Harmonised European Solutions for Testing Automation Road Transport

HEADSTART D3.3 Assessment criteria of CAD functionalities for consumer testing and type approval

Work package	WP3: Procedures, environments and tools
Task	Task 3.3: Assessment criteria definition
Deliverable Lead	**TNO**
Authors	Andrea Steccanella (Fiat Research Center), Athanasios Ballis (ICCS), César Elpuente (IDIADA), Giulia Morandin (IDIADA), Laura Sanz (IDIADA), Marta Tobar (IDIADA), Oriol Flix (IDIADA), Valerio Liga (IVECO), Gerben Feddes (RDW), Jacco van de Sluis (TNO), Jeroen Broos (TNO), Sjef van Montfort (TNO), Bernhard Hillbrand (Virtual Vehicle), Joaquim Castella Triginer (Virtual Vehicle), Patrick Weißensteiner (Virtual Vehicle)
Dissemination level	Public (PU)
Status	Draft
Due date	31/03/2021
Document date	31/03/2021
Version number	1.0
	This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 824309.

PARTNERS

Disclaimer:

Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Revision and history chart

Version	Date	Main author	Summary of changes
0.1	16/12/2020	Jeroen Broos (TNO), Sjef van Montfort (TNO)	Draft outline
0.1.1	01/03/2021	Andrea Steccanella (Fiat Research Center)	*Positioning* section added
0.1.2	01/03/2021	Andrea Steccanella (Fiat Research Center), Valerio Liga (IVECO)	*Technology developers* section added
0.1.3	01/03/2021	Jacco van de Sluis (TNO)	*Communication V2X* section added
0.1.4	01/03/2021	César Elpuente (IDIADA), Marta Tobar (IDIADA), Oriol Flix (IDIADA), Gerben Feddes (RDW)	*Approval* section added
0.1.5	03/03/2021	Jeroen Broos (TNO), Bernhard Hillbrand (Virtual Vehicle), Patrick Weißensteiner (Virtual Vehicle)	*Assessment criteria* section added
0.1.6	04/03/2021	Athanasios Ballis (ICCS), Joaquim Castella Triginer (Virtual Vehicle)	*Cybersecurity* section added
0.2	05/03/2021	Jeroen Broos (TNO), Sjef van Montfort (TNO)	Version with all individual inputs combined
0.3	10/03/2021	Jeroen Broos (TNO), Sjef van Montfort (TNO)	Update for internal review based on task lead review
0.4	17/03/2021	André Wiggerich (BASt), Oliver Bartels (BASt), Anders Thorsén (SAFER), Martin Skoglund (SAFER), Rickard Häll (SAFER)	HEADSTART internal peer reviewed
0.5	24/03/2021	All	Inclusion of peer review feedback
0.6	24/03/2021	Sjef van Montfort (TNO)	Cleaned document
1.0	29/03/2021	Álvaro Arrúe (IDIADA)	Coordinator check. Final submitted version

Table of contents

Index of figures

Index of tables

Glossary of terms

The HEADSTART's proposed glossary definition below are the most relevant terms in this report and mainly based HEADSTART deliverable D2.1 Common methodology for test, validation and certification [1], which can also be found on the HEADSTART website [2].

Term	Description
Accident	Any unplanned event that resulted in injury or ill-health of people or damage or loss to property, plant, materials or the environment or a loss of business opportunity
Attack	Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset
Communication (V2X)	*HEADSTART Key Enabling Technology (KET):* The passing of information from a vehicle to any entity that may affect the road user (e.g. vehicle) and vice versa
Concrete scenario	Parameterised model of the time sequence of scenes (logical scenario) which begins with an initial scene and defined point in time; the behaviour of the main actor (vehicle under test) is not further specified.
Cybersecurity	*HEADSTART Key Enabling Technology (KET):* Cybersecurity is the protection of connected systems including hardware, software and data from internal and external attacks carried by malicious entities with or without authorization.
DDT – Dynamic Driving Task	All of the real-time operational and tactical functions required to operate a vehicle in on-road traffic, excluding the strategic functions such as trip scheduling and selection of destinations and waypoints, and including without limitation: 1. Lateral vehicle motion control via steering (operational); 2. Longitudinal vehicle motion control via acceleration and deceleration (operational); 3. Monitoring the driving environment via object and event detection, recognition, classification, and response preparation (operational and tactical); 4. Object and event response execution (operational and tactical); 5. Manoeuvre planning (tactical); and 6. Enhancing conspicuity via lighting, signalling and gesturing, etc. (tactical).
Driver takeover	Action by the driver to regain manual control of the vehicle
Ego-vehicle	The Ego-vehicle is the automated vehicle from whose perspective the traffic situation is viewed. The data recorded by the ego-vehicle through its sensors describes the traffic situation from its perspective relative to its own condition.
Field testing	*HEADSTART test method:* All types of testing on public roads, with real elements (components, actors and environment), a real system and a real-world high level of variability.
Functional scenario	A functional scenario is a temporal sequence that describes one of the behaviours of a system during a specific use case, with a nominal scenario and alternative scenarios. It is described in a linguistic way or with a structured language. Functional scenarios are derived from driving functions. They are used to describe the use case at a high level (higher than logical and concrete scenarios).
Harm	Physical injury or damage to the health of persons
Hazard	Source of potential harm
Highway pilot	*HEADSTART use case:* The Conditional (SAE Level 3) or Highly Automated Driving (SAE Level 4) in non-congested conditions, on highways and other structurally separated roads, with a speed range of 30 km/h to 130 km/h
Logical scenario	Beginning with an initial scene, a model of the time sequence of scenes whose parameters are defined as ranges; at a defined point in time, the behaviour of the main actor (vehicle under test) is not further specified.

Manoeuvre	Physical movement of an actor in a scenario
ODD – Operational Design Domain	The specific conditions under which a given driving automation system or feature thereof is designed to function, including, but not limited to, driving modes.
Platoon	A group of two or more automated cooperative vehicles in line, maintaining a close distance, typically such a distance to reduce fuel consumption by air drag, to increase traffic safety by use of additional ADAS-technology, and to improve traffic throughput because vehicles are driving closer together and take up less space on the road.
Positioning	*HEADSTART Key Enabling Technology (KET):* The acknowledgment of the spatial position of an asset in time, involving in autonomous vehicles relative positioning (for obstacle avoidance or precise guidance with respect to the road markings) and absolute positioning (for retrieving from the digital map the information needed for the navigation).
Proving ground testing	*HEADSTART test method:* All types of testing on proving ground with controlled environment and no virtual elements (components or actors and environment).
Risk	Combination of the probability of occurrence of harm and the severity of that harm
Safety	This is freedom from unacceptable or absence of unreasonable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment.
Safety case	Argument that the safety requirements for an item are complete and satisfied by evidence compiled from work products of the safety activities during development.
Scenario	Abstraction and general description of a temporal and spatial traffic constellation without any specification of the parameters.
Scenario parameter	A scenario parameter is a value used to describe the characteristics of a scenario (e.g. minimum TTC, average speed, minimum distance and trajectory).
Security	State of relative freedom from threat or harm caused by deliberate, unwanted, hostile or malicious acts
Severity	The severity of the accident describes the injuries to the vehicle occupants and other road users and damage to the vehicle (from material damage to fatal accident)
System	Set of components or subsystems that relates at least a sensor, a controller and an actuator with one another. Note 1 to entry: the related sensor or actuator can be included in the system, or can be external to the system.
Test case	The set of conditions that are applied to test a function or system
Threat	Potential cause of an unwanted incident, which may result in harm to a system, individual or organization
Traffic jam chauffeur	*HEADSTART use case:* Conditional automated driving in traffic jams up to 60 km/h on motorways and motorway similar roads.
Truck platooning	*HEADSTART use case:* A group of two or more automated cooperative trucks drive together in a line, maintaining a close distance.
Type approval	The procedure whereby an approval authority certifies that a type of vehicle, system, component or separate technical unit satisfies the relevant administrative provisions and technical requirements.
Unreasonable risk	Risk judged to be unacceptable in a certain context according to valid societal moral concepts

Use case	Specification of a generalized field of application, possibly entailing the following information about the system: one or several scenarios; the functional range; the desired behaviour; and the system boundaries. Note 1 to entry: The use case description typically does not include a detailed list of all relevant scenarios for this use case. Instead a more abstract description of these scenarios is used.
Virtual testing	*HEADSTART test method:* All types of testing with only virtual elements (components, actors and environment)
Vehicle	A machine designed to provide conveyance on public streets, roads, and highways.
Vehicle Under Test (VUT)	Scenario participant whose behaviour is of primary interest.
XiL-based testing	*HEADSTART test method:* All types of testing where virtual and real elements (components, actors and/or environment) are combined.

List of abbreviations and acronyms

Abbreviation	Meaning
ACC	Adaptive Cruise Control
ACSF	Automatically Commanded Steering Function
AD	Automated Driving
ADAS	Advanced Driver Assistance System
AEB	Autonomous Emergency Braking
AES	Autonomous Emergency Steering
ALKS	Automated Lane Keeping System
BSM	Blind Spot Monitoring
CAD	Connected and Automated Driving
CAV	Connected and Automated Vehicle
CC	Common Criteria
CEN	European Committee for Standardization
CIB	Crash Imminent Braking
DBS	Dynamic Brake Support
DDT	Dynamic Driving Task
DiL	Driver-in-the-Loop
DTLE	Distance To Lane Edge
ECU	Electronic Control Unit
EDR	Event data recorder
ELK	Emergency Lane Keeping
EMC	ElectroMagnetic Compatibility
ESS	Emergency Steering Support
EU	European Union
Euro NCAP	European New Car Assessment Programme
FCW	Forward Collision Warning
FMVSS	Federal Motor Vehicle Safety Standards
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HAL	HEADSTART Assurance Levels
HARA	Hazard Analysis and Risk Assessment
HD	High Definition
HEADSTART	Harmonised European Solutions for Testing Automated Road Transport
HiL	Hardware-in-the-Loop
HMI	Human Machine Interface
IMU	Inertial Measurement Unit
KET	Key Enabling Technology
KPI	Key Performance Indicator
LDW	Lane Departure Warning
LiDAR	Light Detection And Ranging
LKA	Lane Keeping Assist

LSS	Lane Support System
NHTSA	National Highway Traffic Safety Administration
OBU	On-Board Unit
ODD	Operational Design Domain
OEDR	Object and Event Detection and Response
OEM	Original Equipment Manufacturer
PG	Proving Ground
RSS	Responsibility Sensitive Safety
SAE	Society of Automotive Engineers
SAS	Speed Assist System
SiL	Software in the Loop
SOTIF	Safety Of The Intended Functionality
TARA	Threat Analysis and Risk Assessment
ToE	Target of Evaluation
TSF	ToE Security Functionality
TTC	Time To Collision
UN	United Nations
UNECE	United Nations Economic Commission for Europe
V2X	Vehicle to Everything
ViL	Vehicle-in-the-Loop
VRU	Vulnerable Road User
VSSA	Voluntary Safety Self-Assessment
VT	Virtual Testing
VUT	Vehicle Under Test
XiL	X-in-the-Loop (Hardware and software in the loop)

Executive Summary

This deliverable presents the work done in HEADSTART work package 3: Task 3.3 “Assessment criteria definition”.

Task 3.3 describes the assessment criteria that are part of the evaluation within the HEADSTART methodology to perform the safety assessment for a Connected and Automated Vehicle (CAV). These results will be used in HEADSTART T3.5 “Test procedure for defined use cases” to further detail the HEADSTART methodology, procedures and tools for the HEADSTART selected use cases. In HEADSTART work package 4 “Application and demonstration” the criteria will be used to apply and demonstrate the HEADSTART methodology via the different HEADSTART use cases to show its potential.

This report describes existing, current and upcoming, criteria from the HEADSTART key user groups; Approval, Consumer testing and Technology developers. The levels at which the criteria would be met (PASS/FAIL) or score a certain amount of points are not defined, but an overview of assessment criteria that can be considered for the evaluation of the HEADSTART methodology is made for a full system assessment. The existing criteria are used as a basis and additional criteria that might be needed to facilitate the HEADSTART methodology are defined. Additional criteria are related to the fact that the HEADSTART methodology is scenario-based, resulting in a large number of scenarios and test cases being evaluated. Also, the higher level of automation introduces additional requirements as it is less solution specific and individual function driven and gives room for various solutions. For example, the “avoid crash” can be achieved in multiple ways, which needs to be represented in the criteria. Each of the HEADSTART Key Enabling Technologies (KETs): Communication (V2X), Positioning and Cybersecurity is discussed individually, and potential assessment criteria are listed.

1 Introduction

1.1 The HEADSTART project in a nutshell

HEADSTART (Harmonised European Solutions for Testing Automated Road Transport) is a European project funded under Horizon 2020 Framework Programme within the call ART-01-2018 (the type: Research and Innovation action). Within HEADSTART 17 partners that are top automotive manufacturers, suppliers, test labs and researcher institutes are combining their knowledge and expertise.

HEADSTART will define testing and validation procedures for safety assessment of Connected and Automated Driving (CAD) functions including:

- important key enabling technologies (KET): Communication (V2X), Cybersecurity, Positioning
- cross-links of all test methods: Virtual, XiL-based, Proving grounds and Field (real-world) testing
- safety and security performance validation according to the needs of key user groups:
    - Testing and validation; Technology development, e.g. OEMs
    - Assessment; Consumer testing, e.g. Euro NCAP
    - Certification; Exemption and (type approval, e.g. Type approval authorities & Technical services

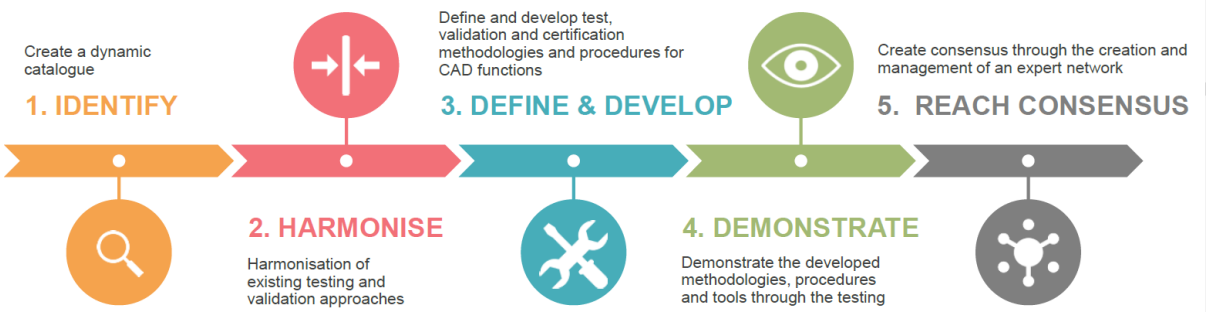

FIGURE 1 HEADSTART OBJECTIVES

The five objectives of the HEADSTART project, represented in 5 corresponding work packages, comprise:

- OBJECTIVE 1: IDENTIFY - Create a dynamic catalogue of existing methods, procedures and tools for testing, validation and certification considering multi-stakeholder requirements.
- OBJECTIVE 2: HARMONISE - Harmonisation of existing testing and validation approaches considering other industries and domains.
- OBJECTIVE 3: DEFINE & DEVELOP - Define and develop test, validation and certification methodologies and procedures for CAD building upon existing initiatives.
- OBJECTIVE 4: DEMONSTRATE - Demonstrate the developed methodologies, procedures and tools through the testing of relevant CAD use cases.
- OBJECTIVE 5: REACH CONSENSUS - Reach consensus by creating and managing an expert network of CAD testing to promote adoption of the project results considering multi-stakeholder needs.

Three additional work packages are created within HEADSTART:

- WP6 Communication and Dissemination – The objective of WP6 is to effectively spread knowledge and information about project research and innovation and secure market adoption of developed systems through promoting its work to standardisation bodies.

- WP7 Coordination and management - The main objective is to ensure the successful execution of the project through a professional and effective management and coordination, with the achievement of the project objectives. WP7 contains all the technical and administration related project management and will deal with all Data Management related issues.
- WP8 Ethics requirements - The objective is to ensure compliance with the 'ethics requirements' set out in this work package.

1.2 HEADSTART methodology

Below the HEADSTART methodology is described in outline, based on the results of the earlier HEADSTART deliverables; D2.1 [1], D2.2 [3], D2.3 [4], D3.1 [5] and D3.2 [6]. An overview of the HEADSTART methodology, also presented during the HEADSTART Mid-term event from October 2020 [7], is shown in Figure 2. Special attention is given to the three HEADSTART Key Enabling Technologies; *Positioning, Communication V2X* and *Cybersecurity*.

The HEADSTART methodology is a safety assessment methodology for Connected and Automated Vehicles (CAVs) centred around a scenario-based approached. The scenarios are abstracted from the real-world traffic situations complimented with relevant scenarios from experts and constructed scenarios. These scenarios are stored in databases (*Database + Mechanics*), where the output of the database is a logical scenario with their respective parameter distributions and exposure calculations. There are existing or germinal scenario databases like PEGASUS [8], StreetWise [9] or MOOVE [10] from different initiatives, which will be utilized in the HEADSTART methodology application and demonstration. HEADSTART will not implement its own database.

The next step (*Selection of Relevant Scenarios and Stochastic Variations*) includes the selection of relevant scenarios for the specific driving function with selecting fixed parameters within the variation and creating testable (concrete) scenarios. After the selection, the scenarios need to be allocated (*Allocation of scenarios*) among the different testing capabilities; *Virtual testing, XiL-based testing, Proving ground testing and Field testing*. Especially, the Virtual testing is an important test method, as the number of tests that can be feasibly performed is huge compared to physical testing, like Proving ground testing. For more detailed and realistic analysis it might be needed to use real physical components, for this testing on proving ground or XiL-based testing is a combination of both virtual and real components might be needed. A special part within the methodology is reserved for Field testing. Due to the fact that specific driving scenarios can hardly be staged in the field, traditional scenario-based testing is not applicable. But Field test results can be used retrospectively and scenario occurrences can be extracted post-testing.

Finally, testing results need to be evaluated with respect to assessment criteria based on the use case and the driving function specific requirements. The human capabilities and related requirements are not evaluated as part of the HEADSTART. The test and evaluation results can also become input to further improve the different steps of the HEADSTART methodology and be used as input to the databases or scenario/parameter selection. The *Cybersecurity assessment* has a special place, due to its unique requirements and approach, more information can be found in HEADSTART D3.1 [5] and D3.2 [6].

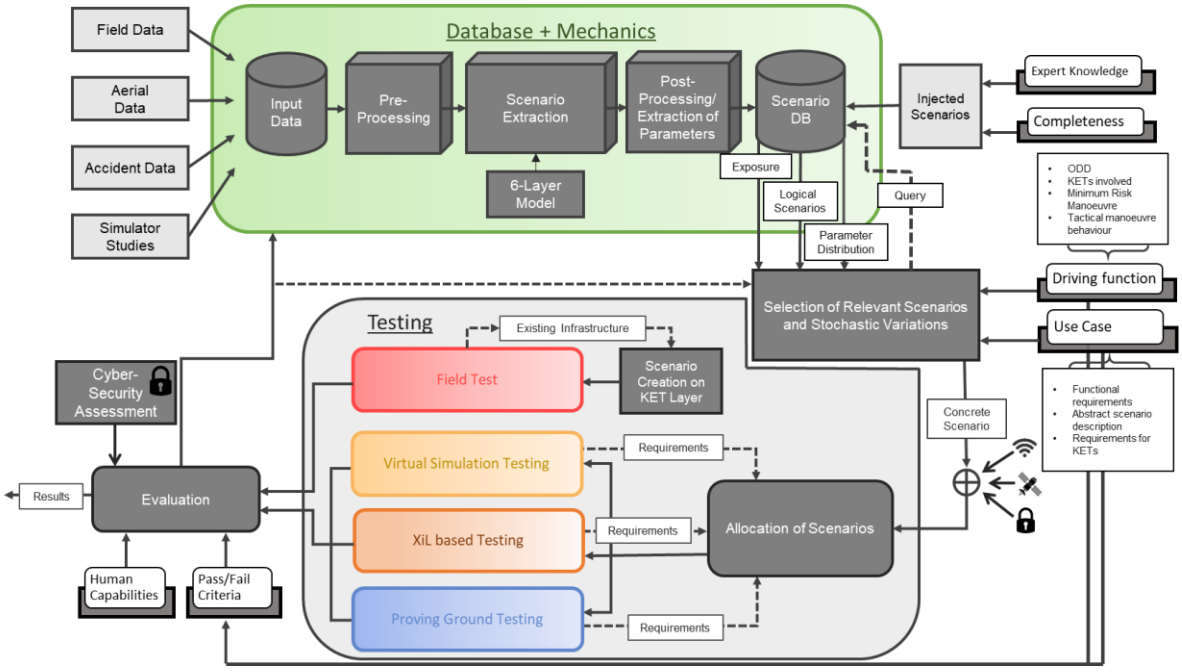

FIGURE 2 OVERVIEW ON THE OVERALL METHODOLOGY OF THE HEADSTART PROJECT

1.3 Approach and structure of the deliverable

The deliverable is structured as follows. After a general introduction to the HEADSTART project (1.1) and the HEADSTART methodology (1.2) the approach of this HEADSTART deliverable D3.3 is described in paragraph 1.3. It is not the intention of this report to define the levels at which the criteria would be met (PASS/FAIL) or score a certain amount of points, but to create an overview of assessment criteria that can be considered for the evaluation of the HEADSTART methodology.

An inventory of existing criteria for the safety assessment of Connected and Automated Vehicles (CAVs), both current and upcoming, is made. It should be taken into account that currently the assessments are mainly focussing on the system that assist the driver and are not yet automated. The criteria that are relevant for the assisted systems are often also relevant for the automated systems. The inventory is based on the three key use groups selected:

- Chapter 2 Approval Type approval and exemption
- Chapter 3 Consumer testing Consumer organisations, e.g. Euro NCAP
- Chapter 4 Technology developers Development by e.g. OEMs and TIERs

Taking in consideration the existing criteria in chapter 5 an analysis is made of additional requirements that might be required for the safety assessment. This is done by evaluation of the possible effect of the introduction of the scenario-based approach (5.1). Besides that, general safety assessment of Connected and Automated Driving (CAD) has been examined by looking at possible omissions with respect to the safe operation in paragraph 5.2. Besides that each of the three HEADSTART KETs are evaluated individually to ensure they are properly covered; Positioning (5.2.2), Communication (V2X) (5.2.3) and Cybersecurity (5.2.4). Where possible also solutions are defined to complete the safety assessment criteria required for the safety assessment of CAVs.

Finally, in chapter 5, a conclusion is drawn and implications are discussed.

During the process the three HEADSTART use cases (Highway pilot, Truck platooning and Traffic jam chauffeur) are taken into consideration and in some cases used as examples. No detailed analysis is made per individual use case as it is believed that the criteria are generic for Connected and Automated Vehicles and in general not use case specific.

2 Existing criteria from Approval

In the following chapter an overview is given of the current Type approval criteria. Also, the requirements on national exemptions in the Netherlands and Spain are discussed.

2.1 Type approval

2.1.1 Current Type approval (EU / National EU)

Europe has an EU type approval system. It provides EU countries with a common set of rules for the approval of motor vehicles and their trailers and of systems, components and separate technical units intended for these vehicles. It makes type approval compulsory for all categories of whole vehicles, including those built in several stages. It lays down a harmonized framework with general technical requirements for the type approval of new vehicles and of systems, components and technical units designed for such vehicles.

Important for assessment criteria:

- Current possibilities are only driver assist systems and optional (e.g. park assist, lane departure warning or continuous lane keeping, blind sport detection, adaptive cruise control).
- Some are safety systems and mandatory (e.g. Lane Departure Warning System and Automated Emergency Brake Systems for trucks, both discussed below). An example for assessment criteria: the system must brake three second before impact.
- New are the behaviour rules of traffic laws for driving as stated in the ALKS regulation. The ALKS regulation (UNECE R157) is described in more detail in 2.1.3.

Lane Departure Warning System (LDWS) (UN Regulation No. 130 [11])

UN Regulation on LDWS together with UN Regulation No. 131 on Advanced Emergency Braking Systems were the first steps of regulations for advanced driving assistance systems. It is important to remark that only commercial vehicles (M2, M3, N2, N3 categories) are included in the scope of both regulations. These systems were required as mandatory in the European General Safety Regulation (Regulation (EC) 661/2009 [12]) since November 2013 for new vehicle types and since November 2015 for new vehicles.

Regulation (EC) 661/2009 is currently replaced by Regulation (EU) 2019/2144 [13]), the so called New General Safety Regulation, which describes the new safety features and systems that the vehicles will have to be equipped with in the near future, in order to increase safety for all the road users and improve environmental conditions.

One of the main contents of the UN R130 is its Annex 3 where several countries declare the dimensions of the lane marking used in their respective roads. This annex is used in other ADAS/AD regulations as a reference for the test scenario.

Main objective of the UN R130 is to ensure that the system is able to warn the driver when the vehicle is leaving its lane. In order to prove the performance of the system the vehicle has to carry out a test consisting in a lane departure simulation. This test must be repeated at different lateral speeds and the Technical Service in charge of the tests has to verify that the warning system start to work before the vehicle is out of the lane.

Additionally, some verifications have to be carried out in order to verify the system is able to detect when the system is not able to warn the driver accordingly to the regulation requirements.

Advanced Emergency Braking System (AEBS) (UN Regulation No. 131 [14])

The Advanced Emergency Braking System was initially introduced in Europe by the Regulation (EU) No. 347/2012, that lately become the UN Regulation No 131. Initial cost/benefits analysis of the technical and safety aspects of the system, gave as a result that the use of this system in vehicle categories M_2, M_3, N_2 and N_3 would increase the overall safety on the road, but should be implemented with two steps in order provide lead time to all the

manufacturers for adapting their systems. Its application is mandatory for new vehicle types as from 2013, and for new vehicle registrations as from 2015 according to the General Safety Regulation (Regulation (EC) 661/2009 [12]). It is also included in the upcoming Regulation (EU) 2019/2144 [13].

The main objective of the system is to automatically detect a potential forward collision with a vehicle and provide the driver with a warning signal. In case there is no reaction of the driver, the system shall activate the vehicle braking system to decelerate the vehicle with the purpose of avoiding or mitigating the collision.

The Regulation on AEBS defines three proving ground tests where the performance of the system is evaluated:

1. Warning and activation test with a stationary target.

The vehicle approaches the stationary vehicle target at 80 km/h without any adjustment to any control. The system shall provide at least two different warnings before starting the emergency braking phase.

For this test, a reduction of the speed of at least 20 km/h shall be obtained before a collision with the stationary target. Additionally, the regulation defines the minimum required time for the different warnings, and the emergency braking phase shall not start before a time to collision higher than 3 seconds in order to avoid activations that could disturb the driver during the normal driving.

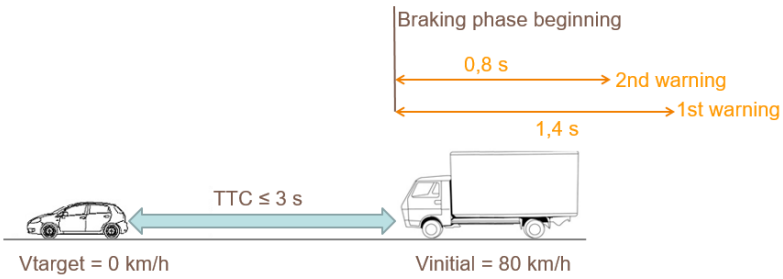

FIGURE 3. AEBS - STATIONARY WARNING TEST

2. Warning and activation test with a moving target.

For this test, the vehicle approaches at 80 km/h another vehicle (target) that is moving forward at 12 km/h. The timing of the collision warnings and the emergency braking phase is the same that prescribed for the stationary target, however, for this test an avoidance of the collision is required.

3. False reaction test.

The vehicle passes through two stationary vehicle targets at 50 km/h and the system shall not be activated during the test.

2.1.2 Current Type approval (Outside Europe)

In USA, the National Highway Traffic Safety Administration (NHTSA) is the organization in charge of issuing the Federal Motor Vehicle Safety Standards (FMVSS). These standards implement the laws of the Congress and are regulations that shall be fulfilled by the manufacturers through a self-certification procedure.

FMVSS standards are divided into three categories:

- Crash avoidance.
- Crashworthiness.
- Post-crash survivability.

The laws regarding testing and operation of automated vehicles in USA depends on the legislation of each state.

Where there are states in which legislation of automated vehicles does not exist, there are many others that are proactive and permissive. That means that the criteria and testing methods may vary a lot depending on the state. However, the U.S. Department of Transport and NHTSA issues almost every year a report with the best practices for the vehicle's assessment (both for States and manufacturers) in order to "harmonize" the criteria and the safety assessment.

The following map shows which states already have legislation on it:

FIGURE 4 US STATES WITH AUTONOMOUS VEHICLE ENACTED LEGISLATION AND EXECUTIVE ORDERS

Despite that the testing and deployment laws depends of each State, the main responsibility of the safety of the function is the manufacturer. For this reason, NHTSA issued a Voluntary Safety Self-Assessment (VSSA) guideline that is used to demonstrate to the public that entities are:

- Considering the safety aspects of CAVs.
- Communicating and collaborating with U.S. Department of Transport.
- Encouraging the self-establishment of industry safety norms for CAVs.
- Building public trust, acceptance, and confidence through transparent development and testing of CAVs.

Entities engaged in ADAS or CAV testing and deployment shall demonstrate how they address (following industry best practices, own best practices or other appropriate methods) the items explained above.

Currently, while FMVSS legislations does not exist for this kind of systems, testing validation is done through other standards that may be applicable. In the case of Lane Departure systems, is performed following requirements and test procedures of ISO 17361 [15], and NHTSA test protocols [16].

On November 2019, the NHTSA released nine draft test procedures intended to help to evaluate certain types of ADAS systems.

Lane Departure Warning System confirmation test.

Tests are conducted at one constant speed of 72 kph, two different departure directions and with three different styles of roadway markings (continuous white lines, discontinuous yellow lines, and discontinuous raised pavement makers). Each test condition shall be performed until 5 valid tests, and if more than five valid tests are performed, the pass/fail criteria shall be determined using the first five valid tests performed.

Lane Geometry	Lateral Velocity	Line Type	Departure Direction	Number of Trials
Straight	Low	Solid	L	5
			R	5
		Dashed	L	5
			R	5
		Botts Dots	L	5
			R	5

FIGURE 5. LDW TEST MATRIX

The pass/fail criteria are based on whether the LDW issues an appropriate alert during the manoeuvre. The LDW alert must occur before the lane departure exceeds 0.3 m (same criteria as UN R130).

Automatic Emergency Braking Test Procedure (for Heavy Duty)

The test protocol defines five different scenarios for the tests:

1. Stopped lead vehicle scenario: the scenario is used to evaluate the ability of the front collision warning and the automatic emergency braking of the system to detect and respond to a stopped lead vehicle in the immediate forward path.

2. Slower moving Lead vehicle scenario: used to evaluate the ability of the system to detect and respond a slower-moving lead vehicle traveling at constant speed.

3. Decelerating lead vehicle scenario: used to detect and respond to a leading vehicle which is allowing with a constant deceleration.

4. Steel trench plate false positive scenario: used to evaluate the ability of the system to suppress driver warnings and brake activations by correctly identifying a non-threatening plate.

5. Stationary vehicles false positive scenario: to evaluate the ability of the system to suppress warning and braking activation while the vehicle is travelling between two stationary vehicles.

2.1.3 ALKS type approval procedure

UN Regulation 157 [17] is the first regulation that will use a new certification approach. It is the first Regulation for a vehicle system to allow an artificial system to completely replace the driver in dedicated driving situations. While the safety of conventional systems (braking system for example), was validated through visual inspections and proving ground testing, ALKS will be assessed by using first steps in the direction of the "multi pillar approach" concept. The multi pillar approach is a proposed new validation method for Automated Driving Systems that validates the system's safety by following different steps as from the development of the system to its final deployment:

- Audit.
- Simulation/virtual testing.
- Proving ground testing.
- Real world testing.

The really new approaches in UN Regulation 157 are the open descriptions of the mandatory test cases to be fulfilled during type approval to prove the fulfilment of the requirements on the system and the general descriptions of the requirements. The test cases are not described in the old way of other UN Regulations, where every detail of any test is described and any parameter is fixed to a dedicated loading condition. The mandatory tests of Annex 5 of UN Regulation 157 only describe the relevant test scenarios with variable parameters like dimensions, speeds, timings, other road users, objects, surrounding conditions, etc. All possible test within these scenarios with different parameters can be performed by the Technical Service during type approval as long as the parameters are within the mandatory requirements written down in the main part of the Regulation. Even more, the Technical Service also is allowed to perform different scenarios, if it appears to be necessary and if they are within the specifications of the mandatory requirements and some possible additional restrictions of the individual system.

All the areas or pillars are connected in a way that results obtained during one of the phases may be used to create a testing scenario for another one to verify or validate the overall safety of the system. Today's difficulties of this approach are, that the standardised tools, methods and data for the pillar 'Simulation/virtual testing' only partly exist and need more development. For the pillar 'Real world testing' the criteria and procedures also are not clear and under development. Therefore, the UN Regulation 157 includes first steps to introduce these additional tools of simulation and real-world tests for these complex electronic systems but also rely on a complete set of proving ground tests to ensure the safety of the systems.

The first step involves the audit of the system, which includes verifying that the manufacturer has considered from the development phase, a process to ensure the functional and operational safety of the automated system. The manufacturer shall declare and document the safety concept of the system, demonstrating that the system has been developed in such a way that it is free of unreasonable safety risks to the driver or road users under faults and non-faults conditions. Additionally, the Approval Authority or the Technical Service has to evaluate the functional safety validation implemented by the manufacturer, so as to ensure the absence of unreasonable risks under hazards of the electric or electronic systems.

In terms of proving ground testing, the regulation splits the tests for the system in the following scenarios:

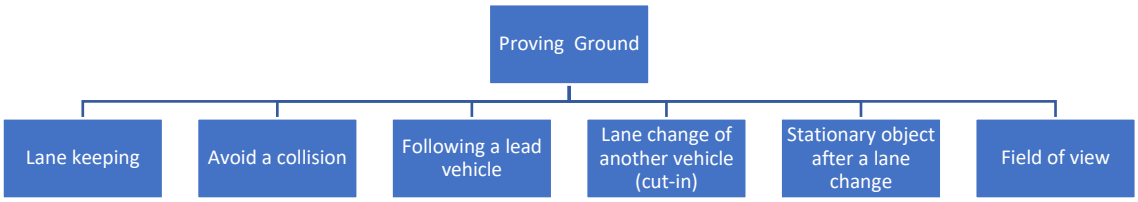

FIGURE 8. PROVING GROUND TEST SCENARIOS

Once the previous test scenarios have been successfully passed and the functional safety has been assessed, the final step after checking the general requirements of the system (activation, deactivation, override, HMI, transition demand, driver availability monitoring,…) is to test in real world conditions. The audit of the system according to the functional safety and the safety concept together with the real-world tests, enable the Technical Services to identify areas of the system that could require further assessment.

Finally, there are also requirements for Human-Machine Interface (HMI), that prevent the misunderstanding or misuse by the driver.

The test procedure includes different steps, but the purposes of this chapter is to summarize the Annex 5 test scenarios for each test during the dynamic driving task. Due to the wide range of options of the system, the Regulation does not specify the values of the testing parameters and leave the floor open to the Approval Authority and the Technical Service criteria.

The Automated Lane Keeping Systems (ALKS) Regulation [18] [17] defines safety requirements for:

- Normal driving with respecting all related traffic rules, reacting on other traffic and avoid collisions;
- Emergency Manoeuvres, in case of an imminent collision;
- Transition Demand, when the System asks the driver to take back control;
- Minimum Risk Manoeuvres - when the driver does not respond to a transition demand, in all situations the system shall minimize risks to safety of the vehicle occupants and other road users.

The Regulations states a number of essential and mandatory requirements regarding:

- System Safety and Fail-safe response:
  - General requirements
  - Dynamic driving task
  - Emergency manoeuvre
  - Transition demand and system operation during transition time
  - Minimum risk manoeuvre
- Human machine interface / operator information:
  - Driver availability recognition system
  - Activation, deactivation and driver input
  - System override
  - Information to the driver
- Object and event detection and response:
  - Sensing requirements
- Data storage system for automated systems (DSSAD):
  - Recorded occurrences

  - Data elements
  - Data availability
  - Protection against manipulation
  - Availability of DSSAD operation
- Cybersecurity and software-updates
  - Requirements for software identification

Dynamic Driving Task

The dynamic driving task of the system is checked separately for the different functional aspects of the system. The Regulation divides it as follows:

- Lane keeping test.
- Avoid a collision.
- Following a lead vehicle.
- Cut in test.
- Stationary obstacle after a lane change of the lead vehicle.
- Field of view test
- Additional verification.

If all these situations mentioned above are tested and verified by the AA/TS, it is understood that the ALKS is able to drive in a safe manner within the mandatory and its individual operation domain that might be more restricted.

- **Lane Keeping test (LK)**

The test shall demonstrate that the ALKS does not leave its lane and maintains a stable position inside its ego lane across the speed range and different curvatures within its system boundaries. This test shall be executed for at least 5 minutes, with different target vehicles as a lead vehicle, and for all the speed range of the system.

- **Avoid a collision with a road user or object blocking the lane**

The test shall demonstrate that the ALKS avoids a collision with a stationary vehicle, road user or fully or partially blocked lane up to the maximum specified speed of the system. The test is performed for different speeds and target vehicles as shown in Figure 6.

- **Following a lead vehicle**

The test shall demonstrate that the ALKS is able to maintain and restore the required safety distance to a vehicle in front and is able to avoid a collision with a lead vehicle which decelerates up to its maximum deceleration. In the picture below the relevant scenarios are depicted.

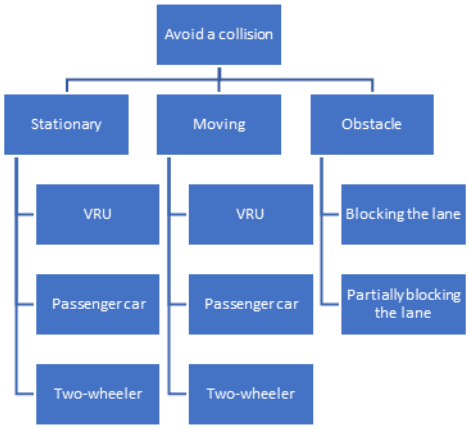

FIGURE 6 TEST SCENARIOS FOR COLLISION AVOIDANCE WITH A ROAD USER OR OBJECT IN THE LANE

- **Lane change of another vehicle into lane**

The test shall demonstrate that the ALKS is capable of avoiding a collision with a vehicle cutting into the lane of the ALKS vehicle up to a certain criticality of the cut-in manoeuvre.

- **Stationary obstacle after lane change of the lead vehicle**

The test shall demonstrate that the ALKS is capable of avoiding a collision with a stationary vehicle, road user or blocked lane that becomes visible after a preceding vehicle avoided a collision by an evasive manoeuvre.

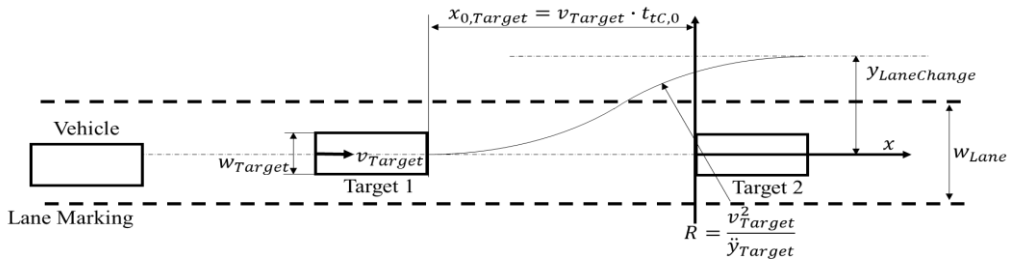

FIGURE 7 CUT-OUT PROCEDURE

- **Field of View test**

The test shall demonstrate that the ALKS is capable of detecting another road user within the forward detection area up to the declared forward detection range and a vehicle beside within the lateral detection area up to at least the full width of the adjacent lane.

- **Additional verification**

- Off mode after new engine start/run
- System can only be activated if
- Means of deactivating
- Means to override the system
- Criteria for deeming driver available
- System behaviour during a Minimal Risk Manoeuvre
- Transition demand & behaviour/escalation
- System behaviour for Emergency Manoeuvre

Additional other test cases may be assessed if it is deemed justified by the Technical Service. Some of the cases may include:

a) Y-split of highway lanes
b) Vehicles entering or exiting the highway
c) Partially blocked ego lane, tunnel
d) Traffic lights
e) Emergency vehicles
f) Construction zones
g) Faded/erased/hidden lane markings
h) Emergency/Service personnel directing traffic
i) Change in road characteristics (no longer divided, pedestrians permitted, roundabout, intersection)
j) Normal traffic flow resumed (i.e. all vehicles moving > 60km/h)

2.1.4 Upcoming Type approval (UN)

Considering the information share by the European parliament on upcoming requirements [19], several ADAS systems will be included in the new approval requirements, see Figure 8. Unfortunately, there is no information available at this moment regarding assessment criteria.

FIGURE 8 NEW UPCOMING REGULATION RELATED TO ADAS

2.2 Exemptions for testing / demonstration

In the paragraph below the criteria used in the exemption procedure of two European countries, the Netherlands and Spain are discussed. This shows examples of the criteria used, which in general are representative of the criteria used of exemptions within Europe. Exemptions under the revised 1958 agreement. Under Article 12.6: A Contracting Party applying a UN Regulation may grant an exemption approval pursuant to a UN Regulation for a single type of wheeled vehicle, equipment or part which is based on a new technology, when this new technology is not covered by the existing UN Regulation, and is incompatible with one or more requirements of this UN Regulation.

2.2.1 National exemptions: the Netherlands

In the Netherlands, there are two possibilities to admit automated vehicles to open roads:

- Exemption: for trials with vehicles where the human driver/steward is in the vehicle.
- Permit: for trials with vehicles where the human driver/steward is outside the vehicle (e.g. in a control room).

National regulation is used to restrict the admission in time and place. Within national regulation, the RDW is allowed to conduct necessary tests to make sure the vehicle is safe. For instance a Hazard Analysis and Risk Assessment (HARA, ISO 26262 [20], ISO/PAS 21448 SOTIF [21]).

The Dutch National Admittance Procedure for Connected and/or Automated Driving on Dutch public roads states a number of useful requirements regarding:

- **Vehicle**
  - a) The vehicle can be identified;
  - b) The vehicle is sound;
  - c) The vehicle is recognizable to other road users;
  - d) Measures have been taken in and around the vehicle to prevent extra personal injury to passengers;
  - e) Measures have been taken for the benefit of safety of other road users;
  - f) Safety measures have been taken for the failure and/or malfunctioning of the innovative systems.
- **Behaviour (people and environment)**
  - g) The vehicle/the driver behaves generally in a safe and responsible manner;
  - h) The vehicle/driver is predictable in its intended traffic movements;
  - i) The vehicle/driver is able to respond to other road users;
  - j) The vehicle/driver deals adequately with the different actions by other road users and traffic situations;
  - k) The vehicle/driver deals adequately with unexpected situations;
  - l) The traffic rules are observed.
- **Other**
  - m) The vehicle is protected against unintended use both via hardware and software;
  - n) Adjustments during the test do not result in unacceptable safety risks.

The National Admittance Procedure is a learning cycle:

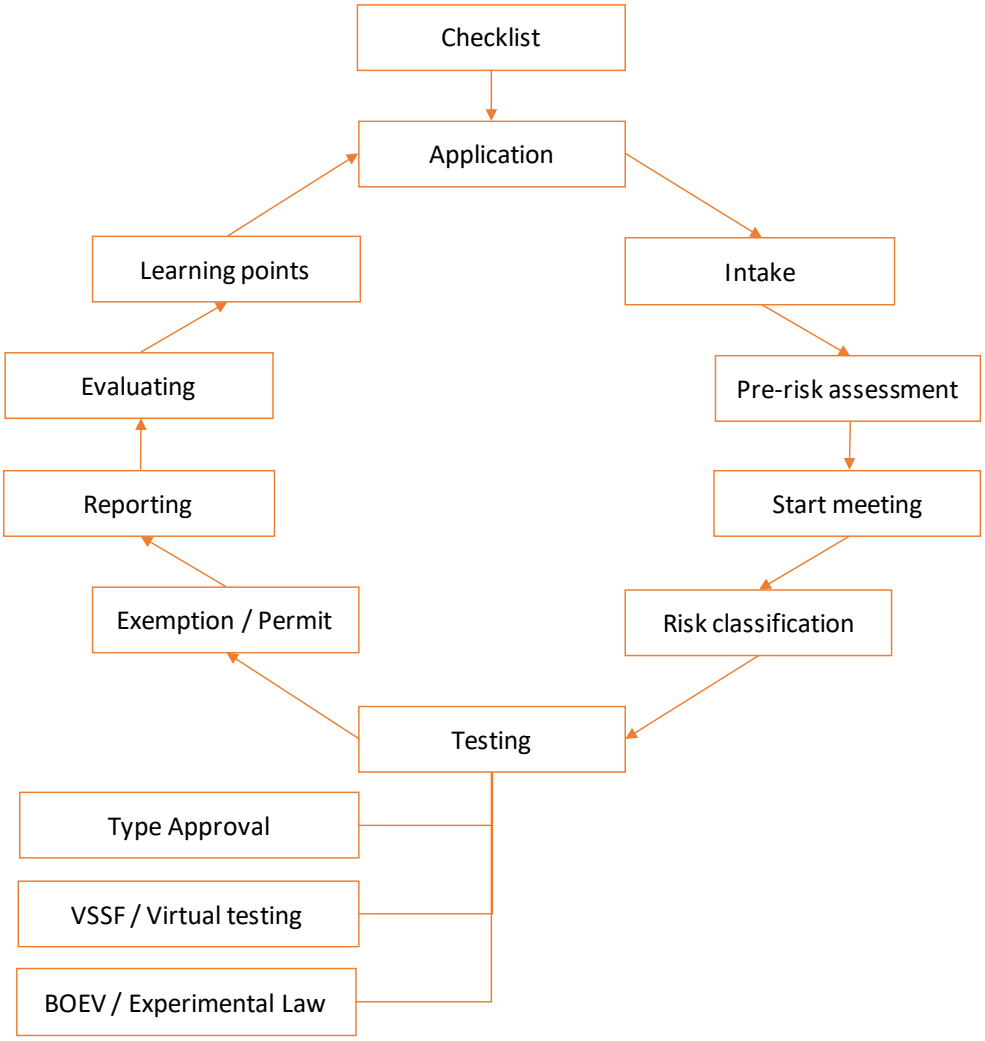

FIGURE 9 NATIONAL ADMITTANCE PROCEDURE – LEARNING CYCLE (THE NETHERLANDS)

The process steps one step deeper:

TABLE 1 NATIONAL ADMITTANCE PROCEDURE – PROCESS STEPS (THE NETHERLANDS)

NAP Process steps:		Process severity: Light	Medium	Full
1.Application				
Application form		X	X	X
Plan of approach		X	X	X
Description automated function (system, behaviour, transition of control)		X	X	X
Description required OD		X	X	X
Initial risk analysis (e.g. HARA / TARA / HAZOP / V&V / ISO 26262 / …)		X	X	X
Any previous trails		X	X	X
EMC statement		X	X	X
Proof of insurance for the trial		X	X	X
Statement of participation in research trial		X	X	X
Data Record Statement.		X	X	X
2. Intake				
Necessity established		X	X	X
3. Pre assessment				
Desk research vehicle, OD and Behaviour		X	X	X
RDW/IenW on risks and learning levels		X	X	X
4. Start meeting				
Shared understanding		X	X	X
Defined actions		X	X	X
Knowledge questions		X	X	X
5. Risk Classification				
Finalized testplan bij RDW / Decision process severity		X	X	X
6. Testing				
Initial assessment				
	Examination of the real vehicle(s)	X	X	X
Type Approval	*use applicable items from:*			
	Declare existing certificates applicable			
	Test what can be tested according type approval			
	Certificates RDW			
Software	*use applicable items from:*			
	Proces engineering: functional safety, cyber security			
	Product evaluation: software verification, system validation			
	Dynamic operations: data, HMI			
	Future autonomy: Perception, planning and control			
Virtual testing	*use applicable items from:*			
	Virtual testing (scenarios / skills)			
	Driving exam			
BOEV / Experimental law				
	Inquiry OD (road authority)			
	Inquiry SWOV			
	Physical testing proving ground (happy flow and stress)			
	Penetration testing			
	Robustness of communication			
	Physical testing onsite (in OD)			
	Indication of the maturity of the system (restrictions in time and place)			
	Testreports RDW			
7. Exemption / Permit				
Admittance & monitoring (in use / safe and predictable / degradation)		X	X	X
8. Reporting				
Safety rapport		X	X	X
9. Evaluating				
Evaluation rapport		X	X	X
10. Learning points				
Input for the learning process		X	X	X

Depending on the application, the Test-step will be light, medium of full. Because applications have unique elements, a tailor-made approach is needed. Which items to use per application will therefore differ.

During the assessment, an estimate is made of how risky the trail is and how severe the testing must be to ensure a safe trail on public roads. The assessment is an 'outside in' approach with an emphasis on the traffic situation and interaction with other road users. The technology is seen as a mean and not as a goal in itself.

TABLE 2 NATIONAL ADMITTANCE PROCEDURE – RISK PROFILE (THE NETHERLANDS)

Part:	Explanation:	Low risk	→	→	High risk
Complexity of the traffic situation (dynamic traffic image)	Dynamic description of the OD. Traffic intensity is the amount of other road users, including VRU. Also the local behavioral culture has to be taken into account.	Lots of overview Low traffic intensity Limited route choice Clear weather During the day			Little overview High traffic intensity Lots of route choices Bad weather At night
Complexity of the Operational Domain (infrastructure)	Static description of the OD. Factors include intersections, traffic lights, speed changes, possibility of oncoming traffic, quality of line markings, barriers, etc.	Completely separated lane	Simple OD	Normal OD	Complex OD
Complexity of the automated driving tasks (degree of maturity)		Driver Assist (ADAS)	Simple task (take into account own vehicle)	Difficult task (take into account other vehicles)	Complex task (anticipate in time)
Human backup: capacity of a responsible take over of the driving tasks.	Gradation can be: test engineer; experienced driver; normal driver; novice driver.	Justified	Reasonable justified	Badly justified	Not justified
Vehicle: mechanics	Classification can also be: heavy (truck, bus) versus light (passenger car). Or: transport of cargo versus transport of people.	ETG on all mechanics	ETG on critical parts of mechanics	Part ETC	No ETC (special build)
Vehicle: In-vehicle IT	can be inclusive communication to enrich the world view.	Complies with VSSF	Complies largely with VSSF	Partly complies with the VSSF	Does not comply with VSSF
Data recording					
Application: the reason of the trail		Demonstration / Field operational test	Transport of cargo	Transport of people	Transport of people
Application: quality of the information document		Good	Complete	Incomplete	Bad or not present
Application: history of earlier results from other trails.		Very useful	Useful	Badly usable	Not usable
Application: extension of earlier application		Not complex	fairly complex	complex	Very complex
Possibility to place restrictions in time and place		Quite possible	Possible	Bad possible	Not possible
Possibility to use compliance based regulation versus performance based regulation		Quite possible	Possible	Bad possible	Not possible

The scoring of the risk and the determination of the items in the test-step is based on expert judgement.

Because what to test during admittance depends on how to cope with real traffic situations, assessment criteria differ from test to test. The criteria are 'performance based' as they assess the ability to show safe and predictable traffic behaviour. Some examples:

- Start driving:
  - no hindrance to other traffic / right lane / right speed.
  - Criteria: no danger or hindrance may occur.
  - Essential: interest of other road users / viewing behaviour / giving priority.
- Driving on straight and winding road sections:

- Taking infrastructure into account / road signs / other road users / weather conditions. Observing and assessing curves / view in curves / adjust speed. No hindrance to other traffic / oncoming traffic / keep distance
- Essential: interest of other road users / viewing behaviour / giving priority / place on road / distance / speed

- Behaviour near and on junctions:
  - Interests other road users. Viewing behaviour. Giving priority. Show desirable driving behaviour (defensive and vigilant). React to traffic lights and traffic signs. Slow down, brake, stop.
  - Criteria: no danger or hindrance may occur / Can an action be done safe and responsible / Don't block an intersection / beware of vulnerable road users / correct use of the road available /keeping distance / right speed / Never without necessity / tailored to the situation.
  - Essential: Interest of other road users / viewing behaviour / giving priority / speed / reaction to lights and signs.
- Overtaking / moving sideways:
  - Obstacle detection (parked vehicles / things on the road). Being aware (road with / time needed to manoeuvre / clarity of the road / available space). Interests other road users. Viewing behaviour. Taking or giving priority.
  - Criteria: Safe and fluent.
  - Essential: Interest of other road users / viewing behaviour / giving priority / place on road.

2.2.2 National exemptions: Spain

With the aim of making compatible the tests of new Automated Driving technologies with the normal use of the conventional vehicles on open road, Spanish traffic authority "Dirección General de Tráfico " (DGT) (Traffic General Directorate) issued the Instruction 15/V-113 in November 2015 [22]. This law suffered some modifications on its annexes at the end of 2020 [23].

In order to get the authorization for the tests in open traffic the applicant must provide the convenient documentation in addition to a test report where an accredited Technical Service proves the fulfilment of the tests specified in the instruction.

In following paragraphs are described the documentation to be supplied by the authorization requester and the tests to be performed by the Technical Service. Nevertheless, an equivalent document from a competent authority of another EU Member State can be used instead the test report issued by the Technical Service. The validity of this equivalent document must be consulted with the Spanish authority (DGT).

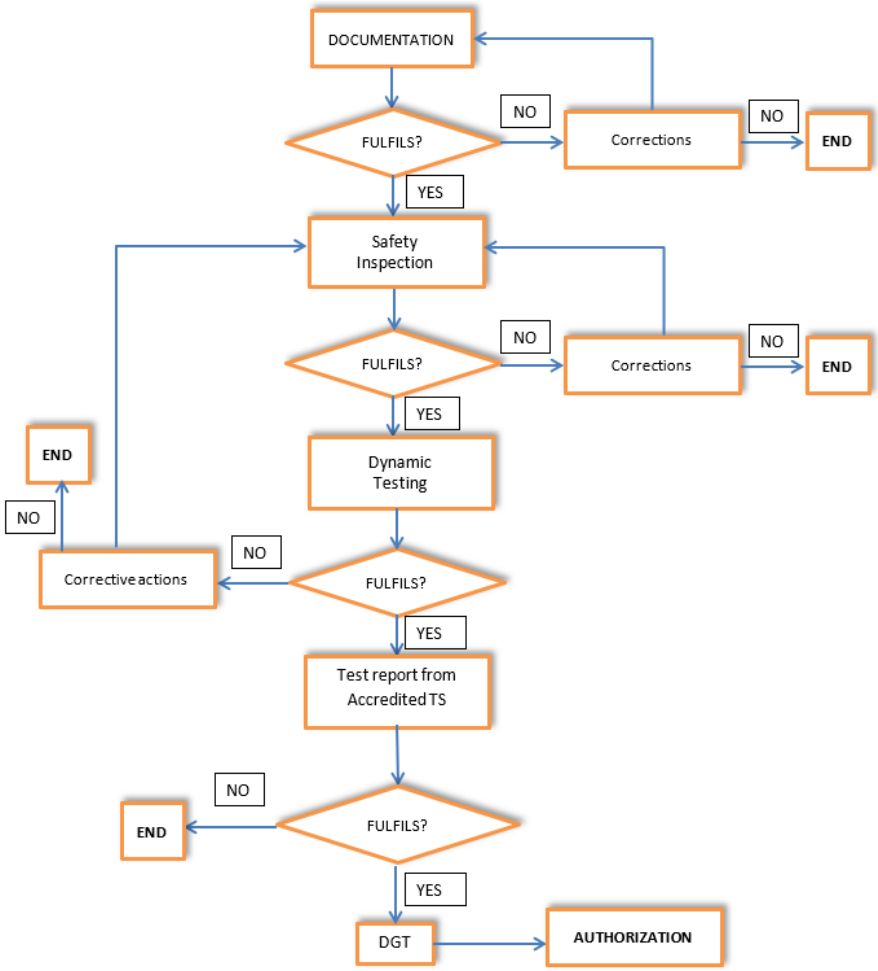

FIGURE 10 PROCEDURE FOR THE SPANISH LICENSE EXEMPTION

The Spanish instruction is aimed at regulating the granting of special authorizations to conduct tests or research trials of automated vehicles on roads open to general traffic. It states a number of useful requirements regarding:

- **Documentation**
  - Official application document
  - Proof of payment of the stablished fee
  - Test report from a Technical Service proving the safety of the vehicle during the tests in the specified scenarios
    - Simplified technical specifications sheet of the tested vehicle
    - Functional Safety Risk Assessment (by means of HARA, FMEA or equivalent method)
    - Control of software versions
    - Emergency stop and 'override' system documentation of automated system
    - Documentation of the system's functionality/design and testing scenarios
      - Description of the Automated Functionalities to be tested
      - Open road Test scenarios
      - Restricted test scenarios in case of potential risk for other road users
    - Cyber Security
    - Electromagnetic compatibility (EMC)
    - Description of the signal recognition function
- **Safety Inspection:** The Technical Service shall perform an inspection of the vehicle before the testing in order to ensure the good condition of the vehicle and its components. Additionally, this inspection will be used to identify in a unique way the vehicle to be tested in open road.
  - Identification and main features of the vehicle
  - External Inspection of the vehicle
  - Engine bay inspection in order to check possible leakages
  - Inspection of the vehicle interior
  - Wheels and wheel arch assessment
  - Vehicle underbody assessment

  A check list is available in the Instruction annexes to perform the checking in an exhaustive way
- **Dynamic tests:** These are the tests to be performed by the Technical Service in order to prove the safety of the vehicle equipped with automated technologies. In the case the vehicle is not able to perform any of these tests due to its construction features (e.g. maximum speed) an alternative test designed by the technical service should be performed. A more extensive list can be found in Annex 1.
  - Conventional (manual) driving

    The aim of these tests is to verify the proper performance of the safety vehicle systems (such as: speedometer, steering, brakes and stability control) when the vehicle is being driven in conventional mode

    To accept these tests the abovementioned systems shall work properly according to their specifications and they shall not suffer any vibration or anomalies while the vehicle driving the vehicle. The acceptation of the tests will be under the criteria of the Technical Service in charge of the authorization tests
  - Override tests:

    These tests are defined with the objective of checking the driver is always under control of the vehicle and the automated driving can be cancelled at any moment under the request of the driver. This override manoeuvre can be done by driver's actuation on the steering wheel, brake pedal or accelerator pedal. Additionally, if the vehicle is not equipped with a driver position with these controls, an emergency button must be fitted in order to interrupt the automated driving function.

    In all the three overriding tests (for steering wheel, brake pedal and accelerator) a previous manoeuvre shall be performed in order to check the system is able to keep a straight trajectory and the vehicle speed. Then when repeating the manoeuvre, an intervention on the control (steering wheel, brake pedal or accelerator) must be done by the driver, the system shall interrupt

immediately the automated driving and the vehicle shall be able to respond to the driver's input. In all the cases the driver's input must be measured and it has to be lower than a maximum allowed force.

- Longitudinal control (braking test, automated emergency braking,)
  In order to verify the longitudinal control of the system, the vehicle has to fulfil two different tests: conventional tests and automated emergency braking tests. With the first of the test, it is proved that the vehicle is able to brake effectively, and the brake system works with the same performance than in a conventional vehicle. In the second of the tests, it is verified that the system is able to detect an obstacle (other car or a pedestrian) in front of the ego vehicle.
  To prove the right working of the brake system the applicant has to perform two different tests, however by presenting to the Technical Service the vehicle braking approval according to UN Regulation No. 13. these tests can be omitted. First of the tests is to verify the performance of the braking system with the cold brakes. To check the braking performance the vehicle deceleration (MFDD) has to be greater than a minimum value, the braking distance shall be shorter than the maximum threshold and the applied force in the brake pedal shall be lower than the maximum specified in the instruction. The second of these tests is the same test but in this case the test must be performed after a controlled heating procedure.
  With regards to the automated braking, the vehicle has to perform two different tests, Car to car test and Car to VRU, in which the vehicle is driven against a target. The objective is that the system must avoid the impact with a target (vehicle or VRU) without driver's intervention
- Lateral control
  The objective of the test is to verify the vehicle is able to stay in a lane marked without any driver's input in the steering wheel. This performance has to be fulfilled for both kind of functions: Lane departure corrective function and Lane Centering function. In this second function the acceptance criteria are subject to the maintenance of the vehicle in the central axis of the marked lane (taking into account a predefined tolerance)
- Recognition and fulfilment with the traffic signs
  The technical Service shall drive the vehicle in the circuit in order to check the recognition of the signals is properly done by the system. In the instruction there are no specifications about the signals to be included in the circuit.
  The technical Service will determine the conditions of the tests depending on the circumstances under the vehicle will be tested in open road traffic.,
  If the vehicle is not able to reach any of the conditions specified in the tests above the Technical Service shall determine adapted versions of the tests included in the instruction according to the tested vehicle features and the operational design domain under the tests in open road will be performed
- Verification of the Functional Safety aspects declared by the applicant
  The technical Service shall determine the suitability of the proposed risks and its mitigations in the technical documentation provided by the applicant (see item about documentation). Additionally, the technical service shall simulate some of the risks proposed in this documentation in order to check the correct application of the mitigations in the vehicle.

2.3 Summary of existing criteria from Approval

Type approval has not provided assessment criteria for automated system (SAE Level 3 and higher) until end of 2020. Only assistance systems up to SAE Level 2 have been regulated up to this point. The ALKS regulation is the first Regulation for a SAE Level 3 system and all criteria are only performance based.

Safe operation

- The activated system shall keep the vehicle inside its lane of travel and ensure that the vehicle does not cross any lane marking.
- The activated system shall not cause any collisions that are reasonably foreseeable and preventable.
- The activated system shall comply with traffic rules relating to the dynamic driving task in the country of operation.

How to test is up to the Technical Service or Vehicle Authority using Annex 5 of UN Regulation 157.

Positioning

The ALKS states that the applicant for type approval provides an outline that includes “Perception and objects detection including mapping and positioning”. How is up to the applicant. Positioning of the vehicle on the road and determination of the positions of other road users and other relevant objects have to be accurate enough to be able to fulfil all requirements of the DDT.

Communication

Current Type approval has no definition of indicators for the assessment of CAD functionalities regarding (V2X) communication.

Cybersecurity

Current Type approval has added UN Regulation 155 on Cybersecurity. The UN Regulation provides a framework for the automotive sector to put in place the necessary processes to:

- Identify and manage cyber security risks in vehicle design;
- Verify that the risks are managed, including testing;
- Ensure that risk assessments are kept current;
- Monitor cyber-attacks and effectively respond to them;
- Support analysis of successful or attempted attacks;
- Assess if cyber security measures remain effective in light of new threats and vulnerabilities.

The Regulation text on Cybersecurity is available at UNECE website [24].

3 Existing criteria from Consumer testing

Consumer Test programmes promote the introduction of new technologies in a way that the safety benefits are realised and by checking that these technologies do not introduce new risks that may entail an impact on safety. The final goal of Consumer Testing is to raise awareness about the safety benefits of increased vehicle automation.

Currently the assessment provided by Consumer Test programmes is concerned with the safe operation of the systems and does not take into account which technologies have been used to implement the different functions.

For instance, in the case of Euro NCAP, the Key Enabling Technologies addressed in HEADSTART are not specifically considered in the Safety Assist or the Assisted Driving assessment protocols; as an example, certain assistance functions such as Speed Limit Information Function could either be provided by vehicle-integrated devices or by connectivity and this does not affect the assessment as long as safe operation is provided.

Nevertheless, Key Enabling Technologies are likely to be included as part of the assessment. In particular for connectivity, Euro NCAP's recognises the safety potential of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2X) technologies, for car occupants, vulnerable road users and powered two wheelers. To support the availability of technology on the vehicle side, the Euro NCAP roadmap for 2025 [25] considers the assessment of V2X as a tool to support and enhance important safety functions.

3.1 Euro NCAP

The New Car Assessment Programme (Euro NCAP) created the five-star safety rating system with the main objective of reducing the number of accidents and move toward vision zero. This ranking helps the consumers to compare vehicles and to identify the safest choice among the ones available on the market.

The starting point of Euro NCAP activity is the monitoring of the frequency and the nature of real-world crashes and the advancements in the technology available on the market. However, the aim of this organization is also to challenge vehicle manufacturers to offer the best possible safety as standard, protecting car occupants of all ages, gender, sizes and to also look out for other road users in traffic.

In its Safety Assist, Vulnerable Road User and Assisted Driving protocols Euro NCAP evaluates the system from the safe operation perspective.

3.1.1 Euro NCAP Rating of Active Safety technology

Every two years Euro NCAP creates new protocols that include more and more challenging test scenarios that are surrogate for critical traffic situations.

The part of Euro NCAP rating that concerns the active safety has the aim of assessing the technology designed to prevent accidents due to excessive speed, to avoid the vehicle from veering out of its lane, or to avoid collisions with other vehicles and with vulnerable road users. Additionally, Euro NCAP is taking first steps to reward system functionality during normal driving conditions that may turn into critical situations i.e. Driver Status Monitoring systems, which detect driver fatigue and distraction.

The assessment of active safety systems is included in two main areas of the Euro NCAP programme: Safety Assist area [26] and Vulnerable Road User protection [27]. This section aims to summarize the assessment criteria and main indicators used to evaluate the Active Safety functions considered in the programme.

SAFETY ASSIST

The Safety Assist score deals with 4 topics:

- AUTONOMOUS EMERGENCY BRAKING / FORWARD COLLISION WARNING (AEB / FCW) FOR CAR-TO-CAR SCENARIOS.

The system is assessed regarding how effectively the AEB system detects the oncoming hazard and decelerates the test vehicle to avoid collision or mitigate the consequence of a crash event.

Performance assessment criteria:

For AEB the assessment criteria used is the relative impact speed.

Alternatively, for certain scenarios where the warning is activated (instead of the AEB), if the performance does not result in full avoidance, the manufacturer has the option to demonstrate to Euro NCAP at the test laboratory that the Emergency Steering Support system will function to avoid the collision by steering support.

In addition to the required audio-visual warning, more advanced warning signals like head-up display, belt jerk, brake jerk or any other haptic feedback is awarded when it is issued at a TTC > 1.2s (considered this time as the minimum time required for the driver to be able to react and minimize an impact). This is only valid for cases where the AEB system is not able to fully avoid the impact at full overlap.

Occupant Status Monitoring: When the system detects a critical situation that can possibly lead to a crash, the belt can already be pre-tensioned to prepare for the oncoming impact. For this reason, Euro NCAP also rewards seatbelt reminders.

In addition to this, new technologies exist which can monitor the condition of the driver and directly or indirectly identify driving behaviours which are characteristic of an impaired driver. These are considered as a plus for the assessment.

- SPEED ASSISTANCE SYSTEMS (SAS)

Euro NCAP assesses different functions of Speed Assist Systems (SAS) that:

- inform the driver on the present speed limit;
- warn the driver when the car's speed is above the set speed threshold;
- actively prevent the car from exceeding the speed, or keep the set speed.

For systems that actively control the speed, tests are performed to ensure the system does this accurately.

Performance assessment criteria:

The Speed Assist System protocol is developed in such a way that it allows different types of Speed Assist Systems to be assessed in two areas: the functions which continuously inform the driver of the speed limit; the functions supporting the driver in his driving task by limiting or maintaining the set speed; or a combination of both.

In general, for information and warning functions the assessment is based on:

- ✓ how visible and clear the speed limit information and warning signs are for the driver
- ✓ time when speed warnings are commenced (with respect to the moment in which the vehicle speed is exceeding the applicable limit by a certain threshold)

For speed control systems the assessment is based on the following:

- ✓ time to adopt a new speed (within certain time after there is a change in the speed limit)
- ✓ the accuracy of the speed control systems.

Speed Limit Information Function

During the journey, the speed limit shall be shown using a traffic sign and shall be clearly seen in the direct field of view of the driver, without the need for the head to be moved from the normal driving position, i.e. instrument cluster or head-up display.

The speed limit information must be shown or accessible at any time with a simple operation and needs to be shown at the start of the next journey (excluding the initialization period).

The indicated speed limit information may indicate the level of reliability of the speed limit.

In the presence of conditional speed limits the system needs to either properly identify and show (for example when raining) the applicable speed limit or alternatively, needs to indicate the presence of a conditional speed limit which the system is not able to compute, in addition to the non-conditional speed limit.

Warning function:

The warning shall commence when the vehicle speed is exceeding the applicable limit by more than a stablished threshold; the warning shall be a flashing traffic sign used to communicate the speed limit or an additional visual signal adjacent to the traffic sign.

Speed control function:

The system should adopt, or offer the driver to adopt, an adjusted speed within a certain time after change in the speed limit.

After a speed control action, the stabilized vehicle speed shall be accurate enough to be within a defined speed range of the set speed.

- **LANE SUPPORT SYSTEMS (LSS)**

Euro NCAP rewards Lane Departure Warning (LDW), Lane Keeping Assist (LKA) and Emergency Lane Keeping (ELK) systems. In order to represent different traffic scenarios, these systems are tested against various types of road-markings, including solid lines and dashed lines, and in situations where the road edge is not marked by a line.

Performance assessment criteria:

The performance is evaluated by considering the proximity of the vehicle to the edge of a lane marking or road edge at the time of intervention. For scenarios in which other cars are involved, the criteria for assessment is the absence of impact. Additional points are awarded to cars equipped with a Lane Departure Warning system and a Blind Spot Monitoring system.

For the LKA and ELK functions, the assessment criteria used is the distance to the lane marking or Distance to Lane Edge (DTLE). The function must not permit the vehicle to cross the inner edge of the lane marking by a distance greater than a defined limit.

For ELK in road edges, being a more critical situation the DTLE is also used, however the threshold is more restrictive, meaning that the function must be activated before a very small part of the front wheel outside of the road edge.

For ELK tests with oncoming and overtaking vehicles, the assessment criteria used is no impact, meaning that the vehicle is not allowed to contact the overtaking or oncoming vehicle target at any time during the test.

Regarding the Human Machine Interface with Lane Support Systems, any Lane Departure Warning that issues a haptic warning before a DTLE of -0.2m is awarded when active at lateral velocities of at least 0.7m/s (these values are given as reflecting the situation in which the driver will be able to react and correct the heading of the vehicle).

The system is also awarded when the vehicle is additionally equipped with a Blind Spot Monitoring system on both sides of the vehicle to warn the driver of other vehicles present in the blind spot.

- DRIVER MONITORING

Performance assessment criteria

For the evaluation of Driver Monitoring Systems, a simplified Euro NCAP Advanced approach is used nowadays: the manufacturer must provide a dossier containing a detailed technical assessment. The dossier should contain:

- Technical detail about the system, to fully understand its functionality, relevant components, and intended availability.
- Test procedures, criteria and limits by which the performance of the system was verified.
- If available, the dossier should summarize the findings from real-world or simulated real-world evaluations.

VULNERABLE ROAD USER PROTECTION

AEB Vulnerable Road User (VRU) systems are AEB systems that are designed to brake autonomously for pedestrian and/or cyclists. For the assessment of the active safety regarding Vulnerable Road Users, two areas of assessment are considered; AEB Pedestrian and AEB Cyclists. Both are assessed in different scenarios.

- AEB Pedestrian; different scenarios are considered: pedestrian crossing scenarios, pedestrian in longitudinal direction with respect to the vehicle, pedestrian crossing when a vehicle is turning in an intersection, and pedestrian behind a reversing car.
- AEB Cyclist; several traffic situations are taken into account: scenarios with the cyclist crossing the path of the vehicle and scenarios where the cyclist is travelling in the same direction as the test vehicle.

To avoid the collisions, or to reduce their severity, the manufacturers can decide to use the AEB or they may also utilise Autonomous Emergency Steering (AES) or Emergency Steering Support (ESS). The AES intervenes only when a collision is otherwise unavoidable. A small but rapid steering input is applied, normally in conjunction with braking, to try to avoid the collision. The ESS instead exaggerates the steering action taken by the driver in the case of an emergency, to try to avoid a collision.

Assessment criteria:

For the AEB system tests (except for reverse direction and turning direction of the vehicle), the assessment criteria used is the (relative) impact speed.

For turning and reverse direction of the vehicle, the assessment is done on a pass/fail basis based on full avoidance.

For the FCW system tests in longitudinal scenarios, the assessment criteria used is the Time-To-Collision (TTC). The system is awarded when the warning is issued at a TTC >= 1.70s. Alternatively, when the FCW issued at a TTC < 1.70 s, the manufacturer has the option to demonstrate to Euro NCAP that their ESS system will provide the appropriate support to avoid the collision by steering.

3.1.2 Euro NCAP AD protocol (for Highway Assist Systems)

Besides the publication of safety ratings, Euro NCAP launched a first release about Highway Assist systems in 2018, and published a more extended test and assessment protocol in September 2020 in order to help the safe adoption of assisted driving technologies by consumers [28]. Since these systems are typically offered as an option, they are not considered as part of the Euro NCAP star rating and are evaluated with a different protocol.

This section summarizes the different categories evaluated and more relevant qualitative and quantitative indicators used in the assessment.

Assessment areas

Highway Assist systems support the driver in monotonous driving situations on motorways by providing longitudinal and lateral control of the vehicle. The longitudinal control is responsible for regulating the vehicle cruise velocity and distance to other vehicles, ensuring safety and comfort; the lateral control supports the driver to keep the vehicle in the centre of the lane. Additionally, the system may adapt the vehicle's driving speed automatically according to curves in the road, speed limits and surrounding traffic. Euro NCAP's grading of these systems depends on two main areas:

1) Assistance Competence, based on the balance between Driver Engagement and Vehicle Assistance.
2) Safety Backup.

ASSISTANCE COMPETENCE

The level of assistance provided by the vehicle must be matched by the perception of the driver and the ability of the system to keep the driver engaged and in the driving task.

The assistance competence score is based on the "*balance principle"* between vehicle assistance and driver engagement: a higher level of assistance requires a higher level of driver engagement.

In principle, the Assistance Competence score equals the Vehicle Assistance score, but only when the Driver Engagement score (at least) matches Vehicle Assistance. Where Vehicle Assistance outscores Driver Engagement, the Assistance Competence score is limited to the Driver Engagement performance.

TABLE 3 ASSISTANCE COMPETENCE: BALANCE PRINCIPLE

Driver Engagement ≥ Vehicle Assistance	Score = Vehicle Assistance
Driver Engagement < Vehicle Assistance	Score = Driver Engagement

- Vehicle assistance looks at how well the AD system supports the control of the vehicle when it comes to reacting properly to different critical and non-critical situations, and to speed control limitations that may be encountered during normal driving circumstances. The protocols here are:
    - Speed Assistance: Highways throughout Europe have changing speed limits depending on weather conditions, density of traffic or time of day. Many systems support the driver to set the speed of the adaptive cruise control (ACC) to the correct speed limit. The best systems will also support the driver to lower the speed in cases where the official maximum speed limit exceeds the safe and appropriate speed for a road, considering features such as tight bends.
    - Adaptive Cruise Control Performance: Well-developed systems will respond in due time to a variety of situations, including those that are infrequent but very critical, like cut-ins or stopped vehicle in a curve.
    - Steering Assistance: the system supports the driver to stay in lane in a sequence of bends, including steer correction or speed reduction in tight bends.

- Driver Engagement: this element refers to how well the manufacturer explains to consumers how the system works, makes clear its limitations and ensures that there is a clear communication so that the driver and the system can cooperate to control the vehicle safely. The Driver Engagement assessment consists of four elements:
  - Consumer Information: the purpose is to examine the information supplied to the consumer relating to the assistance system. The system name should not be misleading and should contain the word Assistance to clearly identify the system design limits.
  - System Status: Any system should clearly indicate its status to the driver (i.e. whether it is engaged or disengaged). This assessment is also designed to evaluate the information supplied to the driver in case the level of assistance by the system changes. This is anticipated to be visual, audible and/or haptic information or warnings.
  - Driver Monitoring: Driver Monitoring sensors should be able to determine the driver level of engagement. When a disengaged driver is detected, the system should issue a warning and should escalate this warning and finally enter an emergency mode. The systems being tested are those that can be broadly grouped together as Highway Assist systems as defined by Euro NCAP, or as SAE Level 2. This means that the driver retains full responsibility and shares control with the vehicle. Both vehicle and driver share OEDR and the driver may not perform any secondary tasks over and above those permitted during normal driving.
  - Driving Collaboration: Driver Assist systems should offer steering support while the driver maintains full control and work with the driver's intentions, not against it. When the driver steers away from the middle of the lane, for any reason, the system should stay engaged but always overridable. This assessment determines how the vehicle responds to a driver steering input, for example to avoid an obstacle within the lane of travel, when the steering assistance system is engaged.

SAFETY BACKUP

Highway Assist systems are comfort features to support the driver during a journey. Where comfort support is not sufficient to avoid an imminent collision, a safety system should take over. In Safety Backup, the extent to which the system is fail-safe is assessed, in cases where the driver has failed to react to a critical event, and how it responds in these emergency situations. Three elements are assessed in this category:

- Collision Avoidance: Where the vehicle comfort level of support would not avoid or would only mitigate an accident, the vehicle should intervene more strongly, using AEB or LSS, to try to avoid an accident in case the driver does not intervene.
- System Failure: In extreme weather conditions like heavy snow or rain or a malfunctioning sensor, it is crucial that the driver is informed and that systems are disengaged.
- Unresponsive Driver Intervention: In another unlikely event where the driver has been disengaged for a long period and the warning sequence has failed to get the driver back in the loop, the system should assume that the driver is physically unable to drive. With that assumption, the vehicle should bring the vehicle to a controlled stop, ideally on the hard shoulder, while maintaining lateral and longitudinal control. Automatic lane change in this circumstance is prohibited by regulation but would be the preferred manoeuvre above bringing the vehicle to a halt in the lane of traffic.

ASSESSMENT CRITERIA

In the AD protocol Euro NCAP covers the evaluation of the safe operation of Assisted driving technology. In this protocol, systems are generally assessed by looking at how they offer a balance between the assistance they provide and the level of driver engagement, plus how they are supported by an effective safety backup.

The tables in Annex 2 offer a summary of the assessment criteria used for the different areas and elements considered.

3.2 US NCAP

As part of the 5-Star Safety Ratings program the National Highway Traffic Safety Administration's New Car Assessment Program (NCAP) recommends that car buyers purchase vehicles equipped with crash avoidance technologies. The rate is based on these 4 features:

- Crash Imminent Braking (CIB) [29]
- Dynamic Brake Support (DBS) [30]
- Forward Collision Warning (FCW) [31]
- Lane Departure Warning (LDW) [32]

3.3 Global New Car Assessment Programme (Global NCAP)

The Global New Car Assessment Programme (Global NCAP) is a platform for cooperation among new car assessment programmes worldwide to incorporate the most important motor vehicle safety standards worldwide. Global NCAP is the umbrella body of Euro NCAP, US NCAP and the following worldwide consumer test and assessment programmes:

- Australasia NCAP (ANCAP): leading independent vehicle safety advocate in Australasia.
- China NCAP (C-NCAP); since its introduction, C-NCAP has proved to be major reference for research and development for automakers. The China NCAP protocol includes tests of Autonomous Emergency Braking and Forward Collision Warning system in Car-to-Car front to rear collision of vehicle. 3 scenarios are considered: stationary, moving and braking, with similar procedures to the Euro NCAP ones. Pedestrian autonomous emergency braking system is also tested. Staring from 2020 and optional audit is performed for Lane Departure Warning, Speed Assist System and Blind Spot Detection.
- ASEAN NCAP: New Car Assessment Program for Southeast Asian Countries.
- IIHS/HLDI: the Insurance Institute for Highway Safety and Highway Loss Data Institute, supported by U.S. and Canadian insurers.
- J-NCAP: Japan New Car Assessment Programme.
- KNCAP: Korean New Car Assessment Programme.
- Latin NCAP: New Car Assessment Programme for Latin America and the Caribbean.

Except for ANCAP and C-NCAP, many of the functions assessed nowadays in Euro NCAP have not yet been introduced as part of the roadmap of the mentioned programmes. However, for the functions already introduced the assessment criteria concepts are very similar.

3.4 Summary of existing criteria from Consumer testing

In the tables below a short summary of the existing criteria from the key use group of consumer testing is provided.

TABLE 4 SUMMARY OF ASSESSMENT CRITERIA FROM CONSUMER TESTING (SAFETY)

Safety Rating – categories		Assisted Driving assessment criteria
Safety Assist	AEB (FCW) Car-to-Car	Impact speed. Full crash avoidance. Time-To-Collision (TTC). Existence of alternative ESS system that provides the appropriate support to avoid the collision by steering.
	Speed Assist Systems (SAS)	Visibility and clarity of information. Time when speed warnings are commenced. Time to adopt a new speed (within certain time after there is a change in the speed limit) Accuracy of the speed control systems.
	Lane Support Systems	Distance to the lane marking or Distance to Lane Edge (DTLE) when system is activated Full impact avoidance Existence of Blind Spot Monitoring system
	Driver Monitoring	Technical detail about the system available Test procedures, criteria and limits by which the performance of the system was verified (i.e. real-world or simulated evaluations)
Vulnerable Road User (VRU) protection	AEB (FCW) Car-to-Pedestrian and AEB (FCW) Car-to-Cyclist	Impact speed. Full crash avoidance. Time-To-Collision (TTC). Existence of alternative ESS system that provides the appropriate support to avoid the collision by steering.

TABLE 5 SUMMARY OF ASSESSMENT CRITERIA FROM CONSUMER TESTING (ASSISTED DRIVING)

Category	Subcategories		Assisted Driving assessment criteria
Assistance competence	Driver engagement	Consumer info	Name should not make the user think that the system is capable to fully drive on its own; correct description of functionality; basic operation guide, handbook
		System status	Existence of continuous, configurable and according to guidelines system status information, per system control mode (longitudinal, lateral, both, none) Audible and/or haptic and advanced warnings to indicate a system change is awarded.
		Driver monitoring	R79 compliance confirmed; additional: existence of driver monitoring system.
		Driving Collaboration	System percentage increase in torque (compared to system off) and steering assistance accompanying the driver manoeuvre.
	Vehicle assistance	Speed assistance	Speed reduction control or information capability when approaching a traffic sign or road features (vehicle-traffic sign distance; time to pass the sign).
		Longitudinal performance	Collision avoidance / speed reduction before AEB activation.
		Steering capabilities	Capability of the system to keep the vehicle in a S-Bend road configuration.
Safety Backup		System Failure	Impossibility for the system to engage in circumstances of sensor blocked / disengagement when sensor gets blocked.
		Unresponsive Driver Intervention	Vehicle capability to maintain steering control and bring the vehicle to a controlled stop or reduce its speed to crawling speed in a driver hands-off situation. Additional scoring is reserved for a more advanced response in case of an incapacitated driver.
		Collision Avoidance	Collision avoidance, impact speed reduction (Either ACC or AEB activation). Time to collision for FCW function
			Distance to Lane Edge (DTLE) in a S-bend road configuration.
			Vehicle's ability to stop the vehicle changing lane into the path of a vehicle travelling in the adjacent lane.

4 Existing criteria from Technology developers (OEMs & TIER1s)

Connected and Automated Driving will increase the number of services for mobility, reducing at the same time the number of driving-related accidents. The new technologies introduced to deal with SAE J3016 L3 [33], and beyond, require a new set of standards and validation procedures to grant the safety of the automated driving systems for all the companies involved in the automotive industry. In the current section is reported the path that OEMs and Tier1 suppliers are following in the automation process.

4.1 Development of CAD functions

An automated driving system must satisfy the following capabilities:

1. DETERMINE LOCATION
   The system should be able to determine its location with a certain accuracy degree in relation to the ODD. The vehicle should be able to understand if it is inside or outside a location-specific ODD.

2. PERCEIVE RELEVANT OBJECTS
   The automated vehicle should perceive moving and static objects.

3. PREDICT THE FUTURE BEHAVIOUR OF RELEVANT OBJECTS
   The environment model should be able to predict future states of any object detected by the vehicle that could interfere with the DDTs of the ego vehicle.

4. CREATE A COLLISION FREE AND LAWFUL DRIVING PLAN
   The vehicle should ensure a collision-free and lawful driving policy: maintain longitudinal and lateral safe distance, in unclear situation the right of way must be given (not taken), comply with all applicable rules within the ODD.

5. CORRECTLY EXECUTE THE DRIVING PLAN
   The vehicle should follow the driving plan based on its capabilities (maximum torque for the steering wheel, minimum and maximum speed, etc.).

6. COMMUNICATION AND INTERACTION WITH OTHER (VULNERABLE) ROAD USERS
   The communication might be passive (i.e. based on the updated perception module) or active through V2X communication.

7. IDENTIFY IF SPECIFIED NOMINAL PERFORMANCES ARE NOT ACHIEVED
   The automated function must detect adverse nominal performance (i.e. unwanted human factors (misuse or manipulation), anomalies in the environmental conditions or technology failure or limitation).

The environment perception sensors are the first element of the automation chain: they should capture all the relevant information to create a world model. A single sensor is not able to provide simultaneously accurate and reliable information in all the driving condition. Therefore, it is necessary to combine multiple sensors in order to guarantee the robustness of the vehicle functions.

TRADITIONAL SENSORS ADOPTED BY THE AUTOMOTIVE INDUSTRY

The list of sensors reported below have been extensively adopted to develop SAE L0-L2 functions.

- *Camera*
  Cameras are the sensors with the highest possible extractable information from the environment in terms of obstacle classification and feature extraction of the road geometry if the resolution of the picture is high enough and the algorithm for object detection and classification is advanced, adaptive and fast. Then cameras

are very similar to human perception. Cameras have limited accuracy in the range measurements and the performances are highly affected by the weather conditions; only an indirect determination of velocities and distances is possible.

- *Radar*
  Radar has high-precision detection and measurement of moving objects and high robustness against weather conditions. A direct measurement of relative velocities and distances is possible, not only an indirect determination. Only a very limited direct classification of objects is possible. Radar has a low resolution.
- *Ultrasonic*
  Ultrasonic are accurate near-field measurements for low-speed manoeuvres. No direct classification of objects is possible with ultrasonic. Ultrasonic has a low resolution.
- *LiDAR*
  LiDAR is a high-precision measurement system for structured and unstructured elements. Medium robustness against environment conditions. The high cost of the sensor limited the spread of the technology in the past, but the sensor is reaching the automotive maturity level (in terms of performances and price) to contribute to the AD functions.

A-PRIORI PERCEPTION SENSORS

Based on the current sensor technologies the development of SAE L3 and L4 automated functions require the introduction of new input information.

- *HD Map data*
  The in-vehicle map data has never played a safety related role in the ADAS systems, but it will be crucial in the Automated Driving functions when the driver is removed from the control loop. The on-boards sensors are unable to cover all the situations that a vehicle might incur in a relatively long period. An actual HD map is able to provide a-priori information of the road that allow the vehicle to perform a driving strategy fulfilling the ODD conditions or to trigger a preventive AD state transition (i.e. minimizing the manoeuvres risk conditions). The map data can also be used as a redundant source of information to the on-board sensors. Map data must be periodically updated and validated continuously by the on-board sensors in safety related functions.
- *GNSS positioning*
  Absolute positioning contributes to the automated vehicle system safety. It is already required for some advanced assistance systems like Automatically Commanded Steering Function (ACSF) Cat. C systems. For Automated Driving, accurate GNSS positioning is crucial in order to perform the identification of the driving path on the map (i.e. the map-matching operation and the evaluation of the driving most probable path). Nevertheless, it can also be used to predict the position of other vehicles that cannot be detected by range sensors (via V2X communication) and to detect modification of the traffic rules: traffic light phases, presence of lane occlusions (traffic jams, road-works area). The absolute position must be accurate but also reliable: a time window of positioning availability and integrity must be defined at various level of accuracy.
- *Vehicle to Vehicle and Vehicle to Infrastructure communication*
  V2X communication provides information beyond the edge of range sensors. It is strictly connected to the geo-localization capability of the road actors. However, since the on-board sensors cannot validate the information exchanged between vehicles a certification of the V2X information must be provided across different OEMs.

4.2 Verification and Validation

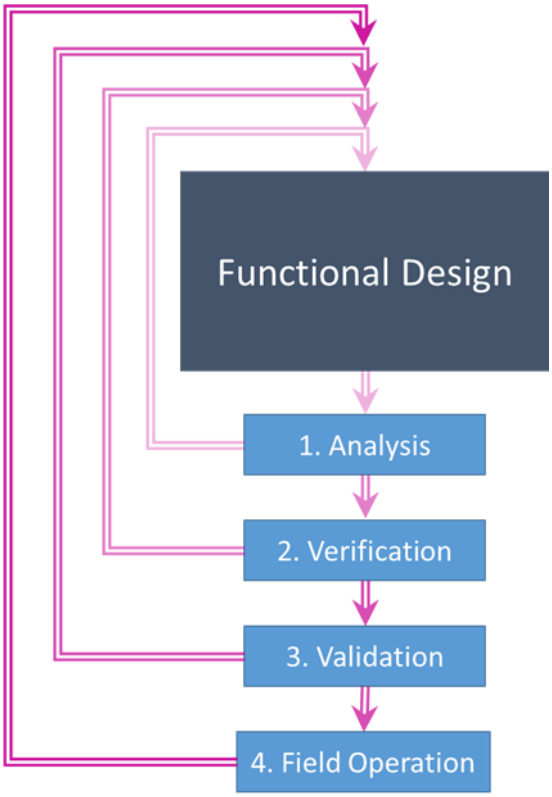

FIGURE 11 TWO PROCESS OF FUNCTIONAL DESIGN ACCORDING TO ISO/PAS 21448 SOTIF [21]

The full validation of CAD functions requires the implementation of a robust system design that complies to several standards such as the ISO 26262 [20] and ISO/PAS 21448 SOTIF [21]. Figure 11 reports the Functional Design process for the development of AD systems. This approach is valid for any SAE level, but additional complexity emerges in the development of L3 and L4 systems. This chapter focuses on the specific needs for the higher automated level functions.

The first step after the initial design is the analysis of the system; this step ensures that all the scenarios are covered and that the system behaves as expected.

The verification process checks if all the requirements are met and might lead to the need for improvements of the functional design, which might result in new verification needs. The iterative process is fundamental to increase the confidence in system design. The verification step alone is not sufficient to cover all the safety threats that might occur in real life; several unknown variables that cannot be foreseen in the design stage will affect the performance of the system.

The validation step aims to build statistical argument to confirm the safety across known and unknown situations with enough confidence. In this stage, the system is tested in scenarios that would be likely encountered in everyday driving through: virtual validation (simulation of pre-defined scenarios), proving grounds (closed-course areas with all the actors involved in scenario under control) and open-road testing. Even after this stage there is risk of occurrence of anomalies in the AD function, therefore it is necessary to perform the Field Operation testing

and to monitor the system with a post-deployment observation phase. This include the field monitoring of the system and the update of the vehicles to address failure identified after the deployment.

Figure 12 shows the main categories for the assessment of the function under test. The impact on safety is the focus of HEADSTART.

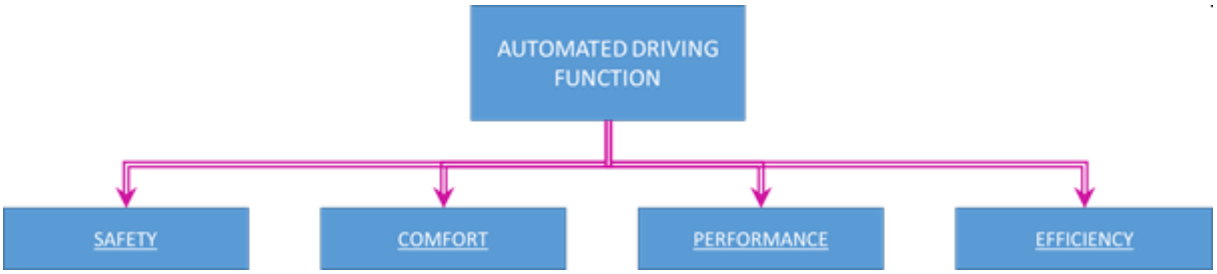

FIGURE 12 MAIN CATEGORIES FOR THE ASSESSMENT OF AN AD FUNCTION

Safety:

So far, there are no more common rules on what it means for an automated vehicle to drive safely than the general requirement to drive at least as safe as a today's human drivers do. The Responsibility Sensitive Safety (RSS) initiative by Intel/Mobileye proposes five criteria and how they can be (mathematically) assessed [34] [35]. The RSS is presented as a framework of rules, which an automated vehicle should obey. Conversely, these rules can also be used to assess the safety of such vehicles objectively. These rules (criteria) are:

- *Safe distance (don't hit the car in front of you)*
  - Like the human driver, the automated vehicle should keep enough distance to surrounding cars to have enough time and space to react on specific occasions when needed. This distance calculation should be executed for longitudinal relevant traffic participants.
- *Cutting in (don't cut in recklessly)*
  - The automated vehicle should always keep enough lateral distance to every other traffic participant. This applies particularly to cutting-in scenarios, potentially leading to dangerous braking of other vehicles if a safe distance is not met.
- *Right of way (right of way is given not taken)*
  - All the traffic rules should always be obeyed. Suppose human drivers e.g. do not properly adhere the right of way rules. In that case, the automated vehicles should give right of way rather than risk a crash because of the other vehicles traffic rule violation.
- *Limited visibility (be cautious in areas with limited visibility)*
  - The automated vehicle should be aware of situations where occluded traffic participants (especially vulnerable road users) can occur. An example of that would be crowded school drop-off zones, where the automated vehicle has to drive extra carefully and reduce its velocity accordingly.
- *Avoid crashes (if you can avoid a crash without causing another one, you must)*
  - If the automated vehicle can avoid a crash (even if it would happen because of another vehicles' mistake) it has to do it.

Safety criteria assessment does not necessarily need access to the driving function. The assessment can also be done with a black-box function. All HEADSTART testing methods can be used to test the safety criteria. However, edge cases should be performed on the proving ground or in simulation.

COMFORT:

This category's criteria relate primarily to driver acceptance values for acceleration, safety distance among road users, maximum curve speed, actuation delays, and braking behaviour. The optimal values strongly depend on the driver experience; three profiles are typically implemented in the vehicle function: conservative driver, normal driver and aggressive driver. These criteria can be tested in a driving simulator and on the real vehicle. Access to the driving function or external measuring devices are needed for the assessment. Furthermore, it depends a lot on the actual driving function, which needs to be assessed. For example, regardless of functions that are longitudinal based (e.g., lane keeping in combination with ACC) a comfort assessment is mainly based on the acceleration signal (either directly or by additional evaluation of the jerk). However, for the lateral comfort (e.g., for lane-change functions), additional signals can be relevant for the assessment (this can include the yaw angle/yaw jerk, swim angle/yerk and more).

PERFORMANCE:

This category deals with the accuracy of the implemented control algorithms. Access to the driving function is needed for the assessment. While this category is particularly of interest to the developer target group, it is not the focus of the HEADSTART project.

EFFICIENCY:

This category is also very important in the development process, but is only listed here for completeness, as this aspect is not a focus of the HEADSTART project.

NEW CHALLENGES FOR THE VERIFICATION AND VALIDATION OF SAE L3 AND L4

CHALLENGE 1: STATISTICAL DEMONSTRATION OF SYSTEM AND POSITIVE RISK BALANCE WITHOUT DRIVER INTERACTION

In SAE L0-L2 systems, the driver is responsible to supervise the vehicle controllability and is always in charge of the driving task. Thus, the validation process focusses mostly on the proper actuation of the AD functions considering the worst-case scenarios. In L3 and L4 systems, instead, the driver is assumed to be not fully alert. The reaction on unforeseen events must be handled by the automated system until the driver recovers the control[1]. This new request for the AD system greatly increases the number of possible scenarios the AD system must face and implies the need to include statistical considerations in the validation methodology.

To respond to the challenge the vehicle must be able to operate assuming no driver intervention at all[2].

[1] For SAE L4 systems, a Minimal Risk Manoeuvre should take place in case the driver does not take back the control.

[2] For SAE L3 systems, the driver should be ready to take-over within a predefined amount of time in case of any failures detected by the AD function. The transition between automated driving and human driving must be carefully monitored and tested.

The following approaches are adopted to implement the driving functions:

1. Collect data from real-world tests to cover the variety of real-world driving scenarios to develop:
    - Statistical validation of the perception in real-world tests with target sensors and survey grade equipment as ground truth,
    - Validation of the complete closed-loop system (supported by the driver in case of request by the system[3]),
    - Identification of the driving scenarios available in the ODD.

2. Implement scenario-based testing for the complete driving system and for specific elements in dedicated test platforms via:
    - Software & Hardware reprocessing validation of perception layer and sensor fusion.
    - Software in the Loop (SiL): validation of trajectory planning and control algorithms using basic sensor models.
    - Hardware in the Loop (HiL): electronic and electrical failure tests, fault injection test.
    - Proving Ground: validation of the complete system in critical (controllable) traffic scenarios.

3. Field monitoring across the entire system lifetime
    - Identify unconsidered scenarios and quantify the occurrence.
    - Increase statistical confidence level with higher statistical power.

Challenge 2: system safety with driver interaction (especially in takeover manoeuvres)

In SAE L3 and L4, the driver can take over the AD functions when the system clearly requests this to the driver, e.g. if ODD conditions are not met anymore. The human driver must receive clear unambiguous indications of why and how to take control of the system. In addition, a cooperation between the driver and AD system must take place in a well-defined amount of time. The misuse of the system by overly confident drivers must be taken into consideration in the design process and have to be addressed by the AD system with a fall-back solution like e.g. performing a Minimum Risk Manoeuvre (MRM).

These aspects are validated in the Driver in the Loop (DiL) testing and in the real-world testing. The following steps are adopted:

1. Simulation to find worst-case traffic scenarios for DiL using basic driver model.
2. DiL testing in combination with HMI warning.
3. Proving ground testing with a SAE L3 or L4 system supported by a safety driver.
4. Proving ground testing with a SAE L3 or L4 system supported by a safety driver and special vehicle equipment which allows the driver to override and inhibit the automated vehicle function at any moment.
5. Proving ground testing with a SAE L3 or L4 system driven by a representative sample of trained customers and incremental ODD scenarios (e.g. increasing velocity) until full ODD is reached.
6. Repeat 3-5 testing steps on open-roads.
7. Perform the tests without trained customers and full ODD.
8. Field monitoring of system performances in the customer fleet.

[3] The driver-automated functions must be validated also for SAE L4 systems since the driver could not react to a vehicle request or it could also interfere with the automated driving manoeuvre.

CHALLENGE 3: CONSIDERATION OF SCENARIOS CURRENTLY NOT KNOWN IN TRAFFIC

New scenarios result from both unforeseen scenarios occurring in real-world conditions and from the interaction between the driver and the AD system. Furthermore, misuse of the AD system from the driver itself and the misunderstanding of the AD manoeuvres from external (vulnerable) road users are additional risks for the AD function.

The test strategy to tackle this challenge is twofold:

- Simulation with bidirectional interaction of AD vehicles at SAE L3-L4 with other road users (including SAE L0-L2 vehicles).
- DiL and open-road testing to identify and assess the AD outcome for unforeseen scenarios.

There is not a standardized list of scenarios shared among OEMs. Simulation tools must use some tuneable parameters as defined in D2.1 and D2.2 to cover these aspects.

Challenge 4: validation of various system configurations and variants

An AD system comprises several elements that are likely to be updated over the lifetime (to solve identified failures or provide additional features). Hardware changes might occur as well from the customer (wear and tear of the vehicle, possible damages and customizations). Each system configuration needs to be verified and validated.

Full traceability along the development process is required to identify the elements and software components affected by the change.

Challenge 5: validation of systems based on machine learning

Some elements of the AD system may rely on artificial intelligence and machine learning algorithms. The verification and validation of these systems are more complex with respect to the traditional approach because the outcome cannot be decomposed in independent modules without changing the overall behaviour of the system.

In Figure 13 is reported an overview of the testing techniques adopted to test the AD components depending on the specific design of the automated driving system: multiple testing techniques must be adopted to verify and validate the entire AD system.

The verification and validation process must produce documentation to certify the type of testing and the results to achieve the vehicle homologation; OEMs and homologation authorities must jointly define the types and the quantity of tests that must be performed before launching the product. The quantity and quality of testing depends on the AD function, the vehicle architecture and the environment in which the vehicle must operate. The combination of real world and virtual testing is necessary to guarantee a high confidence in the proper operation of the function at an accessible timing and cost for the automotive industry.

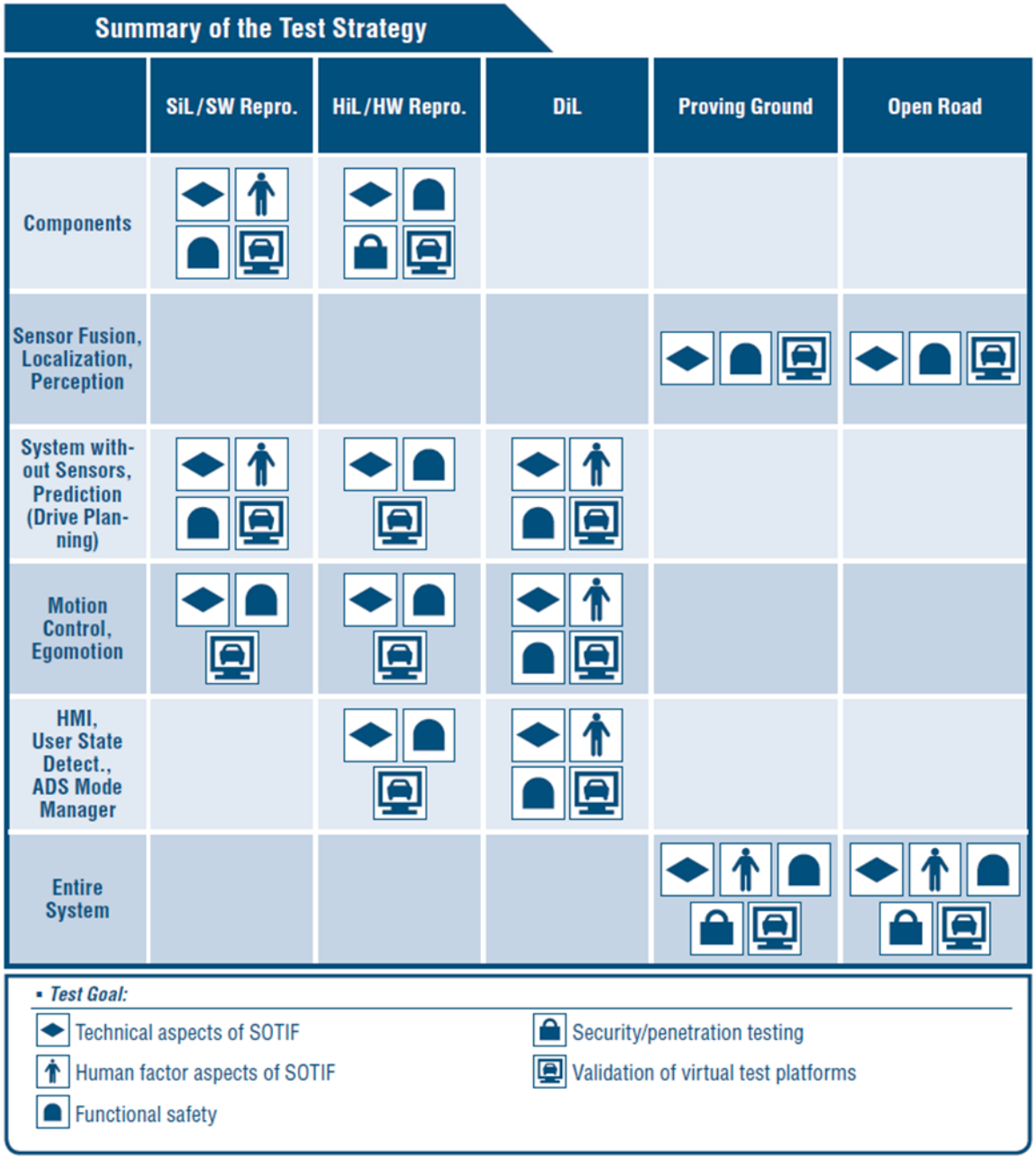

FIGURE 13 TEST STRATEGY FOR AD FUNCTIONS [36]

4.3 Specific needs for SAE L3 and L4 assessment

In this section are described the additional needs introduced by the SAE L3 and L4 functions; the following SAE L0-L2 elements must be also validated but the procedure is almost the same; therefore, the description is left out of this document.

- Processing unit:
  The typical SAE L3-L4 is more complex in respect of the lower levels since more ECUs are integrated but the validation methodology is almost the same.
- Power Supply:
  A redundant power supply is necessary to grant the proper Automotive Safety Integrity Level in accordance to ISO 26262 [20].
- Communication Network and body control:
  The communication network is more complex in respect of the lower AD levels, but the same procedures apply.
- Ego-motion:
  The ego-motion for SAE L3 – L4 should be more accurate in respect to the lower levels but the dynamic of the vehicle can be validated similarly to the lower level scenarios.
- Motion actuators and body control:
  The actuators themselves are tested in the same way for the SAE L0-L2 systems.

To address the challenges presented in the previous section the following new elements must be addressed.

Localization: including GNSS

The input to the localization system may comprise direct observation from external signals (i.e. from the GNSS system) but also local landmarks, in-vehicle sensors (i.e. wheel odometers and IMU data) and V2X. The advantage of the GNSS signal is that it is an absolute positioning technique available at a global level without error accumulation. GNSS receivers lacks accuracy (and stability) when the satellite line of sight signal is blocked by tunnels, bridges or tall buildings. IMUs, on the contrary, provide continuity in the solution for the short term but the output of the solution degrades quickly (due to the accumulation of the errors imposed by the integration of the acceleration values). The two technologies are complementary, therefore the TIER1s supplier usually combines them in a unique component. The GNSS/IMU coupling creates problems in the SiL and HiL testing. It is relatively easy to fake a GNSS trajectory because the ECU has to open an interface to receive the GNSS signals while it is complicated for the IMU since it is designed to rely on its own sensors (i.e. accelerometers and gyro-meters). For black-box systems, the positioning algorithm rejects any incoherence between IMU and GNSS trajectories.

A-Priori information: Map data

Since the world is continuously changing, the map data must be continuously updated. The map is a holistic reflection of the reality for the vehicle: inconsistences between the perceived environment and the map data could result in a failure of the automated functions. The correctness of the map data cannot be granted in all the driving scenarios therefore the vehicle must be able to identify mismatches between what the sensors perceive and what are the expectation from the a-priori source of information. The lack of knowledge of the external map has limited the use of the map data to infotainment and navigation in SAE L0-L2 systems. The testing of the map data should focus on scenarios where it is critical or less controllable for operation.

V2X perception

The capability to geo-localize the vehicles and other road anomalies enable the AD function to preventively react minimizing the risk to incur in driving conditions that exceed the driving capability. As an example, lane-closure knowledge due to road works might trigger a preventive lane-change manoeuvre which allows the vehicle to continue a safely AD L4 journey even if the roadwork barrier is not detected by any in-vehicle sensor. The main

drawback of the V2X technology is that the vehicle must trust into the information detected by sensors outside the design control of the OEM. Several standards regulate which actors can communicate, the quality of the information and the integrity of the messages; but OEMs, infrastructure operators and regulation authorities have not reached a common agreement on the minimum level of services at international level.

Human Machine Interaction

The HMI strategy totally change in SAE L3-L4 scenarios because the driver could not be ready to take control of the system. The takeover strategy must be carefully designed and tested: in DiL, proving ground and open roads. The objective is to verify the awareness of the driver to the danger and the timing necessary to take control of the car. It is important to validate these parameters with drivers that are not familiar with ADAS/AD systems.

Security by design and continuous monitoring

The SAE L3-L4 imposes higher responsibilities to the OEM in respect to any driving function previously developed. The extended number of scenarios imposes the inclusion of new information coming from signals and sensors outside the OEM design domain such as map data, GNSS signals and V2X messages. The security of the vehicle affects the entire life of the product: it starts from the design of the vehicle function and it continues with the verification and validation until the launch of the first validated release. However, the security process does not end there; the vehicles must record the entire driving situations in order to gain statistical information on the reliability of the system. The vehicles will discover unforeseen situations and new vulnerabilities from cyber-attack might occur in the life of the vehicle. It is imperative to monitor continuously the state of the vehicle and perform updates in order to ensure the proper level of safety.

4.4 Summary of existing criteria from Technology developers

The transition from SAE J3016 automation level from the level 2 to the level 3 and 4 will require the introduction of a new design of the vehicle architecture. At this AD level, the carmakers are taking a considerable responsibility for damages and injuries occurring to the driver, the passengers and other road users. The definition of the roles, as well as the homologation procedure, is crucial for the assessment of the CAD functions. The introduction of the connectivity will play an important role in the identification of the environment and the definition of the ODD enabling a certain level of automation fulfilling the safety criteria. New validation strategies must be implemented and shared among carmakers, homologation bodies and the infrastructure operator in order to boost the dissemination of these AD functions.

The verification and validation should be split in specific test goals that must be assessed with appropriate test platforms and test design techniques:

- Components: single components such as sensors or actuators are tested primarily in SiL and HiL. The calibration of the sensors and the definition of the interfaces must be validated at this stage.
- Sensor fusion, Localization and Perception: how the single components interact among each other and how the environment influence them must be verified in proving ground and open read testing. The creation of database with information on representative scenario is crucial for the development of the vehicle functions.
- Drive planning: starting from the environment model and the sensor perception it is possible to plan the vehicle manoeuvres. In this phase SiL and HiL testing play a major role in the system design. The interaction with the driver needs to be also taken into consideration using DiL tools.
- Motion control: the capabilities of the actuator to follow the planned route as well as the driver intervention must the defined and developed with SiL, HiL and DiL techniques.
- Human Machine Interaction and AD function manager: the capability of the driver and AD system to understand each other decisions must be validated with HiL and DiL techniques.
- Entire System: the goodness of the AD function must be finally validated in the real environment (in the proving ground and on public roads).

Carmakers together with the homologation bodies must define the documentation that could proof that the proper quality and quantity of tests has been reached to grant the proper safety level at the production stage.

5 Assessment criteria

This chapter discusses the assessment criteria that should be used in the HEADSTART method for safety assessment. The assessment criteria are partly based on the existing automotive safety assessment methods as discussed in chapter 2 to 4. Paragraph 5.1 discusses assessment criteria needed regarding scenario-based testing as proposed by the HEADSTART method. In paragraph 5.2 assessment criteria regarding assessment of CAD are discussed, with special attention to the HEADSTART Key Enabling Technologies: Positioning, Communication (V2X) and Cybersecurity.

5.1 Scenario-based testing

There are two main assessment criteria categories for scenario-based testing: success and metrics criteria. Figure 14 shows the categories and a list of criteria. Both categories are based on an objective observation of the executed scenario. For success criteria as well as for metrics, different context-specific key performance indicators (KPI) needs to be defined, which gather the necessary data for evaluation and comparison between expected and executed behaviour of the automated vehicle.

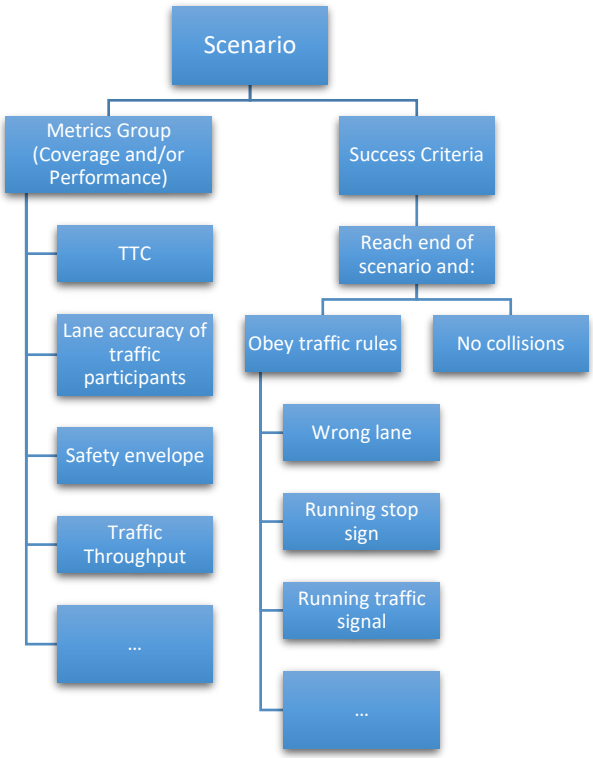

FIGURE 14 LIST OF SCENARIO-KPIS

METRICS:

The category metrics mostly deals with coverage as a measure of test completeness. Usually, coverage metrics come in two forms, structural and functional coverage. Structural coverage is mainly related to implementation; as an example, code coverage could be named. Code coverage (also often called test coverage) is a measure for the amount of source code which is executed during a particular test run. A higher test coverage therefore suggests a lower chance of undetected software-related errors in the source code. Functional coverage, however,

uses user-specified metrics to map the test plan to the intended design functionality. It is, therefore, based on the design requirement specifications and thus independent of the implementation.

Functional coverage measures what have been tested so far (in previously executed scenarios) and what parameters have been specified for a specific test run. It is, therefore, a metric that ranges across all of the executed scenarios in a test plan. A simple example of such a test coverage metric can be found in Figure 14, the time-to-collision (TTC). It could be defined in the test plan that a specific value range needs to be covered, which is then tracked by a respective KPI metric.

Another potential subcategory for metrics is regarding performance. Existing assessment methods are mostly based on accidentology. Test scenarios are based on common accidents resulting in many (severe) injuries or casualties, and/or accidents that lead to high social costs. The assessment criteria are developed to decrease the risk of (severe) injuries, casualties or to avoid accidents. By using scenario-based testing as proposed by the HEADSTART methodology test scenarios could be selected from scenario databases including observed driving scenarios. Typically, these databases contain mainly normal, non-critical, scenarios. So, not only safety critical scenarios will be selected, but also test scenarios including natural, non-critical, driving scenarios can be evaluated. These natural driving scenarios can be used to rate the automated vehicle's impact on other traffic participants, either related to one specific other vehicle or the traffic in general. The natural driving test scenarios need new types of assessment criteria, as it is not necessarily needed to use crash avoidance or injury reduction related criteria for evaluation of such test scenarios. Information regarding the typical behaviour of drivers in these normal, non-critical, test scenarios is also available in some scenario databases. The typical driver behaviour information can be compared to the behaviour of the function under test in the test scenario. So, next to current, mainly crash avoidance and injury reduction criteria, also assessment criteria can be added related to unexpected, potential safety critical, behaviour caused by the function under test. Examples of assessment criteria that assess potential safety risks for other traffic participants due to CAD behaviour in non-critical scenarios could be:

- maximum velocity difference
- speed limit offense
- max acceleration levels
- minimum time headway to other scenario actors
- lateral distance to other scenario actors

SUCCESS CRITERIA:

Success criteria directly evaluate the performance of the automated vehicles' driving function. These success criteria (or sometimes also called safety checks) mostly provide a Boolean result, which means that the result is "True" or "False". Typically, they evaluate a condition through the execution of a scenario. A few examples of such criteria are given in Figure 14. These could be supplemented by further criteria, like checking if a safe distance to the vehicle in front was kept, but also checking if misuse (usage of system beyond specified ODD) of the system is prevented. The RSS, which was presented as a framework for evaluating the driving function's safety (see chapter 4), can be used as success criteria by evaluating it objectively during a scenario's execution. In general terms, this category describes whether a collision occurred and whether specific predefined criteria/traffic rules were met or not. The criteria are characterized by the fact that they were either met or not and are therefore easier to assess. Examples would be whether traffic signs or traffic lights were ignored or whether the vehicle was driving in the wrong lane.

COVERAGE

Furthermore, a vehicle's different ODDs could be identified, and deeper analysed in how the current scenarios inside a given scenario database cover the automated vehicle's respective ODD. This could be done by separating

the given ODD into various subspaces by identifying relevant phenomena. These phenomena could be relevant either for one or for all the automated vehicle subsystems and could be categorized using functional and logical scenarios. By quantifying these phenomena, it becomes possible to apply various metrics to validate the automated vehicles' driving function. For example, analysing potential occlusions inside a given ODD and deriving logical scenarios, including parameters and ranges, each derived and executed concrete scenarios contribution to the total ODD coverage becomes quantifiable.

Furthermore, various scenario coverage statistics from databases can be included, e.g., the importance of scenarios for real-life safety based on occurrence and criticality.

5.2 CAD assessment

Next to new topics that pop-up with respect to assessment criteria due to scenario-based testing, the assessment criteria will also change due to the introduction of CAD assessment. This paragraph discusses these topics with a focus on safe operation and the HEADSTART KETs positioning, communication and cybersecurity.

5.2.1 Safe operation

In most current safety assessment methods individual vehicle functions are evaluated. Different methods are applied to evaluate lateral safety functions (lane keeping, lane departure warning, …) and longitudinal safety functions (AEB, ACC, …). However, CAD vehicle functions combine these different functions. So, for CAD vehicles not only case-by-case testing of individual vehicle functions should be applied, but the complete vehicle has to be evaluated. This will also change the type of assessment criteria. For instance, in current car-to-car AEB test methods, where the vehicle under test approaches a static, braking or slower driving target vehicle, the velocity at a time headway of 0 seconds is one of the assessment criteria. A CAD vehicle can avoid the rear-side crash with the target vehicle by braking (AEB), but also by steering around the target vehicle (AES). A factor that makes this even more complex is that the steering action of the CAD vehicle can increase the crash severity, for instance due to a crash with small overlap that results in high lateral and longitudinal acceleration combined with rotations. This is especially relevant for crashes with oncoming vehicles.

Due to the above described considerations, new types of assessment criteria will pop-up. More generic assessment criteria such "crash avoidance" should be used without considering the method that is used to avoid the crash. Furthermore, new criteria should be used to describe crash reduction as impact velocity does not cover the complete picture. The actual overlap at crash should also be included to better cover the crash severity.

Another topic that have to be covered for CAD assessment are the human factors. Especially, the system behaviour regarding transition of control, when for instance situation beyond the ODD are introduced, is of interest. Possible criteria could be time of transition. The topic of human interaction is very relevant and important, but it is out of scope of the HEADSTART project and is not discussed in more detail.

5.2.2 Positioning

At the time of writing this deliverable, there are no safety functions available that rely on absolute positioning to perform any automated driving manoeuvre. Even the most advanced vehicles rely on on-board sensors such as the camera and the radar to avoid obstacles and maintain the vehicle within the lane markers. The satellite navigation is limited to navigation and infotainment purposes. The first use of absolute positioning, linked to safety, is represented by the geo-fencing and the eCall [37] systems:

- Geo-fencing positioning: the most advanced driving assistance functions limit the automated driving capabilities to roads where pedestrians, cyclist and even vehicles driving in opposite directions are prohibited. Because of today's technical possibilities and limitations also homologated vehicles are currently allowed to drive in SAE Level > L2 only in motorway scenarios. The most convenient way to verify if a vehicle is driving on a motorway is to evaluate the absolute positioning and perform the map matching.

- eCall: from 2018 all new homologated vehicles driving in Europe must equip a telematics unit able to store the absolute position of the vehicle and automatically call rescues in case of sever accident (even if the driver is not responsive).

The positioning requirement for these applications is to perform an absolute positioning with an accuracy error equal to 15 meters (2 sigma value in clear sky conditions). In case of GNSS unavailability, the eCall system is simply disabled without any responsibility for the carmaker and the eCall norm accepts the information of the last known position. For these reasons, there is not a testing methodology specifically design to assess the performances of the positioning engine. The scenario is going to change with the advent of the SAE L3 & L4 driving systems. The availability of HD maps with road information available at lane-level, the possibility to exchange information with surrounding road actors without the need to sense them and the possibility to collect information from traffic lights (and other infrastructure events) will impose the absolute position to be part of the data-fusion algorithm implementing the safety application. The most accepted accuracy expected for SAE L3 & L4 systems is 20 centimetres (2 sigma value in clear sky conditions [38].

A challenge to the assessment of the positioning solution is the lack of a standard procedure, shared architecture or certification authorities that uniform how and in which conditions the vehicles should be able to operate. Several initiatives are going in this direction and the following European Committee for Standardization (CEN) standards have been recently published to assess the performances of the GNSS based positioning solutions for the road Intelligent Transport System (ITS):

- CEN EN 16803: Use of GNSS-based positioning for road Intelligent Transport Systems (ITS)
    - Part 1 [39]: Definitions and system engineering procedures for the establishment and assessment of performances.
    - Part 2 [40]: Assessment of basic performances of GNSS-based positioning terminal.
    - Part 3 [41]: Part 3: Assessment of security performances of GNSS-based positioning terminals.

- CEN TR 17447 [42]: Use of GNSS-based positioning for ITS - Mathematical PVT error model.

- CEN TR 17448 [43]: Use of GNSS-based positioning for ITS - Metrics and Performance levels detailed definition.

- CEN TR 17464 [44]: Use of GNSS-based positioning for ITS - Security attacks modelling and definition of performance features and metrics related to security.

- CEN TR 17465 [45]: Use of GNSS-based positioning for ITS - Field tests definition for basic performance.

- CEN TR 17475 [46]: Use of GNSS-based positioning for ITS. Specification of the test facilities, definition of test scenarios, description and validation of the procedures for field tests related to security performance of GNSS-based positioning terminals.

The idea is to define a procedure similar to the one adopted for the aeronautic industry since many problems affecting the performance and the reliability of the solution have been already faced by that sector. As an example, the necessity to fuse the GNSS solution with IMU data to compensate temporary unavailability of the GNSS signals and the need to create protection levels to ensure the level of trust in the positioning output. However, the automotive industry has its own characteristics that has to be taken into considerations:

- Different performances and integrity requirements.
- Different vehicle dynamics involved into the data-fusion algorithm.
- Different environment: open-sky conditions, urban driving and asymmetric scenarios (i.e. driving close to the mountains.
- Interference impact: the vehicles can drive in areas where interferences might occur by cyber-attackers (jamming or spoofing attacks), accidentally by malfunctioning hardware or unforeseen interferences with other legal telecommunication equipment.
- Presence of obstacles in the trajectory of the vehicles.
- Presence of obstacles hindering the GNSS signals.
- Different correction channel to receive the GNSS corrections. The most common channel is the cellular connectivity, but internet connection might not be available for the lack of cellular coverage or at the country borders. Other solutions are emerging like the satellite link connectivity or the V2X correction dissemination service.
- Different quality & cost of the positioning solution.
- Bigger flexibility into vehicle architecture and companies working into automotive industry.

In next HEADSTART activities will be validated the impact of positioning output in the Highway pilot, Traffic Jam Chauffeur and the Truck Platooning functions. The objective is not to validate the performance of the proposed demonstrators but to identify the problems affecting the positioning performances at all the production stages: Virtual, XiL-based, Proving ground and Field testing.

5.2.3 Communication V2X

Conclusions from previous Type approval (chapter 2) and Consumer testing (chapter 3) related chapters is that there are no defined indicators for the assessment of CAD functionalities regarding (V2X) communication. Although upcoming type approval regulation considers more advanced ADAS technology, these currently do not depend or include (V2X) communications. Examples of more advanced assist functions enabled by V2V communication are Cooperative-AEB system, Cooperative-ACC, both based on sharing real-time ‘intensions’ between vehicles. And possible extensions towards VRU protection, in with information is shared between pedestrians, cyclist and vehicles in a V2X communication setting. But currently basic functions related to V2X are not foreseen before 2025 on the Euro NCAP road map [25].

A basic set of standards for Cooperative Intelligence Transport Systems is available (C-ITS first release and later publications) developed by CEN and ETSI. This to enable vehicle manufacturers to communicate with each other and with the road infrastructure systems in an interoperable and technology agnostic way. Related first cooperative applications/services are more informative of nature like a Road Works Warning application. CAD like applications are considered future, or so-called 2nd day applications, of which Truck Platooning is an example (with related pre-standard studies). Listing the communication (V2X) standards that apply is considered out of scope for this section. Some more general considerations for Communication (V2X) are presented, as enabling technology for CAD functions and its related assessment.

Component level versus vehicle level assessments:

At component level the communication devices, often referred to as on-board units (OBUs), needs to conform to communication standards, adhere to EMC requirements, comply to automotive grade product design rules, etc.

But this does not consider how the communication itself is being used at application level: how the system interconnects to other in-vehicles systems, what kinds of information is being exchanged, and used for operational control, decision-making etc. So, in relation with CAD assessment, this distinction between component level and vehicle level (or application level) is important. Only at this higher level it can be determined if the communication function is a safety-critical element, or not. Is the CAD application using the communication function only for informative services (e.g. traffic information) to the driver, is it a cooperative service providing additional awareness. Or is the communication function enabling higher levels of automation, is it a safety-critical function like in a truck platooning use case.
As communication becomes a safety critical element additional system safety element and "fail-safe" behaviour becomes of interest. Is it possible to monitor system health at system level (hardware, interfaces, software) but also at CAD application level, is the communication function operating as expected and if not take care of some form of graceful degradation of the communication function, from CAD application to the sub-functions down to OBU component level. Also, there can be redundancy in the system design: multiple V2X communication technologies, multiple OBU's, multiple communication channels.
The communication protocols, the exchange of V2X messages can be reliable or unreliable by design, the low-level communication function (OBU component level) will conform to technology standards. At application layer (e.g. Truck Platooning) also mechanisms can be used to make the communication protocols (more) reliable. How to assess this at the full vehicle level. And how to do this as part of a platoon of vehicles.
Concluding that this can become a complex assessment of the CAD system with the inclusion of the communication (V2X) function.

The above considerations relate to functional requirements, system safety and fail-safe response as, so mainly the first two of the four new technical groups (as mentioned in chapter 2, draft proposal of the UNECE framework):

- Functional requirements for automated vehicles
- Validation of the driving capability of automated vehicles
- Cybersecurity and software updates
- Data Storage Systems for Automated Driving and Event Data Recorders.

Considerations related to the other two are for:
Cyber-security and software-updates:

- Requirements and considerations for the in-vehicle communication system:
    - Current standards focus at component level, not at vehicle level.
    - How to apply a layered approach: consider full chain starting at component level, sub-systems up to CAD application layer. And even consider systems-of-vehicles levels (e.g. truck platooning)
    - Special protection consideration: wireless communication increases the attack surface: it enables external remote attacks
    - How to perform/extend TARA to consider full CAD application at vehicle level (system-of-systems). And even consider multiple vehicles (e.g. Truck Platooning)
- General software update considerations apply, and:
    - Can communication software updates impact safety-criticality of the overall CAD application.

Data storage related to Communication V2X:

- What are requirements for logging of V2X messages (for both transferred as well as received messages)
- Meta data requirements: time stamps, location information (GNSS based), system information (status/health information)
- General security (Confidentiality, Integrity, Availability) and privacy considerations related to this data

Related to criteria for communication (V2X) assessment is to consider is “normal” operation versus “critical scenarios” for the communication (V2X) function evaluation. Having suitable scenarios with relevant communication ‘events’ like failures, errors, disruptions etc. (e.g. V2X message delay, drops, loss of communication) to happen in a reproduceable way. This so V2X fault-injection is controllable and can be triggered when needed during test scenario execution.

Another is to find a balance between “generic assessment scenarios” versus “application or use case specific assessments scenarios”, which needs to be highly tailored towards the used CAD application. This is especially the case with cooperative applications, with V2X exchanging operational data directly used to control the vehicle or with communication as safety-critical function. Some examples to consider are:

- Normal operation, system online, generic failure modes
- Use case specific, example communication (V2X) informative Traffic Jam Warning
- Use case specific, example communication (V2X) safety critical Truck Platooning:
    - Will a single vehicle assessment suffice for overall platooning safety or is a multiple vehicle assessment as part of a platoon needed?

5.2.4 Cybersecurity

The HEADSTART cybersecurity assessment defined in D3.2 [6] provides an approach for security evaluation. The cybersecurity evaluation presents a conformity Security Functional Requirements (SFRs) list identified in D3.2 section 8.5 based on Common Criteria (CC). Such scheme assigns an assurance level value to the usage of the HEADSTART conformity list, referred to as HEADSTART Assurance Levels (HAL). To harmonize the HEADSTART procedure, and better assess CAD functions, this is fused to the so-called HEADSTART cybersecurity parameters produced from D2.2 [3] with the HAL. Those parameters will be distributed on the existing CC classes by relative content, providing targeted options in the assessment process which would be more HEADSTART-oriented.

Most of the qualified parameters are bound to the other two HEADSTART KETs, Positioning and Communication (V2X). Even the “pure” cybersecurity ones involve s/w updates, which under the over-the-air update scheme clearly engage communication principles. In the tables in Annex 3 the parameters are matched to the functional classes covered by SFRs, identifying the HEADSTART-wise SFRs that could be of higher interest and thus be weighted more significantly than the others. The HAL value is conventionally calculated setting by setting the communication unit as ToE.

The extracted HAL values indicate how secure the specific parameters could be in the range [0,3], where the higher number sets a more secure result in our evaluation criteria. HEADSTART defines HAL to identify cybersecurity assessment criteria in vehicle level. Such value depends on the relevant interconnected parameters with the involved SFRs defined by the user groups and which, at the same time, will depend on the selected use case.

Below the main characteristics that should apply per parameter are presented:

- For the Reacquisition Time (lack of GNSS fix) positioning parameter a fail-secure characteristic for the vehicle has to be assured
- For positioning offset on spoofing attacks, the vehicle should enforce proof and non-repudiation of origin, identification, authentication and fail-secure techniques
- For the several V2X communication parameters, enforced proof and non-repudiation of origin characteristics should apply, along with vehicle data protection, identification, authentication and fail-secure characteristics
- For V2X messages missing signature, proper cryptographic support and security management should apply
- For delayed V2X messages (record and play back attacks) proper security management should apply
- For V2X communication logs security audit should apply

- For not encrypted, valid and verified V2X messages cryptographic support and privacy issues (pseudonymity, anonymity, unlinkability, GDPR) should be considered
- For embedded virus in V2X messages, security audit and management techniques should apply
- For denial of service (interference, overflow), the vehicle should enforce proof and non-repudiation of origin, identification, authentication and fail-secure techniques
- For certificate rotation, security audit automatic response and alarms, cryptographic support and operation, enforced proof and non-repudiation of origin, identification, authentication and security management should apply
- For over-the-air software updates, enforced proof and non-repudiation of origin, vehicle data protection attributes, identification and authentication should apply
- For applied illegitimate updates, security audit attributes, cryptographic support and operation, security management and revocation and fail secure characteristics should apply
- For misconfiguration or unintentional deletion of communication software part(s), fail secure and failure with preservation of secure state should apply.

The above analysis will be used for the test procedure in the selected use cases, where a relatively lower HAL value would imply the necessity for more tests towards acquiring better assurance levels.

6 Conclusions

This report describes the assessment criteria that are part of the evaluation section of the HEADSTART methodology to perform a safety assessment for a Connected and Automated Vehicle (CAV). It is not the intention of this report to define the levels at which the criteria would be met (PASS/FAIL) or score a certain amount of points, but to create an overview of assessment criteria that can be considered for the evaluation of the HEADSTART methodology. The HEADSTART methodology focusses on the assessment of the full system but is aware of the needed requirements on component and sub-system level.

The existing criteria, both current and upcoming, are evaluated and where additional criteria might be needed when applying the HEADSTART methodology this is discussed. To structure the existing criteria they are organised in separate chapters according the three key user groups defined within HEADSTART: chapter 2 Approval (Type approval and exemption), chapter 3 Consumer testing (Consumer organisations, e.g. Euro NCAP) and chapter 4 Technology developers (Development by e.g. OEMs and TIERs). In chapter 5 the additional criteria that are related to the fact that the HEADSTART methodology is scenario-based are discussed as well as the safe operation of the CAV. Special attention is given to the possible effect of the HEADSTART Key Enabling Technologies (KETs): Communication (V2X), Positioning and Cybersecurity.

The existing criteria are mainly related to assisted driving systems, especially for Approval and Consumer testing, as higher level automation systems are not yet on the market. But already with those assistance systems and the first experiences with the automated system ALKS, the current requirements show that more is needed than some simple tests to ensure the safe operations of the vehicles. The discussed national exemption procedures of the Netherlands and Spain in paragraph 2.2 show that more advanced and systems with higher level of automation complexity will need additional requirements. Also, the requirements used by technology developers listed in chapter 4 demonstrate this.

The UN Regulation 157 is the first Regulation for automated driving systems and demonstrates a new and possible way to address and solve these challenges and to phrase the new requirements needed for Automated Driving in a more general way within a Regulation.

In a scenario-based approach a large number of scenarios and test cases will be examined. This will introduce additional requirements on the evaluation. Part is related to coverage, to ensure that an agreed part of the functionality in its ODD is checked. The statistical information about the scenarios and its parameters that can be extracted from the scenario databases can be included to demonstrate the importance of scenarios for real-life safety based on occurrence and criticality.

When considering the criteria specifically focussing on the scenario-based safety assessment of a CAV a few aspects can be defined:

- General requirements on the vehicle operation:
  This are not specific criteria for scenario-based testing but are related to the general functioning of the vehicle, like normal behaviour of the vehicle without anomalies.
- Comply with traffic laws and behave social:
  The vehicle needs to obey the traffic laws, for example not exceeding the speed limit, but should also behave in a social manner with regard to the other road users.
- Vehicle position on the road and relative to other objects and road users:
  This can be either related to keeping a certain position (relative to other objects), or requirements on when warning needs to be provided.

To simplify the (current) requirements:
  - Longitudinal: distance/gap (distance, time, TCC) with respect to other object(s)/vehicle(s) or impact speed in case of unavoidable impact
  - Lateral: position with respect to lane edge or other objects

  For more advanced and systems with higher levels of automation these requirements will be linked and combined as systems control both the longitudinal and lateral position of the vehicle.
  It is well possible that multiple solutions to handle a scenario are acceptable, as they could all results in "crash avoidance", assuming the scenario is reasonably foreseeable and preventable.
  The criteria can also be related to tests where the system should not be activated, so called true-negative tests. So, despite the close proximity of an object or lane edge the system should not be activated to avoid dangerous situations or driver annoyance.
- Interaction between the driver/operator/other road users and vehicle:
  This includes for example requirements on how the warning should look/sound like, but also how the transition-of-control between automated and assisted driving is handled. These requirements have not been further detailed, as it is out of scope of the HEADSTART project.

The assessment of the KET Positioning is often already indirectly included in the criteria mentioned above, as positioning is an essential part of safe driving. At this moment only limited specific criteria on positioning are present, but it is expected that this will increase, especially if accurate sharing information on positioning is required. But also, if systems operate location specific, for example by geo-fencing, it might be needed to include position specific criteria. Various initiatives are referred to that provide information, which and how the positioning information should be made available. This can be used as criteria within the evaluation part of the safety assessment.

A similar approach holds for the KET Communication (V2X), as also there are only limited criteria defined yet. But also, communication is often indirectly tested when testing the driving capabilities. However especially when the communication is used for cooperative driving and other vehicles use the shared information directly to drive, for example in a platoon, it is essential that criteria are set on how and what is communicated externally by the vehicle. Also, for Communication (V2X) various initiatives are available that can provide criteria within the safety assessment evaluation. Special attention should be paid to how systems interact and behave as a whole, as well as how they react on potential misinformation.

The approach on KET Cybersecurity differs to the other HEADSTART KETs in the sense that it is less directly related to the driving capabilities of the CAV. Off course, it is possible that a hack influences the driving behaviour but in general this will not be scenario specific. Within the HEADSTART project an approach to address cybersecurity is proposed which includes criteria to ensure a cybersecurity safe CAV.

The activities within HEADSTART T3.3 "*Task 3.3: Assessment criteria definition*" and the reported findings in this document, as well as the deliverable D3.1 "*Guideline of a comprehensive validation and certification procedure to ensure safe CAD systems"* [5], D3.2 "*Toolchain for mixed validation – integration of simulation and Physical testing"* [6] and D3.4 "*Harmonisation proposals of test results"* [47], will be used in HEADSTART T3.5 "*Test procedure for defined use cases*" to further detail the HEADSTART methodology, procedures and tools for the HEADSTART selected use cases. In HEADSTART work package 4 "*Application and demonstration*" the HEADSTART methodology, procedures and tools including the criteria will be applied and demonstrated through the different HEADSTART use cases to show its potential.

7 References

[1] HEADSTART Project, “D2.1 Common methodology for test, validation and certification,” 2020. [Online]. Available: https://www.headstart-project.eu/results-to-date/deliverables/.

[2] HEADSTART, “HEADSTART glossary,” [Online]. Available: https://www.headstart-project.eu/homepage/glossary/.

[3] HEADSTART Project, “D2.2 Extension of the Common Methodology for the HEADSTART Key Enabling Technologies,” 2020. [Online]. Available: https://www.headstart-project.eu/results-to-date/deliverables/.

[4] HEADSTART Project, “D2.3 Assessment method for each of the use cases defined,” 2020. [Online]. Available: https://www.headstart-project.eu/results-to-date/deliverables/.

[5] HEADSTART Project, “D3.1 Guideline of a comprehensive validation and certification procedure to ensure safe CAD systems,” 2020. [Online]. Available: https://www.headstart-project.eu/results-to-date/deliverables/.

[6] HEADSTART Project, “D3.2 Toolchain for mixed validation – integration of simulation and physical testing,” 2020. [Online]. Available: https://www.headstart-project.eu/results-to-date/deliverables/.

[7] HEADSTART Project, “HEADSTART Mid-term event - October 2020,” 22 10 2020. [Online]. Available: https://www.headstart-project.eu/headstart-mid-term-event/.

[8] PEGASUS, “PEGASUS,” [Online]. Available: PEGASUS https://www.pegasusprojekt.de/en/.

[9] TNO, “StreetWise,” [Online]. Available: https://www.tno.nl/streetwise.

[10] VEDECOM, “MOOVE,” [Online]. Available: http://www.vedecom.fr/moove-securiser-la-conduite-autonome-grace-a-la-collecte-des-donnees-de-roulage/?lang=en.

[11] UNECE, “Regulation 130 - Uniform provisions concerning the approval of motor vehicles with regard to the Lane Departure Warning System (LDWS),” 18 06 2014. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/d029cda3-f6b9-11e3-831f-01aa75ed71a1/language-en/format-PDF/source-194026407.

[12] UNECE, “Regulation 661/2009 - Type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor,” 13 07 2009. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32009R0661.

[13] UNECE, “Regulation 2019/2144 - Type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles,” [Online]. Available: https://eur-lex.europa.eu/eli/reg/2019/2144/oj.

[14] UNECE, “Regulation 131 - Uniform provisions concerning the approval of motor vehicles with regard to the Advanced Emergency Braking Systems (AEBS),” 19 07 2014. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/302d6594-0f02-11e4-a7d0-01aa75ed71a1/language-en/format-PDF/source-194026302.

[15] ISO, “ISO 17361:2017 Lane departure warning systems — Performance requirements and test procedures,” [Online]. Available: https://www.iso.org/standard/72349.html.

[16] NHTSA, “NHTSA test procedures,” [Online]. Available: https://www.nhtsa.gov/vehicle-manufacturers/test-procedures.

[17] UNECE, “WP.29/2020/81 - Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to Automated Lane Keeping System,” 2020. [Online]. Available: https://undocs.org/ECE/TRANS/WP.29/2020/81.

[18] UNECE, “UN Regulation on Automated Lane Keeping Systems is milestone for safe introduction of automated vehicles in traffic ,” 24 June 2020. [Online]. Available: https://unece.org/transport/press/un-regulation-automated-lane-keeping-systems-milestone-safe-introduction-automated.

[19] European Parliament, “Regulation of the European parliament and of the council on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles,” [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil%3APE_82_2019_REV_1.

[20] ISO, “ISO 26262 Road vehicles — Functional safety,” [Online]. Available: https://www.iso.org/ics/43.040.10/x/.

[21] ISO, “ISO/PAS 21448:2019 Road vehicles — Safety of the intended functionality (SOTIF),” [Online]. Available: https://www.iso.org/standard/70939.html.

[22] Spanish traffic authority, “15/V-113: Authorization to conduct tests or research,” 11 2015. [Online]. Available: http://catalonialivinglab.com/wp-content/uploads/2019/06/15v-113-vehiculos-conduccion-automatizada-english.pdf.

[23] Spanish traffic authority, “15/V-113 modifications: Modificación anexo de la Instrucción DGT 15/V-113 de Autorización de pruebas o,” 7 2020. [Online]. Available: https://www.dgt.es/Galerias/seguridad-vial/normativa-legislacion/otras-normas/modificaciones/2020/Escrito_Directriz_SGGMT_7_2020_Modificacion_anexo_de_la_Instruccion_DGT_15_V_113.pdf.

[24] UNECE, “Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system,” [Online]. Available: http://www.unece.org/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf.

[25] Euro NCAP, “Euro NCAP 2025 Roadmap,” 07 2017. [Online]. Available: https://cdn.euroncap.com/media/30700/euroncap-roadmap-2025-v4.pdf.

[26] Euro NCAP, “Assessment protocol - Safety Assist v.9.0.3,” 6 2020. [Online]. Available: https://cdn.euroncap.com/media/58229/euro-ncap-assessment-protocol-sa-v903.pdf.

[27] Euro NCAP, “Assessment protocol - Vulnerable Road User Protection v.10.0.3,” 6 2020. [Online]. Available: https://cdn.euroncap.com/media/58230/euro-ncap-assessment-protocol-vru-v1003.pdf.

[28] Euro NCAP, “Assisted Driving test and assessment protocol - Highway Assist Systems v1.0,” 10 2020. [Online]. Available: https://cdn.euroncap.com/media/58813/euro-ncap-ad-test-and-assessment-protocol-v10.pdf.

[29] US NHTSA, “Crash imminent brake (CIB) system performance evaluation for the new car assessment program,” 10 2015. [Online].

[30] US NHTSA, “Dynamic Brake Support (CIB) performance evaluation confirmation test,” 10 2015. [Online].

[31] US NHTSA, “Forward Collision Warning (FCW) system confirmation test,” 2 2013. [Online]. Available: https://www.safercar.gov/staticfiles/safercar/NCAP/FCW_NCAP_Test_Procedure_2-7-2013.pdf.

[32] US NHTSA, “Lane departure warning (LDW) system confirmation test and lane keeping support performance documentation,” 2 2013. [Online]. Available: https://www.safercar.gov/staticfiles/safercar/NCAP/LDW_LKS_2-7-2013.pdf.

[33] SAE, “J3016_201806 - Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles,” 07 01 2019. [Online]. Available: https://www.sae.org/standards/content/j3016_201806/.

[34] Mobileye, “Mobileye Responsibility-Sensitive Safety (RSS),” [Online]. Available: https://www.mobileye.com/responsibility-sensitive-safety/.

[35] S. Shalev-Shwartz, S. Shammah and A. Shashua, “On a Formal Model of Safe and Scalable Self-driving Cars,” *arXiv:1708.06374 [cs, stat],* 2018.

[36] Aptiv, Audi, Baidu, BMW, Continental, Daimler, FCA US LLC, HERE, Infineon, Intel and Volkswagen, “Safety First For Automated Driving (SaFAD),” 2019. [Online]. Available: https://connectedautomateddriving.eu/wp-content/uploads/2019/09/Safety_First_for_Automated_Driving.pdf.

[37] European Commision, “eCall in all new cars from April 2018,” 28 4 2018. [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/ecall-all-new-cars-april-2018.

[38] 5GAA, “White paper; C-V2X Use Cases Methodology, Examples and Service Level Requirements,” 29 7 2019. [Online]. Available: https://5gaa.org/wp-content/uploads/2019/07/5GAA_191906_WP_CV2X_UCs_v1-3-1.pdf.

[39] CEN, “EN 16803-1:2020 Space - Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) - Part 1: Definitions and system engineering procedures for the establishment and assessment of performances,” 23 9 2020. [Online]. Available: https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT,FSP_ORG_ID:66697,887985&cs=15DFEDD47F2D4F8478B6330F59C180404.

[40] CEN, “EN 16803-2:2020 Space - Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) - Part 2: Assessment of basic performances of GNSS-based positioning terminals,” 23 9 2020. [Online]. Available: https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT,FSP_ORG_ID:40532,887985&cs=108C38DCBB59B92495E306C7BE2B166B0.

[41] CEN, “EN 16803-3:2020 Space - Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) - Part 3: Assessment of security performances of GNSS-based positioning terminals,” 23 9 2020. [Online]. Available: https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT,FSP_ORG_ID:40533,887985&cs=17A91585AB08E9D3FF53C8AC83B3AD9AE.

[42] CEN, “CEN/TR 17447:2020 Space - Use of GNSS-based positioning for road Intelligent Transport System (ITS) - Mathematical PVT error model,” 5 2 2020. [Online]. Available: https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT:69987&cs=19D31CA41D33A6D02BD236C45703E9E44.

[43] CEN, “CEN/TR 17448:2020 Space - Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) - Metrics and Performance levels detailed definition,” 4 3 2020. [Online]. Available: https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT:69985&cs=1E66249D5510EAC8BB7A354874A6BA1DB.

[44] CEN, “CEN/TR 17464:2020 Space - Use of GNSS-based positioning for road Intelligent Transport System (ITS) - Security attacks modelling and definition of performance features and metrics related to security,” [Online]. Available: https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT:69983&cs=14EB408A04317FB60967127086DF72BA8.

[45] CEN, “CEN/TR 17465:2020 Space - Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) - Field tests definition for basic performance,” 22 4 2020. [Online]. Available: https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT:69986&cs=181805E6035F262AAA9754FE498DF48E1.

[46] CEN, “CEN/TR 17475:2020 Space - Use of GNSS-based positioning for road Intelligent Transport System (ITS) - Specification of the test facilities, definition of test scenarios, description and validation of the procedures for field tests related to security perf,” 29 4 2020. [Online]. Available: https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT:69984&cs=1FD1F743D026E204E3C8B4DE46D17FA17.

[47] HEADSTART Project, “D3.4 Harmonisation proposals of test results,” 2021. [Online]. Available: https://www.headstart-project.eu/results-to-date/deliverables/.

[48] UNECE, “Safety at core of new Framework to guide UN regulatory work on autonomous vehicles,” 3 September 2019. [Online]. Available: https://unece.org/transport/press/safety-core-new-framework-guide-un-regulatory-work-autonomous-vehicles.

[49] HEADSTART Project, “D3.3 Assessment criteria of CAD functionalities for consumer testing and type approval,” 2021. [Online]. Available: https://www.headstart-project.eu/results-to-date/deliverables/.

Annex 1 Spanish License Exemption exhaustive test list [22] [23]

Dynamic tests: These are the tests to be performed by the Technical Service in order to prove the safety of the vehicle equipped with automated technologies. In the case the vehicle is not able to perform any of these tests due to its construction features (e.g. maximum speed) an alternative test designed by the technical service should be performed.

Conventional (manual) driving

Driving in straight direction for speedometer validation.

Objective	The objective of this scenario is to verify the proper behaviour of the speedometer when driving in manual mode.
Acceptance Criteria	- Speedometer is displaying the speed correctly. - No vibration, noise or other anomalies detected while driving the vehicle. - Checks will be performed attending to the technical service criteria.

Manual Driving during bend exit manoeuvre for steering wheel validation

Objective	The objective of this scenario is to verify the proper performance of self-return of the steering wheel when driving in manual mode.
Acceptance Criteria	- The self-return of the steering wheel performs correctly. - No vibration, noise or other anomalies detected while driving the vehicle. - Checks will be performed attending to the technical service criteria.

Manual Driving during bend exit manoeuvre for steering wheel validation.

Preconditions	- No warnings/errors. - Vehicle in manual driving mode.
Acceptance Criteria	- The self-return of the steering wheel performs correctly. - No vibration, noise or other anomalies detected while driving the vehicle. - Checks will be performed attending to the technical service criteria.

Manual driving during weaving manoeuvre for vehicle stability validation.

Objective	The objective of this scenario is to validate the proper performance of the vehicle stability and control when driving in manual mode.
Acceptance Criteria	- The stability and control of the vehicle are working correctly. - No vibration, noise or other anomalies detected while driving the vehicle. - Checks will be performed attending to the technical service criteria.

Manual driving and braking up to 0.5 g.

Objective	The objective of this scenario is to verify the proper performance of the braking system when driving in manual mode.
Acceptance Criteria	- Ego vehicle brakes properly (No deviation, vibrations, noise or other anomalies). - Checks will be performed attending to the technical service criteria.

Manual Driving and braking to wheel lock-up or activation of ABS

Objective	The objective of this scenario is to verify the proper performance of the braking system when driving in manual mode.
Acceptance Criteria	- Ego vehicle brakes properly (No deviation, vibrations, noise or other anomalies). - Checks will be performed attending to the technical service criteria.

Manual driving: Acceleration to 3/4 of the accelerator pedal until 80 km/h

Objective	The objective of this scenario is to verify that the vehicle is able to perform the acceleration from idle to a defined speed with a constant accelerator pedal position. This test shall not apply to vehicles intended solely for urban use and which due to their technical capabilities (e.g. maximum speed) cannot perform the tests.
Acceptance Criteria	- No abnormal behaviour during the test. - Checks will be performed attending to the technical service criteria.

Manual driving: Driving in straight line up to 120 km/h

Objective	The objective of this scenario is to verify the proper behaviour of the vehicle when driving at high velocities in manual mode. This test shall not apply to vehicles intended solely for urban use and which due to their technical capabilities (e.g. maximum speed) cannot perform the tests.
Acceptance Criteria	- No deviation, vibrations, noises or other anomalies detected while driving the vehicle. - Checks will be performed attending to the technical service criteria.

Override: steering wheel

Steering wheel Automated driving test

Objective	The objective of this scenario is to verify that the vehicle is able to go in automated driving mode, at constant speed while maintaining a straight path.
Acceptance Criteria	- The vehicle is able to maintain at the desired straight path for the defined distance.

Override: Steering wheel

Objective	The objective of this scenario is to verify that at any stage of automated driving the driver override is detected after applying a torque to the steering wheel that shall not exceed a defined maximum torque. Also to verify that when override is detected, the automated driving system stops all its actions.
Acceptance Criteria	- The vehicle has maintained the desired trajectory while in automated driving mode. - The driver has carried out the change of path within the limits defined by the doors. - The maximum torque applied by the driver during change of path has not exceeded a defined maximum torque. - The automated driving process has stopped before reaching door 3.

Override: brake pedal

Brake pedal Automated driving test

Objective	The objective of this scenario is to verify that the vehicle is able to drive in automated driving mode, at constant speed while maintaining a straight path.
Acceptance Criteria	- The vehicle is able to maintain at the desired straight path for the defined distance.

Override: Brake pedal

Objective	The objective of this scenario is to verify that at any stage of automated driving the driver override is detected when actuating the brake pedal. Also to verify that when override is detected, the automated driving system stops all its actions.
Acceptance Criteria	- The vehicle has maintained the desired trajectory in automated driving mode. - The maximum deceleration of the vehicle has exceeded the defined threshold. - The average deceleration (MFDD) during braking has exceeded the defined threshold. - Automated driving mode has stopped during braking.

Override: accelerator pedal

Accelerator pedal Automated driving test

Objective	The objective of this scenario is to verify that the ego vehicle is able to stop without reaching impact during automated driving mode with no driver interaction.
Acceptance Criteria	- Ego vehicle is able to stop without reaching impact with no driver interaction.

Override: Accelerator pedal

Objective	The objective of this scenario is to verify that at any stage of automated driving the driver override is detected when actuating the accelerator pedal. Also to verify that the driver's decision always prevails over the automated driving system.
Acceptance Criteria	- The vehicle has maintained the desired trajectory - The override has resulted in impact with the parked car. - The automated driving process has stopped after the driver override.

Override: emergency shutdown

Emergency shutdown

Objective	The objective of this scenario is to verify that at any stage of automated driving the driver override is detected when actuating over the emergency shutdown system. Also to verify that the driver's decision always prevails over the automated driving system.
Acceptance Criteria	- The override has resulted in impact with the parked car. - The automated driving process has stopped after the driver override.

Longitudinal control (braking test, automated emergency braking,)

Braking test Type 0 (Cold)

Objective	The objective of this scenario is to check and ensure the correct operation of the braking system.
Acceptance Criteria	- Ego vehicle speed when braking manoeuvre starts shall not be less than a defined percent of the prescribed speed for the test. - The speed and distance shall be determined using instrumentation whose accuracy must be a defined percent tolerance with respect to the prescribed speed for the test. - The "average stabilized deceleration" may be determined by methods other than measuring the speed and distance; in that case, the accuracy of the "average stabilized deceleration" shall be a defined percent tolerance. - The vehicle must be able to stop according to the limits below: • Distance travelled shall not be greater than the prescribed distance for the test. • Average stabilized deceleration shall be at least the prescribed value for the test. • The force applied to the brake pedal shall be in the limits of the prescribed value for the test.

Braking test Type I (Fatigue)

Objective	The objective of this scenario is to check and ensure the correct operation of the braking system.
Acceptance Criteria	- The braking mean deceleration shall be the defined during every brake application. - The results of the braking test Type 0 performed shall be within the limits defined.

Vehicle control: AEB Car to Car

Objective	The objective of this scenario is to verify that the ego vehicle is able to avoid impact during automated driving mode with no driver interaction.
Acceptance Criteria	- Ego vehicle is able to avoid impact with no driver interaction.

Vehicle control: AEB Car to VRU

Objective	The objective of this scenario is to verify that the ego vehicle is able to avoid impact during automated driving mode with no driver interaction.
Acceptance Criteria	- Ego vehicle is able to avoid impact with no driver interaction.

Lateral control

Lane departure

Objective	The objective of this scenario is to verify that the ego vehicle is able to stay in a lane marked with road markings and prevent crossing the line during automated driving mode with no driver interaction.
Acceptance Criteria	- The ego vehicle has prevented crossing the line with no driver interaction in every situation. Line crossing is defined as when the inner edge of the line touches the outside edge of the front tire closest to the line. - Each combination has been successfully repeated a defined number of times.

Lane centring

Objective	The objective of this scenario is to verify that the ego vehicle is able to stay in a lane marked with road markings and prevent crossing the line during automated driving mode with no driver interaction. So as to ensure that in automated driving mode the vehicle is able to drive within its lane stably without interfering with the adjacent lanes.
Acceptance Criteria	- The automated driving system maintains the vehicle centre on the central axis of the lane in a range of a defined tolerance for at least a defined time. Furthermore, it is required that the steering wheel speed during testing is always less than a defined º/s rotation speed. - Each combination has been successfully repeated a defined number of times.

Annex 2 Euro NCAP Assisted Driving Grading [28]

Assisted Driving Grading		Scoring (max. Scoring = 200)
Very Good	Vehicles graded Very Good are state-of-the-art ACC and Lane Centering systems with additional functions to support the driver and keep him engaged. These vehicles also provide a high-level safety back-up in challenging scenarios, utilizing the extended sensor set these vehicles are equipped with.	>=160 points (>=80%)
Good	Both ACC and Lane Centering perform well in most situations and the system keeps the driver engaged. Good systems also contain some extra features to provide the driver more assistance and provide a good safety back-up.	>=140 points (>=70%)
Moderate	ACC and Lane Centering generally perform well in the less challenging scenarios, but the system has a better performing safety back-up compared to Entry-graded vehicles. Unbalanced vehicles with a good safety back-up also end up in this category.	>=120 points (>=60%)
Entry	An Entry vehicle assistance system typically provides assistance in the less challenging scenarios and comprises only a basic ACC and Lane Centering system, with no additional features. Or, the system's performance in Assistance Competence is highly unbalanced between Driver Engagement and Vehicle Assistance. The safety back-up is limited.	>=100 points (>=50%)

Category	Subcategories		Element	Assessment criteria
Assistance competence	Driver engagement	Consumer info	System name	Contains the word “assistant”, “assistance”, “assist” or another variation (++) Contains “auto”, “automatic”, “automated”, "pilot", "self-drive" or term to imply a level of automation higher than which the system is offering (-) Neither one nor the other (+)
			Marketing material	Adverts, website, published material correctly describe the system functionality
			Quick start guide	Quick start guide supplied to the consumer on the basic operation of the driving assistance system and system limits
			Vehicle handbook	Handbook should detail intended use of the system and limits of the systems operation. It should warn that the driver must be always engaged
		System status	Continuous system status indicator	Per system control mode (longitudinal, lateral, both, none) the following aspects are awarded: - Configurable status information, always indicated and distinguishable from other modes - Additional indicators in a head up display or another additional display in the driver’s eye - When the status indication corresponds to general human factor guidelines and design principles

Category	Subcategories		Element	Assessment criteria
			System status change indicator	An audible and/or haptic warning to indicate a system change is awarded. Additional score is awarded when additional visual information is shown. In case this information meets the general human factors guidelines, more score is obtained.
		Driver monitoring	UNECE R79 Compliance	R79 compliance confirmed
			Direct Driver Monitoring	If a manufacturer already has a Direct Driver Monitoring system as integral part of the assistance system, the manufacturer should liaise with the test laboratory and the Euro NCAP secretariat who will consider if and how the monitoring system can be included in the assessment and are eligible of extra scoring.
		Driving Collaboration	Override torque	This assessment determines how the vehicle responds and collaborators with a driver steering input, for example to avoid an obstacle within the lane of travel, when the steering assistance system is engaged. The difference between system percentage increase in torque (compared to system off) is compared.

Category	Subcategories		Element	Assessment criteria
			Override response (Override torque & system response)	For vehicles where the override torque below a set threshold: - max. awarded when the system provides continuous steering assistance throughout the manoeuvre and centres the vehicle in the lane afterwards - some points are scored when the system cancels steering assistance during the manoeuvre but automatically reengages once the vehicle is centralised in lane again by the driver - If a system cancels steering assistance during manoeuvre and requires a reactivation by the driver afterwards, no points are given
	Vehicle assistance	Speed assistance	Speed assist system	Euro NCAP Safety Assist - Speed Assist Systems assessment is used as basis.
			Reaction to speed limits (fixed limits)	Road test to verify that the system automatically adjusts the speed before the front axle of the vehicle passes a traffic sign. For a system which only provides information, the system must warn the driver with enough time, so the driver adjusts to the speed limit before the front axle of the vehicle passes the sign. Additional points are available for reducing speed when approaching the following road features: - Corners - Roundabouts - Junctions
			Reaction to speed limits (variable and temporary limits)	

Category	Subcategories		Element	Assessment criteria
			Road features (corner)	
			Road features (roundabouts)	
			Road features (junctions)	
		ACC performance	ACC Car-to-Car scenarios	The assessment looks at how the longitudinal assist system fitted to the vehicle reacts to other vehicles during operation. Only ACC capacity, braking level < set deceleration limit. Applied to stationary, moving, braking targets, curves, cut-in and cut-out scenarios. For more to less awarded: Collision avoidance. Speed reduction >= 5 km/h before AEB activation NO speed reduction (no awarded)

Category	Subcategories		Element	Assessment criteria
			Undertake prevention	In most European countries it is only permissible to overtake a slower moving vehicle, in free-flowing traffic, in a lane to one side of the slower moving vehicle. Therefore, an assisted driving system should not overtake a vehicle on the incorrect side in this scenario. For this highway-based assessment, it may be that the system is geofenced and it will be a requirement for the OEM to inform the test laboratory of the function of the system. The manufacturers handbook or supplied information will be used to assess the performance of the system, with its operation confirmed by the test house where possible.
			ACC Auto-resume	This assessment looks at the strategy to resume the ACC after the vehicle has come to a full stop. To be eligible for assessment, the vehicle must be capable of coming to a complete stop under ACC control when the traffic in front stops while also maintain steering assistance.
		Steering capabilities	Steering assistance	A steering assistance function should support the driver to keep the vehicle in lane, not only on straight roads. If a car departs from its lane there is an increased risk of collision. Euro NCAP does not expect vehicles to stay in the centre of the lane in all corners but expects the vehicle to always support the driver by directing the vehicle to the correct heading. Euro NCAP tests the steering assistance in a so-called S-Bend and assesses the capability of the system to keep the vehicle in the lane or redirect it. The assessment is made taking into account whether the systems keeps the vehicle or redirects it in the lane on the S-bend. Positive assessment is given when: • Vehicle stays in lane in both turns • Vehicle stays in lane in the 1st turn and redirects the vehicle in the 2nd turn • Vehicle stays redirects in the 1st turn
			Lance Change assist	

Category	Subcategories		Element	Assessment criteria
Safety Backup		System Failure	Sensor blocked at Start-up	This element evaluates all individual sensors systematically in three different scenarios: - Sensor blocked at vehicle start up. - Sensor becomes blocked when vehicle is moving but Driver Assistance System not activated. - Sensor becomes blocked when vehicle is moving with the Driver Assistance System active and engaged. Score is obtained on the condition the system cannot get / stay engaged in the three situations. If the assistance system can be activated at this time or does not deactivate, there is no score.
			Sensor blocked with vehicle in motion, System inactive	
			Sensor blocked with vehicle in motion, System active	

Category	Subcategories		Element	Assessment criteria
		Unresponsive Driver Intervention	Controlled stop	This element assesses the ultimate reaction of the vehicle to a driver who remains unresponsive after the cascade of warnings and attempts re-engage the driver. When the driver release control "hands-off", a vehicle that maintains steering control and brings the vehicle to a controlled stop or reduces its speed to crawling speed is awarded the scoring.
			Headroom for more advanced solutions	Additional scoring is reserved for a more advanced response in case of an incapacitated driver.
		Collision Avoidance: the capability of the vehicle to avoid a collision using both	ACC/AEB CAR-TO-CAR	For each scenario and test speed, more to less points can be achieved where: - The ACC and/or AEB fully avoids the collision. - The ACC and/or AEB intervenes and reduces the impact speed by more than 5 km/h. The ACC and/or AEB system does not avoid the collision, but an FCW is issued at a TTC >1.5s additional points are awarded. For CCRs, CCRm and CCRb, the same test speeds are used as for the ACC Performance assessment. For Cut-in and Cut-out additional and more critical set-ups are used to verify the Safety Backup.

Category	Subcategories		Element	Assessment criteria
		assisted driving systems and emergency systems combined is assessed.	LSS (S-Bend)	The lane support system – S-bend is designed to determine the ability of the vehicle to stay in lane or alert the driver to a lane departure on a curved section of road using both the AD system and the emergency LSS systems such as ELK, LKA and LDW. More to less points are given where: - An LKA intervention prevents the vehicle from crossing the lane marking by more than a predefined distance, max. points are awarded. - Where there is no intervention by the system, but an audible or haptic LDW is provided before the vehicle has left the lane by more than a predefined distance (half points).
			LSS (Intentional lane change with overtake)	This element assesses the vehicles ability to stop the vehicle changing lane into the path of a vehicle travelling in the adjacent lane. Steering assistance plus LSS. Only the Intentional Lane change with overtake tests from the Euro NCAP LSS Test Protocol v3.0.2 are to be performed.

Annex 3 HEADSTART Assurance Levels overview

nr	HEADSTART Parameter	Related CC class	Compliance of SFRs – HAL value
1	Interference & Jamming	- Protection of the TSF (ToE Security Functionality)	0.43
2	Wrong vehicle path (Spoofing attack)	- Communication- Identification and authentication - Security Management - Protection of the TSF (ToE Security Functionality)	0.74
3	Clock Offset	- Communication - Identification and authentication - Security Management - Protection of the TSF (ToE Security Functionality)	0.74
4	Untrusted V2X messages (Fake messages)	- Communication - User data protection - Identification and authentication - Protection of the TSF (ToE Security Functionality)	0.92
5	Digital signature missing from V2X messages	- Cryptographic Support - Communication - User data protection - Identification and authentication - Security Management	1.19

nr	HEADSTART Parameter	Related CC class	Compliance of SFRs – HAL value
6	Corrupted V2X messages	- Communication - User data protection - Identification and authentication - Protection of the TSF (ToE Security Functionality)	0.92
7	Delayed V2X messages (record & playback attack)	- Communication - User data protection - Identification and authentication - Security Management - Protection of the TSF (ToE Security Functionality)	1.13
8	V2X message is not trustworthy	- Communication - User data protection - Identification and authentication - Protection of the TSF (ToE Security Functionality)	0.92
9	V2X communication logs (Repudiation check)	- Security Audit - Communication - User data protection - Identification and authentication	1.00
10	V2X message not encrypted, validated and verified	- Cryptographic Support - Communication - User data protection - Identification and authentication - Privacy - Protection of the TSF (ToE Security Functionality)	1.33

nr	HEADSTART Parameter	Related CC class	Compliance of SFRs – HAL value
11	Virus is embedded in V2X on-board equipment	- Security Audit - Communication - User data protection - Identification and authentication - Security Management - Protection of the TSF (ToE Security Functionality)	1.40
12	Blocking due to interference. Missing all the V2X messages for X seconds	- Communication - Identification and authentication - Protection of the TSF (ToE Security Functionality)	0.62
13	Overflow communication channel with fake data	- Communication - Identification and authentication - Protection of the TSF (ToE Security Functionality)	0.62
14	Certificate Rotation	- Security Audit - Cryptographic Support - Communication - Identification and authentication - Security Management	1.02
15	Software package updates (Legitimate updates not applied)	- Communication - User data protection - Identification and authentication	0.75

nr	HEADSTART Parameter	Related CC class	Compliance of SFRs – HAL value
16	Software package updates (Illegitimate updates applied)	- Security Audit - Cryptographic Support - Communication - User data protection - Identification and authentication - Security Management - Protection of the TSF (ToE Security Functionality)	1.61
17	Software package updates (Misconfiguration/unintentional deletion of communication Software)	- Communication - User data protection - Identification and authentication - Protection of the TSF (ToE Security Functionality)	1.14

Harmonised European Solutions for Testing Automation Road Transport