Analyses, simulations and related documentation will be necessary for the evaluation of the safety concept (directly included in the report or made available for consultation at the applicant's premises in case sensitive information is included). The assessment, in particular the reporting of the risk assessment outcomes, should provide recommendations for the following physical testing stage as prescribed in the reference Regulation. The PID should also include a statement of the safety principles adopted (see Key Safety Aspects above) and the safety objectives set for the intended design. It should include a statement of the manner of conforming to the fundamental safety

principles and a statement of how the safety objectives are being met. It should contain sufficiently detailed information, specifications and supporting analysis to enable those responsible for safety assessment to conclude whether the vehicle/ADS is acceptably safe throughout its lifetime.

c. *Stage 3 - Final Information Document (FID) for type approval*: in the final stage all results and reports of previous stages shall be integrated in this FID to be submitted to the approval authority in charge. The FID incorporates the revisions to the preliminary design ad complements the PID with results from track testing and real-world test drives prior to the vehicle entering the market. Certification for market distribution will be released based on FID after authorisation by the relevant authority. The final report should demonstrate that the vehicle meets its safety design intent. The final ID should be the basis for the granting of a type approval.

d. *Stage 4 – Additional verification testing by authority*: the purpose of this stage is to substantiate the positive conclusion of the assessment report of stage 3 and to objectively quantify/verify the performance of the ADS. Dedicated, reproducible and challenging tests under situations ranging from nominal operations to worst-case vehicle configurations shall be conducted by the authority. Results from physical testing might also be used to validate the results coming from the simulations and virtual testing. The results of verification testing from the authority shall be summarised in section 7 of the FID, that will be left empty until this stage.

e. *In-use Data Report (IDR)*: Systematic updating of the FID would then become a requirement for the applicant during the remaining lifetime of the vehicle. This would usually be done periodically in order to reflect any feedback of operating experience, software modifications and improvements, new regulatory requirements or changes to the certification basis. Intermediate updates can be recorded in the IDR until major changes require an official update of the ID.

2.2. The IDs should be submitted to the regulatory body sufficiently well in advance prior the need of the authorisation in accordance with an agreed timetable. Such an approach will allow a streamlined authorisation process and help preventing delays.

3. Format and Content of the Information Document

3.1. The ID includes 11 parts, as described hereinafter (see figure 4):

0. *Introduction*, providing introductory information.

1. *Section 1*, providing a general description of the ADS, the definition of the ODD (§1.1), of the basic performance of the vehicle (§1.2) and of the means to activate, override or deactivate the ADS (§1.3).

2. *Section 2*, providing a description of the functions for both vehicle-internal (§2.1) and vehicle-external functions (§2.1), as well as the control strategies (§2.3).

3. *Section 3*, dealing with the hardware relevant to the ADS, namely control units (§3.1), sensors (§3.2), actuators (§3.3) and other hardware (§3.4).

4. *Section 4*, providing schemes, layouts and flowcharts of systems (§4) and sub-systems (§4.1), as well as their interfaces (§4.2).

5. *Section 5*, describing the ADS specifications in Normal (§5.1) and Emergency Conditions (§5.1), the acceptance criteria (§5.3) and the demonstration of compliance with those criteria (§5.4).

6. *Section 6*, providing the implementation of the safety concept, namely the approaches adopted to assure the safety of passengers and other road users, as well

as compliance with road rules, starting from the definition of safety objectives. The section continues with the manufacturer statement (§6.1), the description of software architecture (§6.2) and hardware solutions (§6.3) adopted to achieve the safety objectives, system self-diagnostics and main design provisions adopted to obtain safe operation (§6.4), transition demand (§6.5), human-machine interface (§6.6), protection against simple unauthorised interventions (§6.7), validation and verification by the manufacturer (§6.8).

7. *Section 7*, dealing with the verification and tests performed by the authorities to assess both the vehicle safety functions (§7.1) and the vehicle behaviour when facing failures, operational disturbance, boundary and emergency conditions (§7.2).
8. *Section 8*, describing the data storage system in terms of type of data stored (§8.1), storage location and crash survivability (§8.2), data recorded during vehicle operation and occurrences (§8.3), data security and protection against unauthorised access or use (§8.4), means and tools to carry out authorised access to data (§8.5).
9. *Section 9*, dealing with cyber security aspects, namely: cyber security and software update management (§9.1), identification of risks, mitigation measures, secondary risks and assessment of residual risk (§9.2), software update procedure and management put in place to comply with legislative requirements (§9.3).
10. *Section 10*, describing the information provided to the users to let them be properly informed about their responsibilities, providing models of the information provided (§10.1), as well as reporting extracts of the owner's manual relevant to provide evidence of the information given to the owner (§10.2).

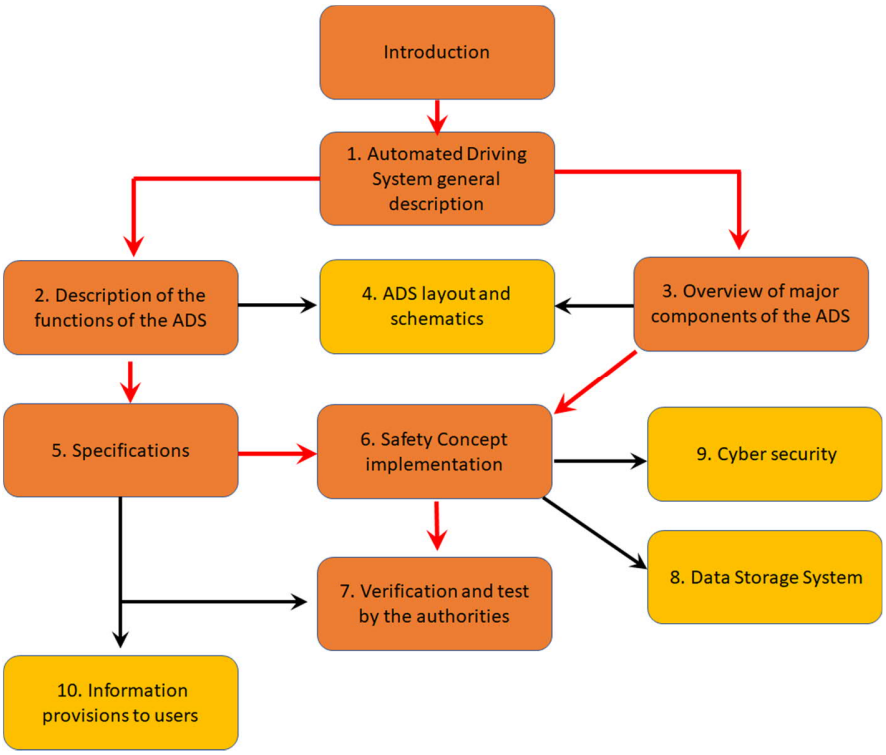

Figure 4 – Information Document structure and navigation diagram.

Introduction

This section should include as a minimum:

a. Definitions and acronyms used for the purpose of the ID.

b. The identification of the ADS, including implemented ADS features.

c. The intended use of the vehicle.

d. A description of the existing approval status.

e. A statement of any similar (or identical) vehicle that the regulatory body has already reviewed and approved and a statement of the specific differences and improvements that have been made since such an approval was granted.

f. A description of the structure of the ID, the objectives and scope of each of its sections and the intended connections between them.

A comprehensive list of applicable regulations, codes and standards should be provided as Annex I to the ID and recalled in this section. Every document from the list should also be recalled in the appropriate sections when describing the context where it is considered.

If the regulations, codes and standards have not been prescribed by the regulatory body, a justification of their appropriateness should be provided.

Any changes made to or deviations from the requirements for the design should be clearly stated, together with the way in which they have been addressed and justified.

1. Automated Driving System Description

The objective of this section is the description of the ADS's mission, the ADS boundaries, and its overall architecture, including the main sub-systems and their relationships. This description constitutes a high-level overview of the ADS.

This section should include:

a. The fields of application and the domain of operation including limitations and restrictions to the use of the automated driving system.

b. The main features of the ADS.

c. A general description of the ADS in terms of hardware and software.

Related to the last bullet, it is worth to provide descriptions of:

1. *Technical Requirements*: the technical requirements define the functions that the system should be able to perform. Note that technical requirements are independent from the adopted solution and from the implemented technology.

2. *System Architecture*: the architecture of the ADS should include the development of related logical architecture models and physical architecture approach. Note that the System Architecture is generally independent from implemented technology.

3. *Physical Architecture*: the physical architecture is related to the selected technologies. It should be documented how the technologies are selected according to the system requirements, and desired functions and related technical requirements. Note that some aspects of Physical Architecture can be selected based on non-functional requirements, such as operational conditions and life cycle constraints (e.g., environmental conditions, maintenance constraints, etc.).

As already stated, this section should report a general description of the ADS. The details about the ADS concerning hardware and software are described in sections 2 and 3.

This section should report also the certifications adopted or applied for the systems included in the vehicles. Systems already approved in different vehicles should be also identified.

1.1. Operational Design Domain

A key aspect for the use of vehicles equipped with ADS technology is defining the ADS capabilities and limitations. The first step is the definition of the Operational Design Domain (ODD) for each ADS sub-system and/or for the ADS as a whole system. The ODD represents the operating environment within which the ADS can perform the Dynamic Driving Task (DDT) as intended in the design.

"Operational Design Domain (ODD)" defines the specific operating conditions (e.g., environmental, geographic, time-of-day, traffic, infrastructure, speed range, weather and other *conditions) within the boundaries fixed by the regulations under which the automated driving system is designed to operate without any intervention by the driver*[4].

The ODD description should contain all the necessary information relevant to its unambiguous definition, namely all the relevant elements must be defined, described and quantified. The ODD description should include at least the elements listed below. It is worth to stress that the following list of elements is not intended to be exhaustive; the applicant shall add all the elements needed to provide a self-standing and comprehensive description of the ODD:

a. Range of vehicle functional parameters (internal conditions) as for e.g., speed range.

b. External conditions, as for e.g., country, road type, road conditions (surface, lane markings), weather conditions (visibility, temperature, humidity, wind), traffic conditions, connectivity.

c. Driver status (if relevant).

Combinations of some of those elements can also be used to specify the ODD where necessary. As an example, a system might be designed to operate with snow or wind within specified limits, but not having snow and wind at the same time.

Whatever is not reported in the description of the ODD must be considered outside the definition of the ODD. Note that the authority might request additional information on any element not mentioned and quantified in the submitted list.

ODD limits expressed by numerical values shall be expressed in measurable quantities in SI units when possible.

Any element listed in the ODD description should be continuously measured or monitored, as appropriate, by the ADS.

Description of any conditions that triggers the Minimum Risk Manoeuvres and transition demands should be provided, including the items listed above as minimum content.

1.2. Basic Performance

This section describes the response of the ADS (in terms of its behaviour and the expected performances) in all the possible conditions falling within the defined ODD.

This section shall include the conceptual description of the behaviour of the ADS in the conditions defined above, possibly including a general description of the elements of the process that determine the performance of the ADS. As an example, a typical sequence of

[4] UN ALKS Regulation

actions starting from the initial signals to the final check of the performed action can be described as follows:

a. Signal formation

b. Signal received

c. Signal elaboration and verification

d. Creation of the signal for actuation of a control

e. Actuation of the components/elements

f. Check of the actuation of the components/elements

g. Expected effects of the actuation of the components/elements

h. Control on the effects of the actuation of the components/elements

i. Features assuring the safety of whole process.

Note that, because of the different level of complexity of ADSs, some of the above steps could be not defined or could be implicitly defined and therefore could be not included in the description.

The behaviour of the ADS shall be described in all the situations included within the ODD for both Normal and Emergency Conditions.

Lists and diagrams can be helpful to illustrate the set of considered actions.

A topic that must be also addressed is the performance related to unexpected conditions, i.e., conditions that are unlikely to occur. A list and description of those unexpected conditions should be provided. Selection of such conditions can be based on the estimated frequency of occurrence, or on analogous analysis for similar systems, or on the engineering expert judgment. Those unexpected conditions correspond to “edge case” events, for example that fall outside the ODD conditions or beyond the legislative requirements (e.g., recognition of an airplane landing on the highway). They should have an exceptionally low probability of occurrence; therefore, the implementation of dedicated systems, sub-systems or components may have been judged as not reasonably necessary (beyond design basis scenarios/accidents). The performance of the ADS for such unlikely conditions should be described with the goal of demonstrating that it still ensures an acceptable performance.

As an example, the section can include a list of considered conditions:

- Condition 1,
- Condition 2,
- ……
- Condition n,

and the corresponding performance of the ADS for each of the identified condition:

- Behaviour of the vehicle in Condition 1,
- Behaviour of the vehicle in Condition 2,
- ……
- Behaviour of the vehicle in Condition n.

Finally, a categorisation of the logic and related performances can be also included. As an example, the logic and related performances can be subdivided in:

1. *Detective*: they are related to identify the cause or symptoms of an event. Identification needs to be based on the signals received by the sensors and on the treatment of those signals.
2. *Preventive*: to avert a negative event from occurring.
3. *Corrective*: typically put in place when a modification of the response of the ADS is necessary. These functions cover both Normal end Emergency conditions.

It is important to provide an exhaustive description of the performances of the ADS under all conditions. What is explicitly excluded or not described will be considered as beyond the capabilities of the ADS itself.

1.3. The Means to Activate, Override or Deactivate the ADS

This section describes the activation and deactivation of the ADS with adequate level of details, including the conditions in which each action is allowed or prevented and the procedural and technical means by which inadvertent and unauthorised activation/deactivation is prevented.

The following aspects must be addressed:

1. Necessary conditions for the activation/deactivation of the ADS under Normal Conditions.
2. Necessary conditions for the activation/deactivation of the ADS under Emergency Conditions.
3. Possibility to override the ADS.
4. Setup and/or options that can be selected by the user to bypass the default setup of the ADS.
5. Possibility to reset the ADS.

Concerning the items 1 and 2, important elements are:

a. Time necessary or admissible for activation/deactivation
b. How the transition occurs between the two states
c. How the ADS recognizes that the conditions for activation/deactivation are met
d. Conditions preventing activation/deactivation

Concerning the items 3 and 4, important elements are:

e. Elements/parameters that can be modified/superseded
f. Conditions allowing ADS override
g. How the transition occurs during ADS override
h. Authorisations needed to override or bypass the default setup of the ADS

Concerning the item 5, important elements are:

i. Conditions that allow the reset of the ADS
j. Authorisations needed to reset the ADS

The aspects and the elements above must be described, discussed and justified.

It is worth mentioning that activation, deactivation and override of the ADS must never be considered as procedures to solve emergency.

2. Description of the ADS Functions

This section should describe the ADS functions and logics adopted, namely, the logical processes connecting conditions (as identified in section 1.1) to performances (as described in section 1.2). The descriptions are not intended to enter the detail of the used hardware, which is the subject of section 3, while the integration between hardware and logic is the subject of section 4.

The functions implemented into the ADS must be described, including how they carry out collection, analysis, synthesis, evaluation and decision making in both Normal and Emergency conditions, as well as all the logical processes covering the acquisition, treatment and interpretation of data, the elaboration process including handling of contradictory information, and the definition of the actions to be performed.

The description of the functions also includes specification of inputs and generated outputs and the involved data processing. The inputs are generated by the measurements or monitoring of both external and internal parameters. Exchange of data through the interfaces between different functions must also be considered.

The ADSs can include several functions: description of functional hierarchy and decomposition of functions can be useful to give a more comprehensible insight.

This section must include an overview of the functions and a description of function hierarchy and interfaces. The details of each function must be described in the following sections, splitting between vehicle-internal (§2.1) and vehicle-external functions (§2.2), while the control strategies are the subject of the last section (§2.3).

2.1. Vehicle-internal Functions

Vehicle-internal functions are characterised by being fully on board of the vehicle, namely input and output data are all generated, collected and treated by on board features. Those functions are independent from external sources of data or external computational power, and all the necessary functions are totally performed in the vehicle. However, interfaces with external systems can exist. Those functions have specific requirements concerning safety and security connected only to the ones of the vehicle itself. Those functions can be monitored by other functions, either internal or external.

2.2. Vehicle-external Functions

Vehicle-external functions (e.g., connectivity-related functions) are characterised by not being fully on board the vehicle. In this case the functions are not under complete control by the vehicle. These functions usually concern conditions not directly detectable, measurable or derivable by on board features, and imply transfer of data from external systems to the vehicle and vice versa (e.g., backend).

2.3. Control Strategies

This section must cover the description of the control strategies adopted by each function and by the ADS to handle the different functions and the interfaces among them.

Some relevant aspects to be addressed are:

a. Logic for the selection to activate or deactivate functions during ADS operations

b. Transitions between the various functions of the ADS

c. Function modes, priorities and limitations.

3. Overview of Major Components of the ADS

This section describes the hardware of components and subsystems devoted to ADS technology. In this framework, hardware important for the driving but not related to ADS tasks is not included, e.g.:

a. Gear system

b. Braking system

c. Engine system

d. Steering system

These systems, although monitored and actuated by the ADS during the DDT, are not specific features of the ADS. On the other hand, the actuators specifically used by the ADS to actuate the above systems are part of the ADS and shall be included in the description.

The hardware to be considered as part of the ADS can be subdivided in the following main categories, to be described in the following sections:

1. Electronic control units
2. Sensors
3. Actuators
4. Other ADS hardware

The hardware related to both Normal and Emergency Operations shall be described.

3.1. Control Units

This section describes the electronic control units. These elements are typically the electronic components hosting the software.

Example of these hardware elements are the processors, wiring, memory banks, electronic boards, wireless and net devices, cabling, hardware framework.

The components can be grouped based on selected preferred approach (e.g., based on the performed function or based on kind of hardware typology) for a better understanding of the reader. The description can be more general for components commercially available; in this case, the model and the manufacturer shall be identified. The reference specifications and certifications can be simply indicated and made available to the authority upon request.

For proprietary ADS specific components, more details must be provided and supported by specific documentation.

The consistency of the characteristics of these components with the expected functions to be performed must be demonstrated, also including limitations in the operation. The accuracy and reliability under the foreseen working conditions should also be reported.

Whenever redundancy and/or diversity are implemented, they shall be declared; in this sense, indicating the number of the elements involved could ease the clarity of the description. Redundancy and diversity shall correspond to the required reliability of the system.

3.2. Sensors

This section describes the sensors. Many kinds of sensors can be implemented in the ADS. The basic function of a sensor is to transform a monitored physical quantity into an electric signal. Typically, sensors are supported with other electronic elements for signal treatment (e.g., amplification, rectification, etc.).

The description can be general for components commercially available, in this case the model and the manufacturer shall be identified. The reference specifications and certifications can be simply indicated and made available to the authority upon request.

For proprietary ADS components, more details must be provided and supported by specific documentation, (even at the applicant's premises).

The consistency of the characteristics of these components with the expected functions to be performed must be demonstrated, also including limitations in the operation. The accuracy and reliability under the foreseen working conditions should be also reported.

Whenever redundancy and/or diversity are implemented, they shall be declared; in this sense, indicating the number of the elements involved could ease the clarity of the description. Redundancy and diversity shall correspond to the required reliability of the system.

3.3. Actuators

This section describes the actuators. These devices provide the interfaces between software and hardware, they transform the logical signals into physical quantities. Many kinds of actuators exist, among the others mechanical, electro-pneumatic or electro-hydraulic actuators.

The description can be general for components commercially available, in this case the model and the manufacturer shall be identified. The reference specifications and certifications can be simply indicated and made available to the authority upon request.

For proprietary ADS specific components, more details must be provided and supported by specific documentation (even at the applicant's premises).

The consistency of the characteristics of these components with the expected functions to be performed must be demonstrated, also including limitations in the operation. The accuracy and reliability under the foreseen working conditions should be also reported.

Whenever redundancy and/or diversity are implemented, they shall be declared; in this sense, indicating the number of the elements involved could ease the clarity of the description. Redundancy and diversity shall correspond to the required reliability of the system.

3.4. Other Hardware

This section shall typically include descriptions of the transmission links used for conveying signals, operating data or energy supply between inter-connected hardware described in the previous sections. In case other hardware is present in the vehicle in addition to the ones described in the previous sections, it shall be described here (e.g., specific hardware developed for the ADS special needs or features). Some examples of such hardware are hereafter reported:

a. Global Navigation Satellite System (GNSS) to localise the exact position of the vehicle. These systems are typically standardised and commercially available, but some special functions and related hardware could be developed for special needs.

b. Hardware necessary for the connection with external infrastructures or external systems (e.g., centralised systems for the automatic parking of the vehicle in dedicated/reserved areas).

c. Special hardware to perform specific functions during maintenance.

The description can be general for components commercially available, in this case the model and the manufacturer shall be identified. The reference specifications and certifications can be simply indicated and made available to the authority upon request.

For proprietary ADS specific components, more details must be provided and supported by specific documentation (even at the applicant's premises).

The consistency of the characteristics of these components with the expected functions to be performed must be showed, also including limitations to the operation. The accuracy and reliability under the foreseen working conditions should be also reported.

Whenever redundancy and/or diversity are implemented, they shall be declared; in this sense, indicating the number of the elements involved could ease the clarity of the description. Redundancy and diversity shall correspond to the required reliability of the system.

4. ADS Layout and Schematics

The systems belonging to ADS are represented in this section by schemes, namely layouts, flow charts, Process Flow Diagrams (PFD), Process and Instrumentation Diagrams (P&ID) and/or any other description of the systems representing the sources of external signals (e.g., sensors or connections with external systems), the processes using the signals and generating the outputs, as well as any interface with other processes and/or functions.

A possible approach to balance the complexity of the information in this section is to limit the information provided to a reasonable level of abstraction and make available more detailed and complete layouts to the authority on request.

4.1. Schematic System Layout

This section should graphically describe all subsystems included in each system. The level of decomposition to be adopted in the description of the subsystems depends on the complexity of the whole system.

In the diagrams presented in this section the main path of the input signals, the elements and components treating and processing the signals as well as the generated output must be clearly described. The elements and components should be identified by a reference ID (as indicated in section 3), and the expected values of the signals should be reported. Redundant and alternative paths of the signals and processes must be included in the description. Both the Normal and Emergency conditions must be considered.

4.2. List and Schematic Overview of Interconnections

In this section, the interfaces and connections between the systems devoted to the DDT and any other system of the vehicle are reported. The interfaces related to systems external to the vehicle are also included in this section.

In addition to the interfaces description, this section should also demonstrate the compatibility between interfacing systems. In this regard, it is needed to show that in all the considered Normal and Emergency conditions the interfaces and interconnections between systems are properly working.

5. Specifications

This section describes in detail the responses obtained when the ADS functions are called to operate. The responses must be based on a quantitative description of the behaviour of the ADS and/or the vehicle. As an example, the quantities to be considered and quantified are as follows:

a. Distances with neighbour vehicles

b. Velocities (longitudinal, lateral)

c. Acceleration/braking intensities

d. Reaction times.

This section is focused on the designed behaviour of both the ADS and the vehicle. Therefore, it shall include the numerical values resulting from the output of the functions having a direct role in ADS tasks. The numerical values of parameters treated and elaborated in the processes internal to the functions or in functions not directly affecting the final behaviour of the vehicle should be also documented if relevant for more complete and comprehensive description

5.1. Specifications in Normal Conditions

This section describes the specifications related to Normal Conditions.

5.2. Specifications in Emergency Conditions

This section describes the specifications related to Emergency Conditions.

5.3. Acceptance Criteria

For any variable used to define the behaviour of the ADS and the vehicle in both Normal and Emergency Conditions, an applicable acceptance criterion must be indicated.

Reference should be made to relevant laws, regulations and norms (as indicated in Annex I, list of applicable codes regulations and standards) and to other acceptance criteria (including those established by the manufacturer).

5.4. Demonstration of Compliance

This section should demonstrate that the values obtained in both Normal and Emergency Conditions comply with the limits and thresholds defined by the acceptability criteria (both legislative and any additional including those established by the manufacturer) mentioned in the previous section.

If no acceptability criterion is defined by law for a variable and the acceptability criterion is thus defined only by the manufacturer, a demonstration should be provided that the resulting numerical values are reasonable in terms of minimised probability and scope of damage to passengers, vehicle and other road users.

6. Safety Concept Implementation

This section is dedicated to the Safety Objectives adopted by the manufacturer to ensure safe operation during Normal and Emergency Conditions. They act as the principles guiding the definition of the safety systems details. The section should describe the approaches adopted to assure the safety of the driver, passengers, and other road users, as well as compliance with traffic rules.

It is important to note that all the systems, components and logics are designed to operate in Normal and Emergency Conditions. They are designed in the way that the ADS/vehicle is operated consistently with specific ranges of acceptability for both conditions. Namely, the safety is indirectly guaranteed by the fulfilment of defined acceptance criteria (Step 1, see definition of Safety Assessment Process). However, the expected behaviour of the ADS/vehicle must be met and verified (Step 2). As an example, the function to keep a proper distance from the other vehicles must be not only included in the ADS (Step 1), but it is also necessary to prove its effectiveness when ADS is called to operate (Step 2).

The approaches to ensure the expected behaviour of the ADS must also be described. The approaches may vary depending on different factors, e.g.:

a. Relevance of the system/sub-system/function/feature

b. Adopted technology

c. The probability of failure of the considered system.

As an example, the following general approaches can be used:

1. *Quality*: of components, processes, manufacturing, supply-chain, etc. to ensure a low failure rate

2. *Redundancy*: the most relevant functions/systems/components are provided with backups

3. *Diversity*: different systems performing the same action based on different physical phenomena

6.1. Vehicle Manufacturer Safety Statement

This section should contain the statement with confirmation that the manufacturer shall provide the ADS free from unreasonable risks for the driver, passengers and other road users.

6.2. Software Architecture

This section should demonstrate consistency with the approaches defined above for the software to prevent and minimize the probability of logic failure and to handle possible logic failure so that to minimise the consequences to the driver, passengers, and other road users.

The possible failure of the logic requests the implementation of algorithms performing the verification of inputs and outputs of the processes and coherence checks to assure that the logic is working as intended (i.e., input and output are inside the proper ranges of variation). These algorithms typically require the development of high-level routines capable to recognise and to evidence abnormal situations and the implementation of parallel and independent systems/routines to check errors. The description of such routines, algorithms and specific systems should be also described in this section

6.3. Means by which the Realization of the ADS Logic is Determined

This section should describe the hardware supporting the ADS logic and its possible failures. The section should demonstrate the application of the approaches defined above to minimize the probability of hardware failures and to handle possible failures so that the consequences to the driver, passengers, and other road users are minimised. Safety relevant aspects to be considered are related to:

a. Allowable operational conditions e.g., temperature limits of components.

b. The hardware hosting the software, e.g., the electronic devices and components.

c. The hardware supplying the input to the software, including sensors, interconnections and the hardware connecting the ADS and its systems with other external systems (e.g., for data transfer).

d. The hardware adopted for the actuators.

6.4. Main Design Provisions for Safe Operation

This section describes the main ADS design provisions in order to ensure its safe operation and interaction with other road users under fault conditions, under operational disturbances and under the occurrence of planned and unplanned conditions that would lead to exceed the ODD boundaries. In addition, this section should include the description of the failure

handling main principles, the fall-back strategy and the risk mitigation strategy, including the minimum risk manoeuvre.

The applicant should also describe the strategy implemented for recognition of ODD boundaries and ADS behaviour when the limits of the ODD are approached and then exceeded until the transition demand is issued.

The first topic to be addressed in this section is related to the means to check the correct operational status of the ADS.

In addition to the functions devoted to the ADS, a set of high-level functions is necessary to check and evaluate the efficiency of the ADS and its systems. These functions are continuously performing cross-checks and comparing selected indicators of the ADS with reference values. If too large discrepancies are revealed corrective actions are taken (e.g., actuation of alternative or back-up systems).

The description of these functions must also include:

a. justification of the adopted approaches.

b. checks and controls performed.

c. description of the consequences of incorrect operations.

The ADS behaviour must be described under expected and reasonable fault conditions, for which specific design provisions could be implemented into the system.

In fault conditions, the system is working outside the normal conditions and outside the requirement assuring the performance of the ADS. It should be noted that when the function of a faulted system is performed by an alternative system, it should not be considered as fault condition, but specific corrective actions must be put in place since the system redundancy is lost.

The behaviour of the ADS under the above-mentioned conditions is described, evidencing its capabilities to react to those conditions by obtaining a response as safe as reasonably possible depending on probability consideration.

A list of possible and reasonable fault conditions must be considered and justified at this stage, and the behaviour of the ADS/vehicle should be described including the interaction with other road users. The consequence of such conditions should be also evaluated

6.5. Transition Demand

This section should describe the transition demands, namely:

a. Conditions that lead to generate transition demands.

b. How the ADS generates the request for transition to the driver.

c. How the transition is performed.

d. Functions passing under the control of the driver.

e. Confirmation of the release of the functions under the control of the driver.

f. ADS limitation and intervention on the functions under the driver control.

g. Functions remaining under the control of the ADS after successful transition.

h. ADS behaviour if the transition is not occurring.

i. Conditions for the return of functions under the ADS control.

j. Signals given to the driver, occupants and other road users in each of the above aspects.

k. Means by which control and checks are executed in each of the above aspects.

l. Management of time constraints in all the items above.

The applicant should also describe the methods and measures put in place in order to monitor and correctly evaluate the driver status relevant to the fall-back request. The special provisions implemented to account for users that may not be receptive shall be described as well.

6.6. Human-Machine Interface

This section should describe the interface between the vehicle equipped with ADS capabilities and the user (driver and vehicle occupants), hereinafter referred to as "Human Machine Interface" (HMI).

The applicant should describe mechanisms put in place to always inform the user about the ADS status and their responsibilities both as a driver and as a fallback-ready user in an understandable and unambiguous way. This section should also report on how the HMI communicates every ADS state, modes of operation, possible limitations, as well as any additional information relevant to the driver. At a minimum, the description should address how HMI is capable of informing the user that the ADS:

a. is functioning properly,

b. is currently engaged,

c. is currently unavailable,

d. is experiencing a malfunction,

e. is requesting a fall-back request to the user.

The applicant should describe the methods adopted to design an HMI that is comprehensible, easy, non-distracting, safe to use, and possibly promoting social inclusion. The whole design process should account for the expected level of driver awareness and engagement. Reference to relevant guidance, best practices, industry standards and well-established design principles is also possible (e.g., ISO 9241 "Ergonomics of human system interaction").

Combined and redundant auditory and visual elements should be implemented in prominent and easily understandable ways for the most relevant information that needs to be provided to the user, e.g., takeover requests. A proper description should be provided.

The applicant should also describe the methods and measures put in place in order to monitor and correctly evaluate the driver status, relevant to both DDT and possible fall-back requests. The special provisions implemented to account for users that may not be receptive shall be described as well.

The applicant should also provide descriptions, models, schemes and graphical representations of the information provided to the user in every mode of operation; namely: Normal Operation, fall-back request, approaching ODD boundaries, Emergency Operation, Emergency Manoeuvre, Incidental Conditions, etc.

6.7. Protection against Simple Unauthorized Activation/Operation and Interventions

This section should describe the measures adopted to prevent the attempt to force the ADS to operate in not allowed conditions and modify the manufacturer's conditions.

The subject of this section is constituted by:

a. Measures and methods adopted to prevent any inadvertent or intentional actuation of the ADS by the user bypassing the controls of the ADS (e.g., trying to limit access to ADS options).

b. Measures and methods adopted to identify and avoid the modification of elements of the ADS by the user (e.g., modification of the sensors).

6.8. Verification and Validation by the Manufacturer

The manufacturer must describe the methodology used to prove the safety of the vehicle. Both verification and validation techniques must be included. This section includes:

a. Description of the adopted approach.

b. Identification and selection of scenarios.

c. Description of the used methods and tools (software, test machines, others) and tools/tool-chains for validation.

d. Description of the results.

e. Uncertainty of the results.

f. Interpretation of the results.

g. Assessment of the results including the requirements to be met by design.

Performed testing should be addressed explicitly.

The description of HMI testing, verification and validation processes (e.g., empirical studies, simulations, test drives, road testing) should also be included in this section.

The means implemented to protect against simple unauthorised activation/operation and interventions into the ADS should also be verified and validated and described in this section

~~7. Verification and Test by the Authorities~~

~~Additional independent testing will be performed by the Authority as part of the Type Approval verifications after the Audit & Assessment phase.~~

~~The applicant must leave this section empty as it will be compiled by the Authority~~

~~7.1. Verification of the Safety Functions of the ADS~~

~~The safety functions of the ADS are described in the previous sections. The regulatory authority will check the behaviour of the ADS as declared by the manufacturer.~~

~~7.2. Examples Analysis for checking the ADS Reaction under the Influence of a Failure or an Operational Disturbance, Emergency Conditions and Boundary Conditions~~

~~The subject of this section are results from tests related to failures and other limiting conditions for the ADS (e.g., operational disturbance, emergency conditions, limits of ODD boundaries).~~

8. Data Storage System

Learning from in-use data is a central component to the safety potential of ADS: lessons learned from a crash involving a single AD could lead to safety developments and subsequent prevention of that crash scenario in other ADSs. On the other side, in order to

identify legal liability in case of crash or traffic rules infringement, the responsibility for the control of the DDT between the ADS and the human driver should be uniquely identified at every moment.

In this section, the applicant should provide evidence of the methods and means used to fulfil the legislative requirements related to the aspects described above, through the implementation of the Event Data Recorder (EDR) and Data Storage System for Automated Driving (DSSAD) onboard the vehicle.

8.1. Type of Data Stored

For each data element recorded, the time-history data and format should be described, including information on the filtering process – if applicable – performed either during the recording phase or during the data downloading phase.

8.2. Storage Location

The storage location should be described, be it on-board the vehicle or through cloud connectivity to a remote server, including system storage capabilities, capability to record data during a crash event (e.g., providing information on resistance to high decelerations and mechanical stress of a severe impact), data survivability after a crash event, trigger condition to initiate the data storage (if applicable) and means to prevent and/or notify to the user possible malfunctions.

8.3. Recorded Occurrences and Data Elements

The applicant should provide details about all the data elements recorded during vehicle operation, whether on a mandatory or voluntary basis, together with information on the recording interval time, data sample rate (samples per second), minimum range, accuracy and resolution. The purpose of the data element collected should also be clarified, be it to satisfy legislative mandatory requirements, voluntary requirements or as source of additional information. Distinction should also be made between EDR and DSSAD data recordings.

8.4. Means to Ensure Data Security and Data Protection

This section should report about means implemented by the manufacturer to ensure that recorded data are appropriately protected from unauthorised access or use, according to the data protection legislation into force, including post end-of-life data management and security. Information on data management by the applicant during the whole vehicle life cycle should also be provided, including the eventuality of discontinued production of the vehicle or of the Company business.

8.5. Means to Access the Data

The applicant should describe the tool(s) that can access and retrieve the data stored on-board the vehicle in case of crash event and granting data protection and security requirements. In case data recorded are stored in a remote server through cloud connectivity, the means and tools to access the data remotely should also be described.

9. Cyber Security

The Regulation into force mandates process audit of the manufacturer’s cyber security and Software Update (SU) management system. It also establishes the testing requirements to verify that the design of vehicle architecture, the risk assessment procedures, and implementation of cybersecurity controls were executed correctly. This section is dedicated to the description of how those aspects are managed by the applicant. A summary of the

evidence provided to comply with the cybersecurity regulation requirements might be presented. Reference to additional relevant codes, regulations and standards might also be included.

9.1. General Description of the Cyber Security and Software Update Management Scheme

The manufacturer should describe in this section the cybersecurity and Software Update Management System put in place to comply with legislative requirements. The following sections will address how the management system processes are implemented and applied to the vehicles on-road.

9.2. General Description of the Different Risks and Measures put in Place to Mitigate Risks

This section focuses on methods and measures put in place by the manufacturer to protect the vehicle against risks identified in the vehicle risk assessment. The applicant should provide a description of the process adopted for risk management, starting with the identification of objectives, then risk identification and assessment, selection of risk response, implementation of risk response, monitoring and reporting. The identified risks and mitigation measures should also be discussed, including identified secondary risks and assessment of the residual risk. The applicant should also describe the approach adopted for periodic revision and update of risks

9.3. General Description of the Update Procedure

The applicant should describe in this section the software update procedure put in place to comply with the legislative requirements, in particular for what concerns: the SU delivery mechanism, software identification, vehicle readiness for SU, measures to ensure safe execution and function restoration in case of failure, information to the users. The description of the approach adopted to ensure that additional safety risks due to SU are avoided should also be part of this section (e.g., a software failure due to a faulty software update in functions related to braking should not generate critical safety risks).

10. Information Provisions to Users

The applicant should describe the methods and measures (e.g., communications, tests, courses, trainings, certifications, signals) put in place in order to inform the user about its responsibilities and tasks during the DDT, transition demands and any other applicable conditions.

Distinction shall be made between information provided to the owner and to the users.

10.1. Model of the Information Provided to Users

The applicant should provide models of the information given to inform the user about its responsibilities and tasks during the DDT, transition demands and any other applicable condition.

The models may include written communications, tests, courses and trainings materials provided to the users, but also signals, auditory and visual elements when on board.

10.2. Extract of the Relevant Part of the Owner`s Manual

The applicant should provide extracts of the owner’s manual relevant to provide evidence of the information given to the owner.

ANNEX I. Applicable Regulations, Codes and Standards

A comprehensive list of applicable Regulations, Codes and Standards should be provided in this Annex and referenced to where appropriate. If these regulations, codes and standards have not been prescribed by the regulatory body, a justification of their appropriateness should be provided. Any changes made to or deviations from the requirements for the design should be clearly stated, together with the way in which they have been addressed and justified.