connected automated driving.eu

EUROPEAN COMMISSION

HORIZON EUROPE PROGRAMME

CALL TOPIC HORIZON-CL5-2021-D6-01: Framework for better coordination of large-scale demonstration pilots in Europe and EU-wide knowledge base

FAME

Framework for coordination of Automated Mobility in Europe

D5.3: Recommendations for European framework for testing on public roads

Deliverable no.	5.3
Dissemination level	PU
Work Package no.	5
Lead editor	IDIADA
Version number	1.3
Status (F: final, D: draft)	F
Keywords	Public road testing, Harmonization, Safety, Automation, Cross-border, Regulation, Ethics, Cybersecurity, Risk Assessment, Data Protection, Mutual Recognition
Due date	29/02/2025
Document date	23/06/2025

Funded by the European Union

Document Control Sheet

Author(s)	Justin Hidalgo (IDIADA), Carlos Luján (IDIADA), Pablo Rodriguez (IDIADA), J. Karahasanović (ATE), A. Jungmann (MD), S. Koskinen (VTT), Marcel Huschebeck (PTV), Erik Svanberg (CHALMERS)
Work area	WP5 Test and data framework for CCAM Task 5.4 Recommendations for a European framework for testing on public roads

Version history:

Version	Date	Author	Summary of changes
0.1	11/12/2024	Justin Hidalgo (IDIADA), J. Karahasanović (ATE), Erik Svanberg (CHALMERS), A. Jungmann (MD), S. Koskinen (VTT), Marcel Huschebeck (PTV),	First consolidated draft of the deliverable. Development on external stakeholder feedback from workshops.
0.2	03/03/2025	Justin Hidalgo (IDIADA), J. Karahasanović (ATE), Erik Svanberg (CHALMERS), A. Jungmann (MD), S. Koskinen (VTT), Marcel Huschebeck (PTV), Vasilis Sourlas (ICCS), Mats Rosenquist (VOLVO), Marcos Nieto (VICOMTECH), Jo Ann (LEEDS)	Chapter organization. Further development after internal review.
1.0	05/04/2025	- Joint Research Centre - CCAM Partnership - Austrian Ministry - Wayve - Swedish Transport Agency	External review by members of the organisations listed. From this review process the following chapters were further developed: Safety operator, Test permit procedure, Mutual recognition, Proving ground pre-tests, Monitoring process and reporting and Data requirements.
1.1	20/06/2025	Hi-Drive Project	Alignment with the Hi-Drive Project.

Funded by the European Union

			Development of chapter “Case Study: Applying the FAME Framework to Hi-Drive Use Cases”
1.2	31/06/2025	Justin Hidalgo (IDIADA), Carlos Luján (IDIADA), J. Karahasanović (ATE), Erik Svanberg (CHALMERS), A. Jungmann (MD), S. Koskinen (VTT), Marcel Huschebeck (PTV),	Final review after authors workshops per topic (Legal, Data and Ethics)
1.3	22/10/2025	Nadia Martínez Sheikhi	Final review for submission working out comments from AustriaTech quality assurance review

Approval:

	Name	Organisation	Date
Editor	Justin Hidalgo Vélez	IDIADA	31/06/2025
Peer Reviewer	Jo-Ann Pattison	LEEDS	16/01/2025
Peer Reviewer	Biagio Ciuffo	EC-JRC	11/03/2025
Peer Reviewer	Tobias Reich	EC-JRC	11/03/2025
Authorized by	Aggelos Soteropoulos, Martin Russ	AustriaTech	03/10/2025

Submission:

Submitted by	Date of submission
Project Coordinator	10/11/2025

Legal disclaimer:

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Climate, Infrastructure and Environment Executive Agency (CINEA). Neither the European Union nor CINEA can be held responsible for them.

Table of Contents

Funded by the European Union

Funded by the European Union

Funded by the European Union

Funded by the European Union

Table of Figures

Funded by the European Union

Table of Tables

Funded by
the European Union

Abbreviations & definitions

Term	Description
ADAS	Advanced Driver Assistance Systems
ADS	Automated Driving System
AEB	Advanced Emergency Braking
AI	Artificial Intelligence
ALKS	Automated Lane Keeping System
AM	Automated Mobility
ASIL	Automotive Safety Integrity Level
AV	Automated Vehicle
CAD	Connected Automated Driving
CAN	Controller Area Network
CCAM	Connected, Cooperative and Automated Mobility
CCAM Partnership	European Partnership on Connected, Cooperative and Automated Driving
DCAS	Driver Control Assistance Systems
DDT	Dynamic Driving Task
DSSAD	Data Storage System for Automated Driving
EC	European Commission
ECU	Electronic Control Unit
EDR	Event Data Recorder
EU	European Union
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
GDPR	General Data Protection Regulation
GRVA	Working Party on Automated/Autonomous and Connected Vehicles
GSR	General Safety Regulation
HARA	Hazard Analysis and Risk Assessment
HE	Horizon Europe (EU R&I funding programme succeeding Horizon 2020)
HTSG	Homologation Testing Subgroup
ISO	International Organization for Standardization

Funded by the European Union

ITS	Intelligent Transports Systems
IWG	Informal Working Group
MRM	Minimum Risk Manoeuvre
MVWG-ACV	Motor Vehicle Working Group on Automated and Connected Vehicles
NATM	New Assessment and Testing Methodology
ODD	Operational Design Domain
OEDR	Object and Event Detection and Response
PDI	Physical and Digital Infrastructure
R&I	Research and Innovation
SVG	Safety Validators Group
TARA	Threat Analysis and Risk Assessment
UNECE	United Nations Economic Commission for Europe
V2X	Vehicle-to-Everything
VIN	Vehicle Identification Number

Funded by the European Union

Executive Summary

Automated vehicle (AV) deployment on public roads requires meeting two key conditions: establishing a legal framework and proving vehicle safety through type approval. In the European Union, national variations in AV testing legislation create significant challenges for manufacturers and R&D centers, resulting in increased workload, costs, and harmonization difficulties.

The United Nations Economic Commission for Europe (UNECE) defines a type approval process through the New Assessment and Testing Methodology (NATM), which includes multiple assessment "pillars": safety management system audit, in-service monitoring, reporting, track testing, virtual testing, and real-world testing.

Prior to type approval, AVs must undergo multiple public-road prototype tests serving two primary purposes. Validation Testing, as part of the type-approval process, validates vehicle performance in real-world conditions as required by regulations like Regulation (EU) 2022/1426. Development Testing allows manufacturers and R&D centers to refine the autonomous driving system based on real-world performance. Both testing approaches are essential for ensuring AV safety and reliability before widespread deployment.

This document provides recommendations for a European framework for testing AVs on public roads. It was prepared within the EC-funded Research & Innovation Action FAME (Framework for coordination of Automated Mobility in Europe) that supports the commitment of the European Commission and the CCAM Partnership to provide a long-term coordination framework for R&I and large-scale testing and evaluation activities in Europe.

Rather than serving as a strict checklist, these guidelines offer a comprehensive yet flexible approach to assist national and local authorities, technical services, manufacturers, and R&D centres in managing AV test permit applications. By streamlining requirements, the framework aims to harmonize AV testing procedures across EU member states, addressing the current fragmented regulatory landscape. This harmonization benefits all stakeholders involved and lays the groundwork for policymakers. Moreover, this framework is aligned with the Guideline on Pre-Homologation ADS-Testing developed by the Homologation Testing Sub-Group (HTSG) of the Motor Vehicle Working Group - subgroup on Automated/Connected Vehicles (MVWG-ACV), ensuring a consistent and coordinated approach to AV testing across Europe. This alignment reinforces the goal of establishing a more cohesive and efficient regulatory environment, reducing inconsistencies, and facilitating mutual recognition among member states. It is important to note that the purpose of this document is to provide the guidelines for authorities to implement or adapt their own national legislation that is aligned with the rest of the EU Member States as well as the European commission. These recommendations serve as a flexible framework that member states can adapt when developing their own national legislation, ensuring alignment across the European Union while respecting national sovereignty in implementation approaches.

The report begins by outlining the current legislative basis for AV testing in EU countries, highlighting the diversity in approaches ranging from dedicated automated driving laws to adaptations of existing traffic regulations. It then proposes a structured process for obtaining test permits, including the designation of a safety validation responsible entity, which could be the applicant (through self-

assessment), the approval authority, or a third-party assessor. Following, a key focus is placed on safety considerations, with detailed requirements for safety operators who oversee AV testing.

The document defines a two-stage submission process for AV test permits. In the first stage, applicants provide initial documentation covering key aspects such as the testing activity, ADS system description, cybersecurity compliance, and system risk assessment. The safety validator then reviews this submission to determine whether the identified risks are acceptable and sufficiently mitigated, considering both system-related and test-specific risks. If the documentation is deemed sufficient, the permit can be granted; otherwise, additional clarifications or supporting evidence may be requested. This additional submission, referred to as the second stage, includes recommendations such as conducting proving ground pre-tests to validate vehicle behaviour, implementing a data logger, and employing a remote safety operator before proceeding to public-road testing.

The framework introduces a mutual recognition process to facilitate cross-border testing, proposing the establishment of a Safety Validators Group (SVG) comprising representatives from multiple member states. To streamline the process further, creating an online European platform for test permit applications and processing should be a priority. This would not only increase efficiency but also provide a centralized system for data collection and analysis. This process aims to streamline permits while maintaining rigorous safety standards across borders. That said, it is important to note that this document explores these concepts in depth and provides comprehensive considerations for implementation, while intentionally avoiding prescriptive step-by-step procedures. This approach allows member states to develop their own concrete workflows that align with their specific legal, administrative, and operational contexts.

Industry-recognized risk assessment procedures are encouraged for adoption to contribute to a more consistent and comprehensive approach to safety evaluation, encompassing both system and activity risk evaluations. Safety by design can be implemented following specific automotive industry standards such as HARA (Hazard analysis and risk assessment). For the assessment of the activity risk, this document provides a comprehensive risk assessment matrix that gathers various impact dimensions. This approach enables a structured and objective identification of potential risks across different operational conditions, providing a clear framework for risk classification. While this document provides the conceptual foundation and key considerations for risk assessment, practical implementation will require member states to develop specific procedures and criteria adapted to their regulatory frameworks.

The document also addresses cybersecurity concerns, proposing a management plan to identify and mitigate potential vulnerabilities.

Data requirements for testing are extensively covered, including accident reporting processes, periodic test reporting, and software version traceability. The framework emphasizes the importance of data privacy and compliance with GDPR regulations.

These guidelines propose to appoint a person in pilot projects responsible for monitoring ethical aspects – using the provided checklist that covers safety assurance, ethical decision-making in algorithms, data privacy, security, user consent and control, accessibility and inclusivity, regulatory compliance, transparent impact assessment, and public engagement – to ensure ethical issues are closely tracked throughout the tests.

Funded by the European Union

The document proposes that public documentation of system safety should be required when automated vehicles are tested on public roads – briefly outlining how vehicles avoid accidents and how they handle emergency situations – drawing inspiration from the UK's Safe and Ethical Operational Concept (SEOC) to boost transparency and public trust.

In conclusion, this comprehensive framework aims to create a more unified approach to AV testing across Europe, balancing innovation with safety and ethical considerations. By addressing key aspects such as safety validation, mutual recognition, data management, and ethical practices, it provides a roadmap for the responsible development and testing of automated driving technologies on public roads.

Looking forward, the implementation of this framework should be accompanied by a pilot program to test its effectiveness in real-world scenarios. Establishing a dedicated working group on EC level to monitor this implementation and gather feedback will be crucial for future refinements. Additionally, developing comprehensive training programs for safety validators and safety operators will ensure consistent application of the framework across different jurisdictions.

As the field of autonomous driving continues to evolve rapidly, this framework should be viewed as a living document that provides conceptual guidance rather than fixed operational procedures. Annual reviews and updates will be necessary to incorporate technological advancements, regulatory changes, and lessons learned from practical applications across different member state implementations.

Funded by
the European Union

1 Introduction

The EC-funded Research & Innovation Action FAME (Framework for coordination of Automated Mobility in Europe)[1] supports the commitment of the European Commission and the CCAM Partnership[2] to provide a long-term coordination framework for R&I and large-scale testing and evaluation activities in Europe.

The mission of FAME is to engage an active community of stakeholders across the complex cross-sectorial value chain of CCAM, and capitalize on shared knowledge, to improve cooperation, consensus building and data sharing for CCAM testing and large-scale demonstration activities in Europe.

FAME will establish a stakeholder-validated European framework for testing on public roads. This framework will include a Common Evaluation Methodology, a CCAM test data space (TDS), a Taxonomy tool, an ethics framework, and an inventory of current legislation, approval processes and procedures. It is intended to enable comparability, complementarity and upscaling of R&I results for future research, development and testing of CCAM-enabled solutions and services, and facilitate the evaluation of their wider impacts.

The FAME approach is based on the integration and further development of existing elements such as stakeholder networks and the CAD Knowledge Base. FAME builds on a strong legacy of EU-funded Coordination and Support Actions ARCADE[3], CARTRE[4], VRA[5] and FOT-Net[6], which have developed harmonised methodologies and federated large networks of stakeholders to drive consensus building on challenges, needs and requirements for CCAM.

1.1 Rationale

In the process of developing an automated vehicle (AV), its deployment on public roads is the ultimate goal, but it requires several preliminary steps. To achieve this, two key conditions must be met: the existence of national legislation or a legal framework supporting AV deployment, and proof of vehicle safety through type approval. The current situation in the European Union involves national legislation for AV testing. This creates challenges for manufacturers and R&D centres, particularly when testing across different member states or regions, as they may face varying regulatory frameworks. These differences can result in additional workload, costs, and obstacles to the final objective of AV deployment ultimately leading to a lack of harmonization.

---

[1] Under Horizon Europe programme (HORIZON-CL5-2021-D6-01, 2022-2025)

[2] European partnership on connected cooperative and automated mobility, https://www.ccam.eu

[3] Aligning Research & Innovation for Connected and Automated Driving in Europe (EU H2020 DT-ART-2018, CSA, 2018-2022)

[4] Coordination of Automated Road Transport Deployment for Europe (EU H2020 ART06, CSA, 2016-2018)

[5] Support action for Vehicle and Road Automation network (EU FP7-ICT-2013-10, CSA, 2013-2016)

[6] Field Operational Tests Networking and Interaction (EU FP7-ICT-2007-2, CSA, 2008-2010) and follow-up Actions FOTNet2 (2011-2014) and FOT-Net Data (2014-2016)

The type approval process for AVs involves several steps as defined by the United Nations Economic Commission for Europe (UNECE) in their New Assessment and Testing Methodology (NATM). This methodology employs multiple "pillars" to assess vehicle compliance with established requirements. These pillars include the assessment of the manufacturer's safety management system in terms of an audit, in-service monitoring and reporting, track testing, virtual testing and real-world testing.

Prior to receiving type approval for deployment, in the development of an AV, real world public-road testing occurs multiple times as a prototype. These public-road tests serve three main purposes:

- Development Testing: This is part of the system's development process, allowing manufacturers, OEM's and R&D centres to gather data, redefine and improve the autonomous driving system or function based on real-world performance focusing on research in an early stage of development.
- Validation Testing: This is part of the system's development process, allowing manufacturers, OEM's and R&D centres to validate the autonomous driving system or function based on real-world performance on a late stage of development.
- Homologation Testing: This is part of the type-approval process as defined in legislations such as Regulation (EU) 2022/1426. It aims to validate the vehicle's performance in real-world conditions as required for type approval.

All types of public-road testing are essential steps in ensuring the safety and reliability of AVs before they are type approved for widespread deployment.

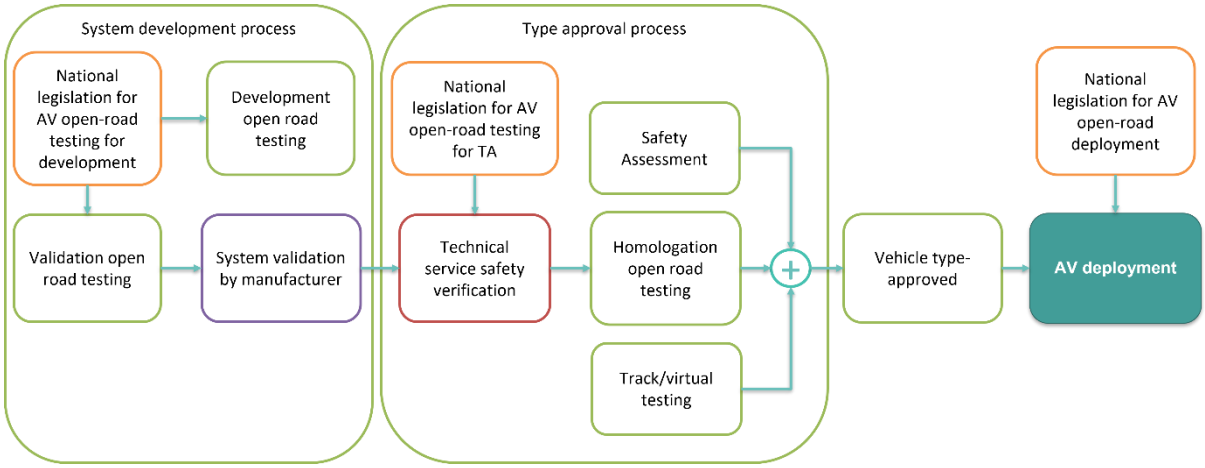


Figure 1. Regulatory eco-system for automated vehicles.

1.2 Purpose of the document

This document aims to address the complexities in the AV testing process for both validation and development purposes. The primary objective is to streamline the process for obtaining authorization for testing, proposing a harmonized framework and set of guidelines for AV public road testing across Europe. This framework seeks to reconcile differences between existing national legislations and provide a foundation for new regulations in countries currently lacking specific AV testing legislation. By doing so, it aims to facilitate cross-border testing, enhance safety standards, and accelerate the responsible development of automated driving technologies throughout the European Union.

Funded by the European Union

Specifically, this document aims to:

- Identify the necessary legislative frameworks at national and European levels.
- Describe the technical safety verifications and assessments required.
- Highlight the importance of harmonization across different jurisdictions.
- Address the challenges faced by stakeholders in navigating diverse regulatory landscapes.

The guidelines provided herein are not meant to be followed as a strict checklist, but rather as a comprehensive tool for all parties involved in bringing automated driving technology to public roads to enhance their capabilities and knowledge in assessing AV test permit applications.

1.3 Scope

This framework primarily focuses on the testing of AVs corresponding to SAE J3016 [1] Levels 3 and 4 of driving automation. Specifically:

- Level 3: The driving mode-specific performance by an Automated Driving System of all aspects of the dynamic driving task with the expectation that the human driver will respond appropriately to take over the DDT.
- Level 4: The driving mode-specific performance by an Automated Driving System of all aspects of the dynamic driving task, even if a human driver does not respond appropriately to a request to take over the DDT.

The framework addresses various aspects of AV testing, including safety validation, risk assessment, data management, ethical considerations, and cross-border testing protocols. It is designed to provide a comprehensive guide for manufacturers, researchers, and regulatory bodies involved in the development and approval of Level 3 and Level 4 automated driving systems. This scope aligns with the current state of AV development and the most pressing needs for harmonized testing procedures across the European Union.

1.4 Intended audience

By providing a comprehensive overview of the AV testing and approval process, this document aims to foster collaboration and understanding among all parties involved in bringing automated driving technology to public roads, ultimately facilitating the safe and efficient deployment of AVs for a wide range of stakeholders involved in the development, testing, and regulation of AVs, including:

- Policymakers and legislators working on AV regulations.
- Automotive manufacturers and technology companies developing AVs.
- Research and development centres involved in AV testing.
- Technical services for type approval and safety assessors.
- National and regional authorities responsible for authorizing AV testing and deployment.
- Transportation and mobility sector stakeholders interested in automated driving technology.

Funded by the European Union

2 Current legislative basis in European countries

The analysis of testing procedures and administrative framework conditions on AV testing on public roads[7] revealed that even though some countries share common concerns such as safety, ethical considerations and the need for data management, there is clear diversity in their legislative approaches. In Europe, 22 countries have a framework for AV testing on public roads. 9 countries implemented a special legislation dedicated to automated driving – Austria, Denmark, France, Germany, Greece, Norway, Slovakia, Spain and Sweden. 11 countries adapted their national acts to allow testing of AVs on public roads or consider their existing national acts (mostly the road traffic act) as not prohibiting automated driving – Belgium, Czech Republic, Finland, Hungary, Italy, Lithuania, Luxembourg, Netherlands Poland, Slovenia and Switzerland. 2 countries allow testing based on guidelines or a code of practice, established as a regulatory basis for automated driving, even without having a special act on CCAM testing – Latvia and the UK. Anyhow, also the countries with no corresponding regulatory framework state their interest in supporting the development of automated driving technology and implementing an automated mobility system.

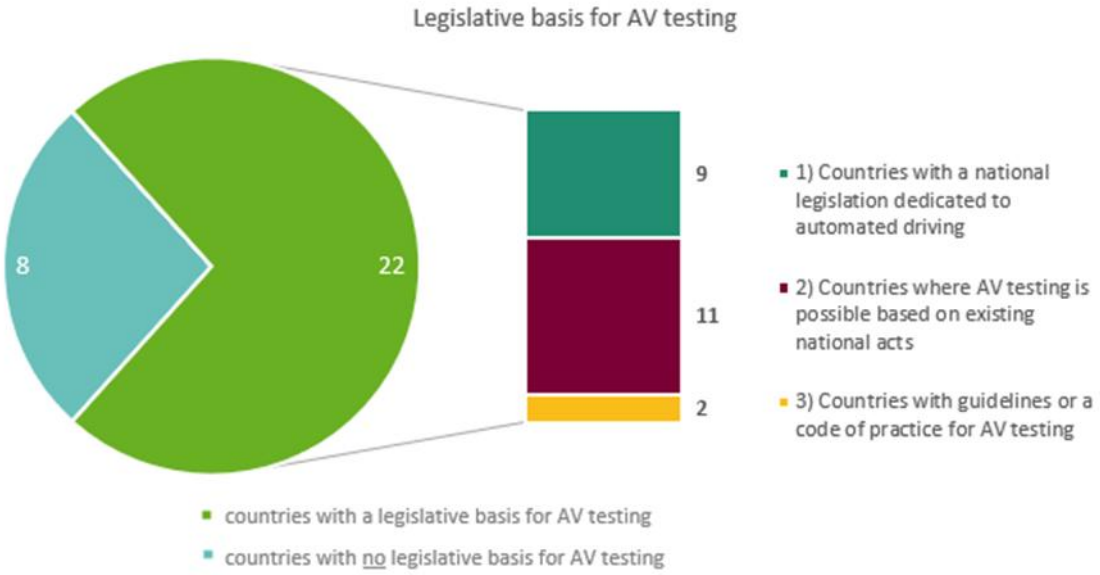


Figure 2: Number of countries where testing AVs is possible differentiated by category of legislative basis

Throughout Europe, some advanced and some higher technology-open legislative approaches can be highlighted. For example, Germany and France are set into focus when it comes to automated driving on public roads with Level 4 vehicles, even beyond testing (in Germany) and with no operator in the vehicle (also in France). Looking at the UK, unlike in most of the other countries allowing AV tests, the trialling organisation does not need to obtain a test permit for testing on public roads. Each trialling organisation needs to ensure by means of self-assessment that the planned test complies with the law and all relevant regulations, like having (a) a driver or operator, whether in or out of the vehicle, who is ready, able, and willing to resume control of the vehicle, (b) a roadworthy vehicle and (c) appropriate

[7] FAME deliverable D5.1 available at https://www.connectedautomateddriving.eu/analysis-ccam-testing-procedures/

insurances are in place. In 2023 the UK created a new safety framework for commercial deployment of AVs, addressing clear liability for the user, safety threshold for self-driving, and a regulatory scheme to monitor the safety ongoing. The technical requirements for the safety framework that the UK is currently developing could also serve as a basis for a harmonised European framework for AV testing on public roads.

Some further examples of legislative approaches open for innovation can be found in Finland or Italy for instance. Finland established a test plate certificate procedure that is quite flexible and adapts to new technologies. It provides a structured framework for tests with non-type approved AVs. Italy stated its intention to enable quick testing and development of emerging technologies. Therefore, it created a legal and procedural environment ("Sperimentazione Italia") providing projects with an exemption from current legal provisions for a specified timeframe.

Throughout all regulations, the requirement for the presence of a safety operator is evident as the fundamental safety mechanism for testing on public roads. Some countries set stronger restrictions on operators, others are less strict. For example, France currently is working on a legal basis to allow remote operators to manage more than one vehicle at the same time. Therefore, specific conditions need to be defined.

Previous EU-funded pilot projects show that the lack of common procedures and regulations for testing AVs on public roads has been a major challenge, especially when it comes to cross-border testing. Harmonisation is essential to guarantee the safe and efficient integration of CCAM technologies into the European transportation network. This requires harmonisation already during the testing phase. Thus, this report provides recommendations for a harmonised European framework for AV testing on public roads.

Funded by
the European Union

3 Safety validation responsible

In the EU, as presented in FAME deliverable 5.1, different approval authorities have diverging capabilities and structures. This is the reason why FAME's recommendations do not define just one option for the safety validation responsible. It is expected that each country's authority chooses one of the following options, studying which is the most appropriate one for each application. The three considered options for the safety validator entities are:

- Applicant (by self-assessment).
- Approval authority.
- Third party assessor (e.g., technical service).

The decision about who should be the safety validator must be made by the corresponding approval authority considering two main aspects:

- Capabilities of each safety validator option.
- Complexity and risk of the activity to be validated.

A validation performed by the applicant, or the approval authority would make the process to obtain the permit faster. It is only recommended for those cases in which the complexity and risk of the activity is low according to chapter 8.2 Test-specific risk evaluation.

For cases in which the activity is complex or risky a validation performed by a third party would be necessary unless the capabilities and resources of the approval authority for performing the validation are high enough to validate a complex or risky activity.

The selected safety validator will be responsible for reviewing the documentation provided by the applicant, ensuring fulfilment with the requirements set by the application process. In case, the safety validation responsible is the applicant, by means of self-validation, activity risk evaluation should be performed jointly with the approval authority as stated in chapter 8.2.

Funded by
the European Union

4 Safety operator

The concept of a safety operator as defined in this document is distinct from that of an operator as defined in EU 2022/1426 involved in deployment activities for type-approved Automated Driving Systems (ADS). According to EU 2022/1426 [2], an operator is a person located either inside (on-board) or outside (remote) the vehicle whose role is to ensure vehicle control in hazardous situations. However, it is important to note that the operator does not drive the AV; instead, the ADS continues to perform the DDT.

As defined in this document, a safety operator has broader safety responsibilities. In the context of testing AVs, it is crucial to understand the role of the safety operator. These vehicles, still under development, may demonstrate a certain level of safety but cannot be guaranteed to always be robust in all conditions.

A safety operator must:

- Always be engaged and supervise the vehicle's systems to detect potential issues the vehicle itself might not identify
- Order the ADS to start a minimum risk manoeuvre. In this situation, the safety operator does not drive the AV and the ADS shall continue to perform the DDT.
- Take over the control of the DDT partially or fully when necessary (unlike standard operators in deployed vehicles).

Safety operators can be positioned either inside the vehicle or operate remotely. Their role is critical in maintaining safety during testing phases, where the automated systems are not yet fully proven in all scenarios. This expanded role of supervision and potential full control is aligned with the Homologation Testing Subgroup (HTSG) guidelines [3] and distinguishes safety operators from operators as per EU 2022/1426, making them an essential component in the development and testing of AVs. Their presence ensures an additional layer of safety and control during the crucial testing phase of these evolving technologies.

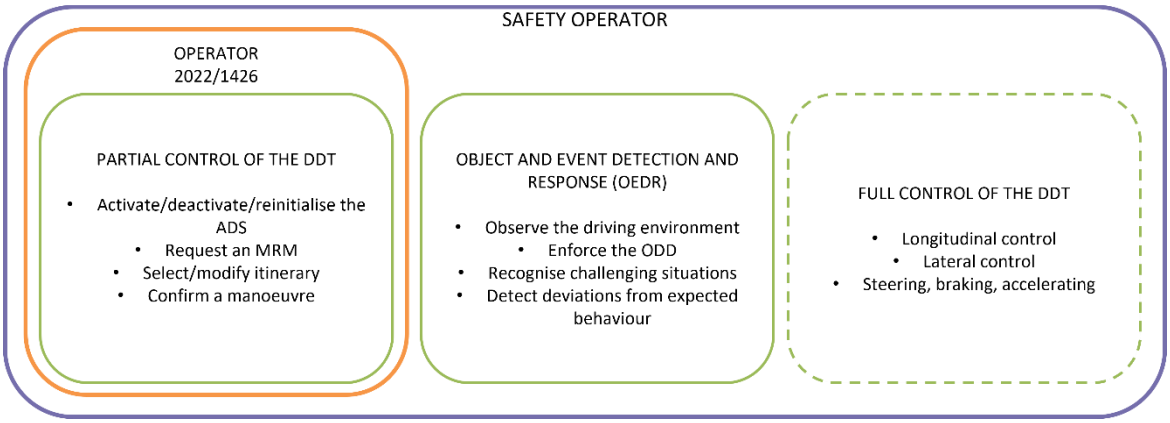


Figure 3: Diagram. Evolution from operator as per regulation (EU) 2022/1426 to safety operator.

Funded by
the European Union

4.1 Safety operator requirements

- The vehicle safety operator will always be accountable for monitoring and intervening to handle the vehicle in risky conditions.
- During operation, the safety operator shall be able to always take control of the vehicle, whether he or she is inside the passenger compartment or operating it remotely. In any case, the safety operator will be obliged to take control of the vehicle in the event of any eventuality that poses a risk situation to the occupants of the vehicle or to other road users.
- Each safety operator shall be properly trained to supervise or perform the testing activities in which they are involved, including the execution of minimal risk manoeuvres when required.
- Each safety operator shall have a valid driving license according to the vehicle type and necessary jurisdictions.
- The use of remote safety operator(s) exclusively, shall be evaluated by the safety validator, considering the information contained in the system documentation package and in the tests' description. Further requirements for this point can be found in chapter 5.2.3.

Funded by
the European Union

5 Test permit procedure

To test the prototype vehicle on public roads with development aims, the applicant must comply with the specific requirements of the country, which could contain items as the registration and insurance of the vehicle, the permit for testing or even the notification to the concerning road operator or authority.

In this part of the document, recommendations for procedures or actions necessary to obtain the permit for testing are provided. This is divided into a mandatory first documental submission and a second documental submission if the safety validator, based on the risk assessment, determines that additional evidence of safety is necessary

This framework is designed with flexibility at its core, allowing for customization based on each specific use case, ODD, and system under consideration. It is expected that a qualified safety validator will review and adapt these guidelines as necessary for each application. Not all steps and points outlined in this document will be required for every test scenario; instead, they should be selectively applied based on the complexity, risk level, and unique characteristics of each proposed test.

How safety validators apply these guidelines in practice can be based on different key factors that directly impact the safety of the testing activity. For instance, applications involving remote safety operators, cross-border testing, or extensive system modifications will typically trigger more stringent documentation requirements and pre-testing procedures. Conversely, tests with limited scale, established safety operators, and minimal modifications might follow a more streamlined process. By considering these factors within the flexible framework, safety validators can ensure that oversight is proportionate to risk, applying appropriate scrutiny where needed while avoiding unnecessary administrative burden for simpler test scenarios.

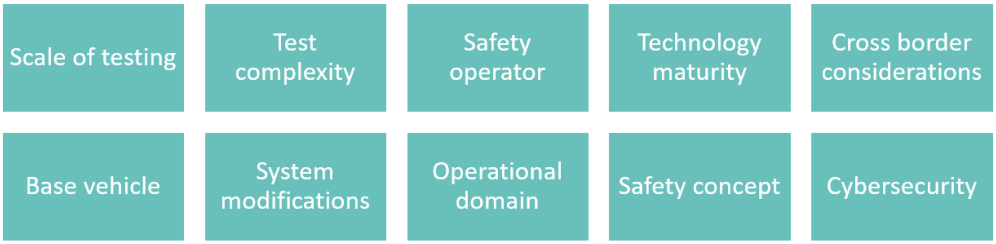


Figure 4: Main key factors influencing test permit procedure assessment

This procedural framework, depicted in Figure 5Figure 5: Diagram workflow of the first documental submission test permit procedure, is grounded in national AV testing legislations such as the Spanish national legislation for AV testing, specifically the VEH 2022/07[4] regulatory framework, and draws substantial guidance from the Homologation Testing Sub Group (HTSG) and its "Guideline on a Uniform EU-Wide Procedure for the Subjects of Pre-Type Approval Assisted (ADAS) and Automated Vehicle (ADS) Testing and Recognition of Testing Approvals among Member States"[3]. By integrating these authoritative sources, the document provides a comprehensive and harmonized approach to testing permit procedures, reflecting both national regulatory requirements and the broader European perspective on AV testing protocols.

Funded by the European Union

5.1 First documental submission stage

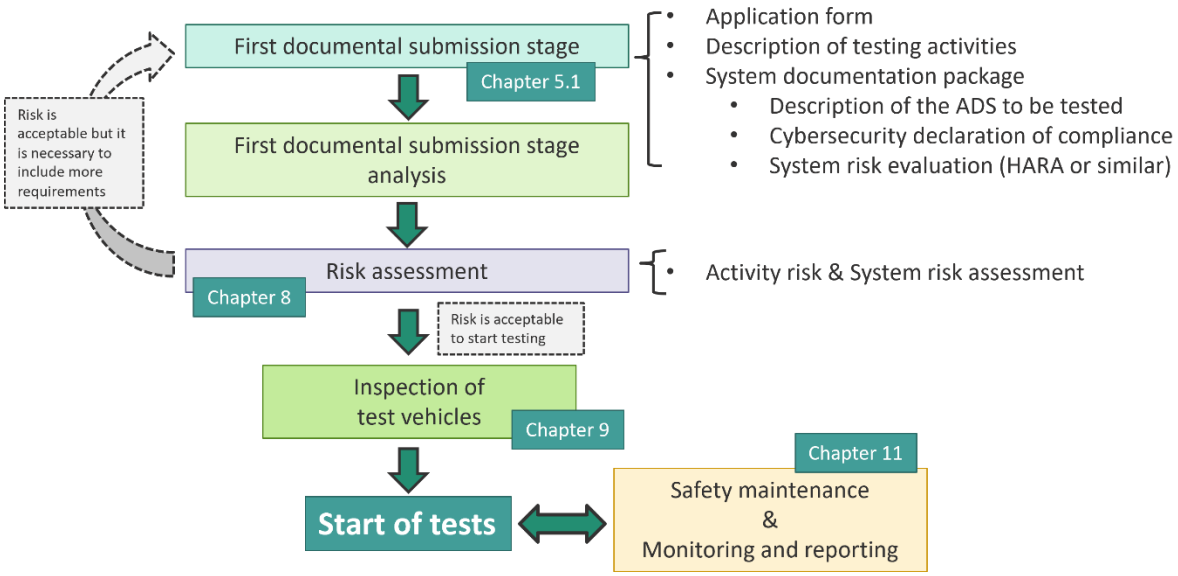


Figure 5: Diagram workflow of the first documental submission test permit procedure

As the first step, the following documents shall be submitted to bring to the safety validation responsible a clear overview of the testing plan. The structure and contents described below are indicated as a recommendation. In the case in which, due to the nature of the tests, a different level of detail may be required, the safety assessor can flexibly define variations to such information.

5.1.1 Application form

An application form should be submitted. Example of the content of the application form is in Annex I – Application form content example.

When an applicant intends to test multiple vehicles with identical hardware, software configurations, and ODD within the same testing activity, a streamlined approach to the test permit process is recommended. The safety validator should approve a single comprehensive application that covers all identical vehicles rather than requiring separate full applications for each individual vehicle.

The application must clearly specify the number of vehicles (n>1) to be deployed and provide unique identification for each vehicle (such as VIN numbers) as stated in 5.1.2. While the technical documentation regarding the automated driving system from 5.1.3 and risk assessment may be shared across all vehicles.

5.1.2 Description of testing activity

A comprehensive description of the test activity to be carried out on public road shall be attached to the application form, including:

- Objectives of the activity.
- Connected/automated features to be deployed.
- Description of the scenarios and test procedure to be tested for each feature.
- Detailed time schedule for the activities of the testing plan.
- Identification and detailed description of the area requested to carry out the tests.
- Physical and Digital Infrastructure (PDI) requirements for the test setup

Funded by the European Union

- Identification of the affected populations.
- Number and characteristics of vehicle(s):
  - Information allowing vehicle(s) identification such as VIN.
  - Type of vehicle(s)[8] including dimensions and masses.
  - Base approval and description of the modifications. (If based on type approved vehicle).

  The template given in "Annex II – Template for test vehicle data" shall be followed for each vehicle under test provided they have different hardware and software configurations.

- Safety operator documentation: training requirements of the safety operator should be acknowledged in dependency of the maturity of the ADS function and the safety concept.

  - Documentation describing the safety operators' training program implemented to favour safety while testing.
  - Declaration certifying under applicant's responsibility that safety operators know the technology and systems of the vehicle and have received the described training.
  - Reporting responsibilities and action plan in case of a critical/non-critical occurrence.
  - Monitoring processes and responsibilities.

5.1.3 System documentation package

The applicant shall provide a documentation package which gives access to the basic design of the system and the means by which it is linked to other vehicle systems or by which it directly controls output variables as well as off-board hardware/software and remote capabilities.

5.1.3.1 Description of the automated driving system to be tested

As part of the documentation package, a description of the automated driving system to be tested shall be provided. Including control strategies of the system and the methods employed to achieve the objectives, including a statement of the mechanism(s) by which control is exercised. Including contents as the following ones:

1. Name of the function(s)

2. Original Software version(s) of the function(s) following chapter 11.4 Software version traceability

3. Description of control functions of the system, including:
   - Sensing and perception: input variables such as sensors involved in gathering all real-time data and their involvement in perception.
     E.g. Camera captures images of lane markings and image processing is used to identify lines on the road.
   - Decision making and planning: based on sensor data how decisions are made.
     E.g. Path planning and trajectory generation determine the optimal trajectory the vehicle should follow.

[8] https://alternative-fuels-observatory.ec.europa.eu/general-information/vehicle-types

- Control execution: actions or signals that the system generates to control the vehicle in response to the input data. In other words, how previous decisions are implemented.
  E.g. The control adjusts the steering angle to maintain or adjust the vehicle's lateral position in the lane. It also controls brakes, electric motors and hydraulic systems that physically alter the vehicle's direction and speed.

4. Operational Design Domain (ODD)
   Refers to operating conditions under which the system is specifically designed to function, including, but not limited to:
   - Infrastructure: Road type (highway, urban, rural), curvature and incline, lane markings, for instance.
   - Traffic conditions: Traffic density, behaviour of surrounding vehicles (e.g. lane changing). Roadwork and Obstructions (temporary lane diversions, cones, and roadblocks that alter normal lane patterns)
   - Environmental conditions: weather (clear, rainy, or snowy conditions), lighting (daytime, nighttime, or low-light conditions)
   - Speed range: range of speeds within which the automated driving function is designed to operate
   - Lateral/longitudinal acceleration range: range of accelerations within which the automated driving function is designed to operate

   It is strongly advised to standardize the ODD description. For formatting, it is recommended to adhere to the guidelines outlined in ISO 34503 (2023) for the ODD definition format.

5. Boundaries
   Means the boundaries of the external physical limits within which the ADS is able to perform the dynamic driving tasks including, but not limited to road surface condition, other road users, adverse weather conditions (fog, mist), imminent collision risk, failures, reduction in the maximum operating speed.

Table 1. Exemplary summary of the ADS attributes to be defined.

Function(s)	SW version(s)	Description	Operational Design Domain	Boundaries
Automated lane keeping	V0.1 V0.9 V1.2	- Sensing and perception - Decision making and planning - Control Function	- Infrastructure - Traffic conditions - Environmental conditions -Speed range - Lateral/longitudinal acceleration range	- Inclement weather - Light conditions - Pedestrians
Automated collision avoidance	V0.3			

5.1.3.2 Compliance with traffic regulations

The country-specific requirements must be known and respected from the beginning of the development and application process. Applicants testing across different jurisdictions must follow chapter 7 “Mutual recognition” and consider not only the written traffic rules but also local driving customs, road conditions, and infrastructure characteristics particular to each testing area, ensuring the automated system can safely interact with other road users in all proposed operational environments.

Table 2. Traffic legislation compliance per function

Function	SW version	Will the system comply with traffic legislation?
e.g. Automated lane keeping	VX. XX	Yes/No/Why and in which circumstances e.g. The system will cross solid lanes when facing obstacles in the current lane

For cross-border testing, special attention must be paid to the adaptation mechanisms that allow the system to transition between different regulatory frameworks. Evidence of regulatory compliance should be provided, along with clear descriptions of how the system responds to situations where compliance with specific traffic regulations becomes challenging.

Table 3. Traffic legislation compliance per country and compliance challenges

Country	Assessed	Comments on any restrictions
e.g. E9 Spain	Yes/No	

5.1.3.3 Optional extra requirements

In case the safety validator considers it as necessary, it can request to the applicant to include more evidence about the topics listed below.

1. Specific road events the function will not be able to respond to:
   Scenarios or conditions that the automated driving function is not designed to handle. For instance, toll station, end of highway, permanent lane ending, railway crossings, long terms construction zone, intersections, tunnels, traffic lights, etc.
2. Assistance Termination Strategy.
   This strategy outlines how and when the automated function will disengage or alert the operator if it can no longer operate safely.
3. (Remote) Safety operator unavailability response.
   System's response if a remote safety operator (or onboard safety operator) is unavailable to take over control when required. This might involve minimum risk manoeuvres (MRM) such as the vehicle stopping safely or moving to a safe location until control can be reassumed.

Funded by the European Union

Table 4. Optional requirements on the description of the ADS

Function	Specific road events the function will not be able to respond to	Assistance termination strategy	(Remote) Safety operator unavailability response
	Toll Station End of highway Permanent lane ending Railway crossings Long terms construction zone Intersections Tunnels Traffic lights		

4. Modifications to the type-approved systems of the vehicle.
   These modifications could involve integrating sophisticated computer control systems, adding complex sensor networks like LIDAR and radar, and implementing advanced electronic control units that can safely manage vehicle dynamics.
   The primary objective is to ensure the modified vehicle meets rigorous safety standards and regulatory requirements while maintaining the core performance characteristics of the original type-approved system.

5. Override implementation:
   The applicant should include in the documentation package information regarding how the system detects and reacts to an override performed by the safety operator, including the following situations:

   - The safety operator activates the braking system
   - The safety operator accelerates
   - The safety operator intervenes in the steering system

   In addition, the behaviour of the system after an override should be described.

6. Emergency disconnection implementation fulfilling:
   - The system shall have an emergency disconnection that stops the action of the actuators (steering wheel, brake, accelerator and gearbox if applicable).
   - The emergency stop must be accessible to any occupant of the vehicle or any operator with access to the vehicle controls, including to remote safety operator, if applicable, at any time.

Funded by the European Union

It must be justified that the emergency stop, and the override are independent of each other and of the autonomous driving algorithms and that they will always have priority over the autonomous driving actions.

7. Applicant's PDI Readiness
   - Communication Systems: The applicant should demonstrate compatibility with local cellular networks, showing adaptability to varying connectivity levels along the route. They should outline fallback mechanisms for communication failures, including safe-stop procedures and local decision-making capabilities.
   - Digital Map Integration: The system should be able to use and update HD-maps in real-time. The applicant must describe methods for handling discrepancies between onboard maps and actual road conditions, explaining decision-making processes when faced with conflicting map information.
   - CCAM Interaction: If the vehicle is capable of receiving and processing V2X messages or any CCAM message types. The applicant should provide examples of how CCAM data influences vehicle behaviour and decision-making, demonstrating integration of CCAM information with onboard systems.
   - Remote Operation Capabilities: If a remote operation system will be used, technical specifications of the system should be provided. The applicant must outline strategies for latency management and related safety protocols, describing failsafe mechanisms for connection loss. This is further developed in chapter 5.2.3

5.1.4 Cybersecurity declaration of compliance

The applicant must present a declaration that all test vehicles, as well as all their systems and subsystems, have been developed taking into account the provision of appropriate cybersecurity levels. A signed declaration using the model in Annex III – Compliance with cyber security template should be submitted. In case the safety validator considers it as necessary a cybersecurity management plan should be designed following the process described in chapter 10 Cybersecurity management plan.

5.1.5 System risk evaluation

To identify and categorize hazardous events regarding automated driving systems and functions and to specify safety goals related to prevention or mitigation of the associated hazards, the applicant should submit a system's risk evaluation. Safety by design can be implemented through process analysis following specific automotive industry standards such as HARA (hazard analysis and risk assessment), FMEA (failure mode and effects analysis) and FTA (fault tree analysis).

These standards and methodologies are presented as recommendations, it's crucial to note that adherence to specific standards like HARA or any other is not mandatory. Instead, these are provided as examples of well-established methodologies encouraging the adoption of industry-recognized practices that can contribute to a more consistent and comprehensive approach to safety evaluation.

For example, following ISO 26262[5] part 3 where HARA is defined, a risk assessment process would ideally include the following steps.

Funded by the European Union

1. Potential hazards identification: Identifying possible sources of harm or potential hazardous events of the function derived from operational situations and operating modes and its consequences.

2. Classification of hazardous events:

   - Severity: The severity of potential harm shall be estimated. This can be determined using the severity table from ISO 26262-3:2018.

Table 5. Classes of severity for risk assessment

	Classes of severity			
	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

   - Exposure: How likely you are to encounter a situation in which an error may have an impact.

Table 6. Classes of probability of exposure for risk assessment

	Classes of probability of exposure regarding operational situations				
	E0	E1	E2	E3	E4
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

   - Controllability: To what extent people involved in the hazardous event can still avoid injury by reacting in time in the event of a malfunction. For this purpose, it is assumed that the safety operator is in appropriate condition, has the proper driver training and is complying with applicable legislations.

Table 7. Classes of controllability for risk assessment

	Classes of controllability			
	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

3. Risk Assessment: Evaluating the severity of the consequences, the exposure and the controllability of occurrence for each identified hazard to determine the level of risk. Based on the classification of ISO 26262 an Automotive Safety Integrity Level (ASIL) is determined. ASIL A, B, C and D where ASIL A is the lowest safety integrity level and ASIL D is the highest.

Funded by the European Union

4. Risk Mitigation: Implementing measures to reduce the identified risks to an acceptable level by either eliminating the hazard, reducing its likelihood, or mitigating its consequences to bring the vehicle to a safe state.

As a simplified example, let's analyse a hazard of remote operation.

1. Hazard related to loss of connectivity during remote operation
2. Severity: S3 – Potentially fatal injury
   Exposure: E3 – Medium probability (depends on the route and network coverage)
   Controllability: C3 – Difficult to control or uncontrollable (assuming no immediate human intervention possible)
3. ASIL D (highest safety integrity level due to the combination of high severity and difficult controllability)
4. Safety goal: The remote operation system shall ensure safe vehicle behaviour in the event of connectivity loss. Safety is covered from mitigation and prevention strategies such as:
   - Design test routes with robust and redundant communication infrastructure.
   - Implement an automated MRM to bring the vehicle to a safe state upon detecting connectivity loss.
   - Develop and test fallback systems for local decision-making in the absence of remote control. Establish clear thresholds for connectivity quality below which MRM is automatically initiated.

The items defined above should be evaluated considering the characteristics of the testing activity, such as, location, technologies to be deployed or experience of applicant and of people involved in the activity, such as safety operators.

5.2 Second documental submission stage

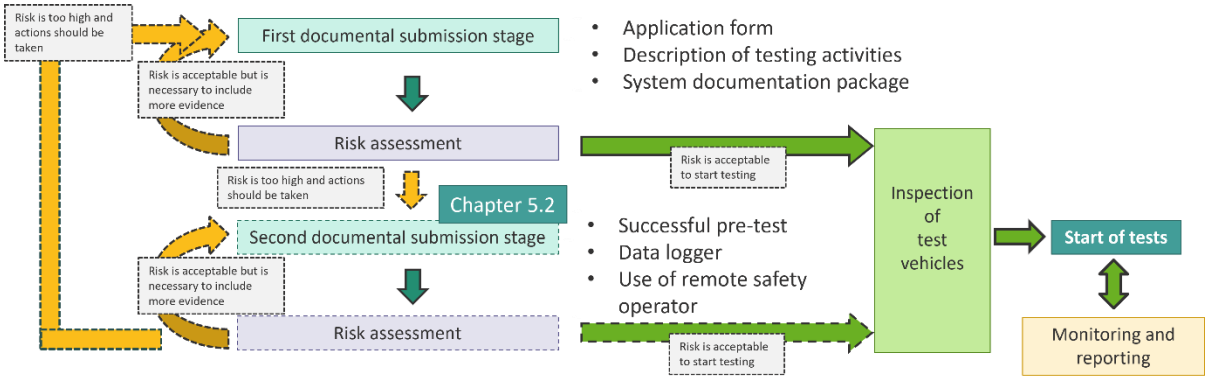


Figure 6: Diagram workflow of the first and second documental submission test permit procedure

After analysis of the documents in the first documental submission stage and the risk assessment of chapter 8 Risk Assessment, the risks associated with testing may be too high due to key risk factors such as:

1) Large scale testing involving multiple vehicles or extensive public road exposure,

2) Absence of an onboard safety operator,

3) Use of prototype vehicles that have not received type approval, and

4) Cross-border testing involving different regulatory environments.

Additional high-risk factors include testing new features, navigating complex, dynamic traffic conditions such as roundabouts, operating in mixed traffic environments with unpredictable elements, challenging road conditions or extreme weather conditions (e.g., heavy snow in a low adherence road surface) or when testing could involve safety-critical responses. Other risk factors include high-speed testing, abrupt manoeuvre testing, or testing in challenging areas for the safety operator (e.g., dense traffic, crowded areas).

Furthermore, we can find risk associated to the vehicle construction itself. For instance, when the vehicle lacks essential safety features such as active safety systems like seatbelts and airbags or does not have seating, lateral and longitudinal controls.

Due to these elevated risks, the safety validation responsible may ask the applicant for further requirements in order to verify the capabilities for safe operation on public roads. These can be:

- Successful pre-tests on proving ground.
- Use of Data Logger.
- Use of remote safety operator.

This second documental submission should identify and verify the behaviour beyond the system capabilities. Specifically, it has to certify the following aspects:

- Demonstrate the ADS capabilities within the ODD and certify the behaviour outside the ODD.
- Demonstrate the ADS capabilities by regularly occurring conditions, like for example fog, rain, snow etc., and document the situations the ADS is incapable of or does not operate reliably.
- Describe what kind of measures will be taken to react to a situation the ADS is incapable of handling or that is outside of the ODD, like notification, transferring the control to the operator, transition to minimum risk condition etc.

5.2.1 Successful pre-tests on proving ground

The safety validation responsible may request the applicant´s verification of ADS's behaviour by means of conducting tests or methods for safe operations on public roads. These tests can take place on a track or road closed to traffic. These tests can be based on dynamic tests listed in chapter 6 and/or on additional scenarios not covered in this document. The responsible authority may define the required scope of the tests depending on the analysis of the documents in the first documental submission and the risk assessment in chapter 8.

Tests listed in chapter 6 are indicated as a reference and may not be required in their totality in the case in which the responsible authority does not deem all of them necessary.

New test definition can be developed by means of simulations. These tests may be supervised or not by the safety validation responsible. Evidence of results shall be provided.

5.2.2 Use of Data logger

The safety validation responsible may request the applicant to include a data logger system in the vehicle during testing, taking into account the risk assessment from the first stage.

A data logger for AV testing is a comprehensive system or device within a vehicle designed to continuously record, store, and retrieve a wide range of vehicle operational data. This may include, and is not limited to, dynamic time-series data, crash event information, interactions between the

Funded by the European Union

ADS and human operators, system activations and deactivations, failures, and other significant driving events. The data logger captures both routine operational data and critical incident information, providing a holistic view of the vehicle's performance and behaviour over time.

5.2.2.1 General requirements

- Data accessibility and readability: The applicant must provide all collected data in an easily accessible and readable format. This includes using standard file formats, clear documentation, proper organization, and metadata. If proprietary formats are used, necessary interpretation tools must be provided ensuring efficient analysis without requiring specialized systems.

- Data availability during power loss: Data must remain retrievable even if the vehicle's primary power supply is compromised, ensuring that testing authorities can access critical data after a major event or system failure.

- Data durability post-Collision: The data logger should withstand severe impact forces, high deceleration, and mechanical stress to ensure data integrity in the event of a collision.

- Sufficient data capacity: Adequate storage capacity to log all required ADS performance data as specified, ensuring continuous monitoring over the entire duration of testing.

- Fallback storage in case of off-board transmission failure: If data designated for off-board storage cannot be transmitted (e.g., due to connectivity issues), the data must remain stored on the vehicle until it can be successfully retrieved, ensuring data continuity.

- Clear time-stamped event logs: Precise timestamps for each event, allowing an accurate reconstruction of system performance and human-vehicle interactions during testing.

- Data retention period: Define a minimum retention period for data to support investigation and analysis post-testing. Retention policies should adhere to data privacy regulations, such as GDPR[6], with specified durations for stored data.

- Compliance with Data Privacy Laws: All data handling procedures must follow GDPR and other relevant privacy laws to protect sensitive or personally identifiable information collected during testing.

5.2.3 Use of remote safety operator

The use of a remote safety operator can be required when there are limitations and risks associated with relying solely on an on-board safety operator or even when this operator cannot be inside the vehicle due to vehicle design.

A remote safety operator helps addressing these challenges by providing continuous, real-time monitoring and control capabilities, ensuring the safety and reliability of AV systems in rigorous testing environments. This approach allows for a more comprehensive evaluation of ADS functionality while maintaining the highest possible safety standards for operators and the public. A remote safety operator performs the entirety or part of the DDT, sometimes in conjunction with an ADS starting from Driving Automation Level 3. The DDT consists of operational and tactical functions. Operational functions refer to the lateral and longitudinal motion control (e.g., steering and brake/throttle control,

respectively). Tactical functions include sub-tasks related to Object and Event Detection and Response (OEDR), e.g., planning and execution for object avoidance, and expedite route following.

The European Commission is intensifying its focus on remote operations to promote sustainable and intelligent mobility solutions. This commitment is exemplified by project calls like HORIZON-CL5-2025-01-D6-01, titled "Advancing remote operations to enable the sustainable and smart mobility of people and goods based on operational and societal needs (CCAM Partnership) – Societal Readiness Pilot." This initiative aims to develop a comprehensive set of principles, guidelines, and requirements for remote operations, addressing operational complexities such as safety, cybersecurity, liability, privacy, certification, operator training, interoperability, and cross-border operations. By establishing a standardized approach, the project seeks to extend the Operational Design Domain (ODD) of Cooperative Connected and Automated Mobility (CCAM) solutions, thereby enhancing their applicability and societal acceptance.

An example for a remote operation is provided by EINRIDE [7] operating all-electric and automated SAE Level 4 heavy trucks on public road. EINRIDE received permission in the US, and for testing in several EU countries (e.g. Sweden). Practically, the EINRIDE remote operator is supervising the ODD conditions during operations, and provides assistance to the ADS through suggested inputs during operations particularly in cases where the ADS cannot handle a condition.

5.2.3.1 Requirements and best practices

Considering the EINRIDE best practice the safety challenges to be considered when regulating remote operations are specifically:

- Staff training.
- Staff health, fitness and vetting.
- Staff attention and rest periods.
- Ergonomic workstation layout.

With regards to the needs and requirements on the remote safety operations the following should be considered:

- Incident protocols.
- The adequacy of the communication network and connectivity.
- Cybersecurity.
- In the case of connectivity or other remote failures the ADS should execute an appropriate minimum risk manoeuvre.
- The remote safety operator should hold an appropriate licence for the vehicles operated and necessary jurisdictions.
- The remote safety operator is permitted to assist in the event the vehicle enters into a minimum risk mode and, e.g. to direct into a reboot or resume position to reactivate the ADS.
- The applicant should submit a safety case on how the vehicle will be operated safely.
- The dedicated entity can be required to provide evidence of their good reputation, financial stability, professional competence, and capability to operate within the ODD.

5.2.3.2 Documentation for use of remote safety operator

- Certifications and licenses to ensure that the safety operator is able to drive safely.

- Documentation that connectivity is suitable.
- Documentation of minimum risk manoeuvres.
- Documentation of training, vetting, health checks etc.
- Documentation that passengers and freight are safely and securely loaded.
- Documentation on the maintenance of the vehicles (updates, cybersecurity).
- Provide insurances for the vehicles and full liability coverage.
- In the case of incidents provide video and data recordings.

5.3 Case Study: Applying the FAME Framework to Hi-Drive Use Cases

This chapter demonstrates the practical application of the FAME framework to exemplary use cases from the Hi-Drive project. The alignment between these projects represents a strategic bridge between theoretical frameworks and practical implementation of a demonstrator to test an AD functionality on public roads.

Through a comprehensive safety validator assessment, we examine how FAME's requirements for documentation, risk assessment, safety validation, and cross-border testing would apply in this Hi-Drive example use cases. This assessment covers critical aspects including technical modifications, V2X communications, cybersecurity measures, and testing protocols.

Figure 7: Example view for on Hi-Drive Vehicle demonstrator vehicle.

The Hi-Drive example use cases have been derived from the actual use cases that are tested in Hi-Drive. A description of the Hi-Drive demonstrator vehicles is available in Deliverable 3.3 “Description of vehicles” (Vignard et al., 2023). The basis for the example Hi-Drive use cases was Deliverable 5.3 “Description of Operations” (Sauvaget et al., 2023). This basis has been extended by last considerations from the project. A description of example Hi-Drive use cases can be found in “ANNEX VII – Hi-Drive use case description”.

The objective of this analysis is not to decide whether the described systems would be approved in real cases, but rather to discuss which steps and information would be required according to the FAME framework, serving as a valuable reference for regulatory authorities, technology developers, and safety validators.

Funded by
the European Union

5.3.1 Tests are carried out only in one country

In this use case the tests of the AD system are carried out only in one country and a specified ODD. In this case the ODD are urban roads up to a speed limit of 50 kph.

A research vehicle is built up to test a functionality on public roads. The purpose of the test is to study technical capabilities of an AD system. The original vehicle is an already type approved one. To enable automated driving (AD) several changes are made:

- The braking and steering system is changed to a protype system.
- Additional sensors of different kinds (radar, LiDAR) are installed in the vehicle. The sensor set up can be presumed suitable for the ODD.
- The HMI (cluster display, switches) are changed to activate the system.

Additional safety layers are installed in the vehicle to allow the driver to override the AD system at any time.

- Redundancy for sensors and power supply.
- Emergency power off switch.
- System monitoring displays.
- The vehicle is only operated by a trained safety driver which has certain internal driving license.

During the test period the logic of the AD system as well as the sensors that are used for the AD system are changed to investigate the technical implications of different configurations.

For the following sub-use-cases it shall be considered that the research vehicle is built up by the OEM that has homologated the original vehicle.

5.3.1.1 Safety assessment

System Modifications

☑ Modified series vehicle with full sensor setup (cameras, LiDAR, radar).

⚠ **CONCERN**: Prototype braking and steering systems represent significant safety-critical modifications.

❓ **RECOMMENDATION**: Detailed documentation of these system´s safety architecture and fail-safe mechanisms required to assess the modifications performed. If considered relevant track tests from “6.3 Manual driving tests” should be performed.

Sensor Configuration

☑ LiDAR with 360° field of view for reference measurements of dynamic and static objects.

☑ Outside camera with 120° horizontal field of view for depth estimation and object detection.

☑ GPS and IMU for vehicle positioning via Ethernet interface.

⚠ **CONCERN**: The use of sensors will change during the test to investigate advantages and disadvantages.

❓ **RECOMMENDATION**: Clarify the different sensor setups and the relation to the safety security.

Safety Operator Arrangements

☑ Professional safety driver with specialized training.

☑ Emergency stop switch accessible to both driver and co-driver.

☑ Two-hand switch for ADF activation shows good safety practice.

☑ Logging of AD status and driver interventions.

❓ **RECOMMENDATION**: Clarify the emergency procedures when pressing the emergency stop switch.

HMI Design:

❓ **RECOMMENDATION**: The HMI concept with the vehicle (remote) safety operator when ODD limits are approached and then reached shall be explained. Signals (visual, acoustic, haptic) and information given to the (remote) safety operator and vehicle occupants shall be described.

Data Logging

☑ Raw data recording capability.

☑ Fusion object level recording.

☑ 0.24 TB/h data volume capacity.

❓ **RECOMMENDATION**: Consider providing evidence for the general requirements from 5.2.2.1.

Processing Requirements

☑ Sufficient network capacity and computer hardware (GPUs) for data processing.

☑ Neural network processing capabilities for handling video streams.

Testing Environment:

⚠ **CONCERN**: Urban testing involves complex scenarios with vulnerable road users.

❓ **RECOMMENDATION**: More detailed definition of the test scenarios to perform. Gradual approach to testing complexity needed. This information was not available to the author yet, but it is presumed that this is available.

ODD Definition:

☑ Clear speed limitations (up to 50 kph).

☑ Environmental limitations defined (temperature >3°C, no adverse weather).

☑ Boundaries: Construction sides (Roadworks).

V2X Testing

⚠ **CONCERN**: V2X testing at "preselected intersection" needs detailed protocols.

⚠ **CONCERN**: No information on V2X security measures.

❓ **RECOMMENDATIONS**: Require specific documentation for V2X testing scenarios, validation objectives, security measures and fallback procedures (if applicable).

Cybersecurity Considerations

⚠ **CONCERN**: Extensive HMI modifications, exposed vehicle network ports, and integrated V2X communications in place, all of which introduce potential cybersecurity vulnerabilities. No evidence of a risk assessment like TARA (Threat Analysis and Risk Assessment). This information was not available to the author yet, but it is presumed that this is available.

❓ **RECOMMENDATION**: Conduct comprehensive TARA as required by FAME framework chapter 10 addressing vulnerabilities in Annex IV.

Safety concept

⚠ **CONCERN**: No explanation of the design provisions built into "The System" so as to ensure functional and operational safety, such as:

- fall-back to operation using a partial system,
- redundancy with a separate system,
- diversity of systems performing the same function,
- removal or limitation of the automated driving function(s),
- second (back-up) means (i.e. change-over mechanism to driver).

❓ **RECOMMENDATION**: Develop comprehensive failure mode effects analysis (FMEA) or similar.

❓ **RECOMMENDATION**: Description of the design provisions such as partial performance mode of operation under certain fault conditions (minimum risk manoeuvres) (state the conditions).

Conclusions

1. **First Submission Stage**:
    - Complete system documentation package with detailed descriptions of prototype systems.
    - Safety concept documentation with failure mode analyses for modified braking/steering systems.
    - Comprehensive test plans for gradual introduction to traffic situations.
    - Expanded HMI specification to ensure adequate driver feedback.
    - **ADDITIONALY REQUIRED**: TARA documentation covering V2X communications.

- **ADDITIONALY REQUIRED**: PDI checklist verification for system readiness.

2. **Second Submission Stage**:
   - Proving ground pre-tests are **MANDATORY** due to critical system modifications.
   - Tests must demonstrate safe behaviour in failure scenarios before public road testing. For instance: demonstration of system behaviour under communication failure scenarios.
   - Test case covering areas where there are no modifications from the base vehicle are not required.

5.3.2 Tests are carried out only in one country with ODD extension

After successful testing without technical and safety relevant issues, it is decided to extend the ODD of the AD system to roads with a speed limit up to 70 kph, one lane per driving direction, traffic lights, conducting right and left turns (with and without VRUs). The tests are mainly conducted on urban roads, but since rural roads might become relevant later in the project the testing organization wants to apply already for both types of roads.

5.3.2.1 Safety assessment

ODD Extension

⚠ CONCERN: Rural roads introduce new road characteristics and scenarios.

❓ RECOMMENDATION: Update risk assessment and activity risk assessment taking into account the new risks and hazards from the odd extension.

Software version changed

⚠ CONCERN: Software changes between versions need documentation (changed from V1.0.0 to V1.1.0).

❓ RECOMMENDATION: Follow the recommendations of chapter “11.4 Software version traceability”.

PDI readiness for Extended ODD

⚠ CONCERN: V2X performance at higher speeds not validated. Message latency becomes more critical at higher speeds.

❓ RECOMMENDATION: Verification of message authentication timing at increased velocities.

⚠ CONCERN: Network coverage variations in rural roads may affect PDI interactions.

❓ RECOMMENDATION: New identification of PDI requirements for the test setup as per “5.1.2 Description of testing activity”.

5.3.3 Tests are carried out only in one country and demonstration for final event on public roads in a second country

At the final stage of the project the research vehicle should be show-cased at the final event of the project. The plan for the final event is to demonstrate the vehicle on public roads in the ODD in which the vehicle was tested in the beginning (50 kph, urban roads). Sensors and logic configuration are chosen that have been tested beforehand without any issues.

5.3.3.1 Safety assessment

Mutual Recognition considerations

⚠ CONCERN: Compliance with both countries' regulations required.

? RECOMMENDATION: Complete SVG process with both countries' authorities according to chapter “7 Mutual recognition”.

? RECOMMENDATION: V2X standards or implementations between countries may differ. Verify V2X infrastructure compatibility in Brussels.

Software Version

⚠ CONCERN: Changes from V1.1.0 to V1.1.1 must be documented.

? RECOMMENDATION: Follow the recommendations of chapter “11.4 Software version traceability”.

Safety operator

? RECOMMENDATION: Perform site reconnaissance before demonstration.

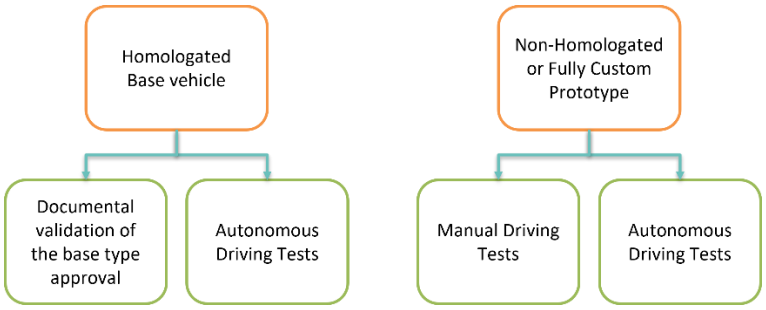
Funded by the European Union

6 Proving ground pre-tests

6.1 Scope

The proving ground pre-tests outlined in this chapter represent a flexible and adaptive testing framework that serves as a critical safety assessment mechanism, with their applicability varying based on the vehicle's homologation status and the prototype development phase of the vehicle.

This approach recognizes that not all autonomous vehicle prototypes are created equal, and therefore requires a nuanced methodology for safety validation ensuring a tailored yet comprehensive assessment of each unique autonomous vehicle prototype.



Homologated base vehicle

Some autonomous vehicle projects utilize existing type-approved vehicles as a foundation for technological integration. These vehicles have already undergone comprehensive safety testing during their original homologation process, with established type approval numbers for critical systems like braking and powertrain. When adapting such vehicles for autonomous technologies, the fundamental safety parameters may have already been validated.

For these vehicles, basic proving ground pre-tests may be partially or fully waived. Instead, a documental validation of the base type approval should be done. The testing focus shifts to evaluating the specific autonomous modifications and their interaction with existing vehicle systems, preventing redundant testing while ensuring new technologies meet rigorous safety standards.

Non-homologated or fully custom prototype

Alternatively, some autonomous vehicle prototypes are developed from scratch, lacking any existing type approval. These custom prototypes require comprehensive proving ground pre-tests that validate every fundamental safety parameter. Unlike modified vehicles, these prototypes must undergo testing of manual driving characteristics, braking performance, powertrain functionality, and overall system integration.

For these vehicles, proving ground pre-tests represent a critical first step in establishing basic vehicular safety, serving as a comprehensive assessment of the vehicle's core safety capabilities.

Funded by the European Union

6.2 Testing requirements and provisions

- The safety validator shall evaluate if any of the following tests are necessary to evaluate the system's safety behaviour and adapt these tests to the vehicle characteristics (e.g. maximum velocity).
- The tests must be carried out on dry asphalt unless it is necessary to verify a system characteristic, or it is decided otherwise with the applicant.
- Test vehicle(s) inspection described in chapter 9 shall be performed prior to proving ground pre-tests.
- During testing if the vehicle is operating in autonomous driving mode, access to the vehicle controls (or, if applicable, the emergency disconnection control) must always be available, and these must be able to be operated manually by the safety operator.
- The vehicle safety operator will be responsible for supervising the tests, as well as acting in case of emergency.
- In the case of an automated vehicle that does not require a driver inside the vehicle's cabin and can therefore be controlled remotely, the applicant must provide the necessary equipment to carry out the dynamic verification tests described in the following sections.

6.3 Manual driving tests

These tests are intended for prototypes and modified type-approved vehicles, requiring comprehensive proving ground validation of fundamental safety parameters including manual driving characteristics, braking performance, powertrain functionality, and overall system integration. It is understood that some of the test cases presented below may not be reproduced due to the technical characteristics of the test vehicles (e.g. vehicles not equipped with manual controls, vehicle with a range of speeds below the test speeds indicated, etc.). In such cases, the proposed test parameters may be modified by the responsible authority.

6.3.1 Dynamic safety checks

In case the vehicle can be driven in manual mode, following tests are recommended to ensure the possibility to control it longitudinally and laterally in a safe way:

- Driving straight up to the maximum speed allowed in the country or, if lower, its maximum by construction to check the speedometer and absence of deviation, vibrations, noises or other anomalies.
- Curve exit up to 50 km/h (or maximum by construction if lower) for steering wheel autorotation check (if vehicle is equipped with a steering wheel) and absence of vibrations, noises or other anomalies.
- Support changes within the same lane with initial speeds of up to 50 km/h (or maximum by construction, whichever is lower) for the assessment of stability, control and absence of vibrations, noises or other anomalies.
- Braking up to 0.5 g with initial speeds up to 50 km/h (or maximum by construction if lower) to verify the absence of drift, vibrations, noise or other anomalies.
- Braking until ABS is blocked or activated (if the vehicle has ABS) with initial speeds of up to 50 km/h (or maximum speed by construction if lower) to check for absence of drift, vibrations, noise or other anomalies.

- Acceleration at 3/4 throttle up to 80 km/h (or maximum speed by construction, if lower) for the assessment of stability, control and absence of vibrations, noises or other anomalies.

6.3.2 Braking test

The main objective of this test is to check and ensure the correct operation of the braking system. To meet this objective, the vehicle will have to be able to brake in different conditions and situations as explained below.

The regulations "*ECE R13H Uniform provisions concerning the approval of passenger cars with regard to braking"* and "*ECE R13 Uniform provisions concerning the approval of vehicles of categories M, N and O with regard to braking"* have been taken as reference documents. Vehicles of category L are excluded from this test but will have a trial to ensure minimum performance.

6.3.2.1 Type 0 - Cold test

It is considered that the braking system is cold if the temperature measured on the disc or on the outside of the drum is between 65 and 100 °C.

The tests shall be performed at the vehicle maximum load declared for public road testing.

The test must be carried out as follows:

- Test with the engine/motors disengaged.
- Test with the engine/motors engaged. (In the case of a vehicle equipped with an electric regenerative braking system it should be turned off or with a level of battery high enough to avoid its intervention)

The prescribed limits for the minimum braking efficiency, both for tests with the vehicle in minimum load condition and with the vehicle in maximum load condition for M1, will be as set out below:

Table 8. Type 0 test with engine disengaged

Type-0 - With engine/motors disengaged	v	=	100 km/h
	s	≤	$0.1v + 0.006 \cdot v^2$ (m)
	d_m	≥	6.43 m/s^2
	F	between	6.5-50 daN

Table 9. Type 0 test with engine engaged

Type-0 - With engine/motors engaged	v	=	80% vmax < 160 km/h
	s	≤	$0.1v + 0.0067 \cdot v^2$ (m)
	d_m	≥	5.76 m/s^2
	F	between	6.5-50 daN

The prescribed limits for minimum efficiency, both for tests with the vehicle in minimum load condition and with the vehicle in maximum load condition for M2, M3 and N will be as established below:

Table 10. Type 0 test for different vehicle category with engine dis/engaged

			M2	M3	N1	N2	N3
Type-0 - With engine/motors disengaged	v	=	60 km/h	60 km/h	80 km/h	60 km/h	60 km/h
	s	≤	$0.15v + v^2/130$ (m)				
	d_m	≥	5 m/s^2				
	F	between	6,5-50 daN				
Type-0 - With engine/motors engaged	v	=	80% vmax <100 km/h	80% vmax <90 km/h	80% vmax <120 km/h	80% vmax <100 km/h	80% vmax <90 km/h
	s	<	0.15v + v2/103,5 (m)				
	d_m	>	4 m/s2				
	F	between	6,5-50 daN				

Where:

- v = test speed, in km/h
- s = braking distance, in meters
- d_m = average stabilized deceleration, in m/s2
- F = force applied to the brake pedal, in daN
- vmax = maximum vehicle speed, in km/h

6.3.2.2 Type 1 - fading

Heating:

The service brakes of all vehicles shall be tested by accelerating and braking a number of times (respecting the braking intervals between braking and braking), with the vehicle loaded, under the conditions shown in the following table (braking initial will be 3 m/s^2):

Table 11. Fading test for different vehicle categories

	Conditions			
	v1 (km/h)	v2 (km/h)	Δt (sec)	n
M1	80%vmax ≤ 120 km/h	$0.5v_1$	45	15
M2	80%vmax ≤ 100 km/h	$0.5v_1$	55	15
N1	80%vmax ≤ 120 km/h	$0.5v_1$	55	15
M3, N2, N3	80%vmax ≤ 60 km/h	$0.5v_1$	60	20

Where:

- v1 = initial speed, at the beginning of braking
- v2 = speed at the end of braking
- vmax = maximum vehicle speed
- n = number of brakes

Funded by the European Union

- Δt = duration of a braking cycle: time that elapses between the start of one brake application and the start of the next.

Hot performance

At the end of the type I test, the hot performance of the service braking system will be measured under the same conditions as for the type 0 test with the engine disengaged (temperature conditions may be different). This hot efficiency must not be less than 75 percent of that prescribed for M1 and 80 percent for M2, M3, N1, N2 and N3, nor 60 percent of the figure recorded in the type 0 test with the engine. disconnected.

System evaluation

The performance of the braking system will be determined by measuring the braking distance in relation to the initial speed of the vehicle and/or by measuring the average stabilized deceleration developed during the test.

- The braking distance will be the distance travelled by the vehicle from the moment the operator begins to operate the braking system control until the moment when the vehicle stops; The initial speed will be the speed at the moment in which the operator begins to activate the braking system; The initial speed shall not be less than 98 percent of the speed prescribed for the test in question.
- The stabilized average deceleration (dm) will be calculated as the average deceleration in relation to the distance in the interval vb to ve, according to the following formula:

$$dm = \frac{vb^2 - ve^2}{25.92 \cdot (se - sb)}$$

Where:

- vo = initial speed of the vehicle in km/h,
- vb = vehicle speed at 0.8 vo in km/h,
- ve = vehicle speed at 0.1 vo in km/h,
- sb = distance travelled between vo and vb in meters,
- se = distance travelled between vo and ve in meters.

The speed and distance will be determined by instrumentation, the precision of which must be ± 1 percent with respect to the speed required for the test. The dm may be determined by methods other than the measurement of speed and distance; In that case, the precision of the dm will be ± 3 percent.

6.3.3 Steering equipment test

The main objective of this test is to check and ensure the correct operation of the steering equipment system. To meet this objective, the vehicle will have to be able to steer in different conditions and situations as explained below.

The regulation UN-R79 "*Uniform provisions concerning the approval of vehicles with regard to steering equipment*" [8] has been taken as reference document.

The measurement procedure of steering efforts on motor vehicles with intact steering equipment is as follows:

The vehicle shall be driven from straight ahead into a spiral at a speed of 10 km/h. The steering wheel control effort shall be measured at the nominal radius of the steering control until the position of the steering control corresponds to turning radius given in the table below for the particular category of vehicle with intact steering. One steering movement shall be made to the right and one to the left.

Requirements are explained in table below:

Table 12. Maximum steering effort per vehicle category

Vehicle Category	Maximum effort (daN)	Time(s)	Turning radius (m)
M1	15	4	12
M2	15	4	12
M3	20	4	12
N1	20	4	12
N2	25	4	12
N3	20	4	12

6.4 Autonomous driving tests

6.4.1 Override

The vehicle shall go in autonomous driving mode, at a constant speed, maintaining a straight path. The distance travelled during the approach phase by autonomous driving before starting override must be greater than 200m. Override shall be tested with intervention of any safety operator possibility for the three following systems:

- Braking system: The test will be performed at a constant speed, 100km/h or the maximum allowed by the system (whichever is lower), in a straight line and the brake will be activated with less than 300 Newtons after the approach phase.
- Accelerator: The manoeuvre consists of approaching a stationary vehicle in a straight line at 30km/h, and at the moment the vehicle begins its deceleration phase to prevent impact, the operator will fully actuate on the accelerator resulting in impact.
- Steering system: The test will be performed in a straight line at constant speed, at 70% of the maximum speed allowed by the system, and a lane change will be made at a maximum effort of 50N to the right and left.

E.g.: If is it is intended to perform public road tests with an on-board safety operator and/or a remote safety operator, at least the following list of pre-tests shall be performed:

- Braking system intervened by the on-board safety operator.
- Braking system intervened by the remote safety operator.
- Accelerator intervened by the on-board safety operator.
- Accelerator intervened by the remote safety operator.
- Steering system intervened by the on-board safety operator.

Funded by the European Union

- Steering system intervened by the remote safety operator.

The test is considered as passed as soon as the safety operator (either on-board or remotely) intervenes in any of the three systems and the autonomous driving process stops.

In case that the applicant has declared a different override logic, it shall be checked that the autonomous driving process stops when conditions agreed are met.

6.4.2 Longitudinal control tests

The objective of these tests is to evaluate the vehicle's ability to maintain longitudinal control and brake in case of an emergency. For vehicles in which it is not possible to apply the tests described due to system limitations or other justified reasons, a different set of tests shall be agreed between the safety validator and the applicant.

6.4.2.1 Emergency braking in autonomous mode

The regulation UN R152 "*Uniform provisions concerning the approval of motor vehicles with regard to the Advanced Emergency Braking System (AEBS) for M1 and N1 vehicles*" *[9]* has been taken as reference document.

The autonomous emergency braking performance will be evaluated in the different scenarios in which the vehicle should avoid hitting the target in all of them under different conditions following the applicant's strategy declared (e.g. avoid, brake)

- Target vehicle stationary:

Table 13. Test vehicle speeds for stationary target vehicle for AEB test

Test vehicle speed (km/h)	Relative impact speed (km/h)
20	0
40	0
60	35

- Target vehicle moving:

Table 14. Test vehicle speed and target vehicle speed for AEB test

Test vehicle speed (km/h)	Target vehicle speed (km/h)	Target vehicle deceleration (m/s^2)	Initial distance between vehicles (m)
50	20	No	-
50	50	-4	12
50	50	-4	40
70	20	No	-

- Pedestrian crossing from the right of the road:

    - Adult pedestrian with an impact point in the centre line of the test vehicle.
    - Child pedestrian with an impact point in the centre line of the test vehicle.

6.4.3 Lateral control tests

The objective of these tests is to evaluate the vehicle's ability to stay in a lane marked with road markings (solid/dashed line). A minimum of lateral controllability of the vehicle is required, so that it can be guaranteed that in autonomous driving mode the vehicle is capable of circulating within its lane in a stable manner and without interfering with neighbouring lanes.
To meet this objective, the vehicle will have to be able to maintain itself in different conditions in a lane indicated by road markings.

6.4.3.1 Lane Keeping

The vehicle will circulate in autonomous driving mode in a lane with lane markings on both sides. The vehicle must remain stable within the lane, without oscillations for the next conditions:

Test vehicle Speed (km/h)	Lane radius (m)
30	**Straight**
50	**Straight**
80	**Straight**
30	**<400**
50	**<400**
80	**<400**

6.4.3.2 Lane change

The vehicle will circulate in one of the lateral lanes of a road with at least 3 lanes, it shall start a lane change and another vehicle shall start changing into the same space within the target lane.

The test vehicle shall avoid the collision in a safe way for the following conditions:

Test vehicle Speed (km/h)	Lane radius (m)
30	Straight
50	Straight
80	Straight
30	<400
50	<400
80	<400

Funded by the European Union

6.4.4 Emergency disconnection of the ADS

The test will be conducted at a constant speed of 30 km/h or at a speed deemed safe for performing the manoeuvre, maintaining a straight-line trajectory. The manoeuvre consists of approaching an object in the middle of the lane (type of object shall be agreed between safety validator and applicant, if they are different entities), performing it with an emergency disconnection of the ADS will verify that the operator's decision always prevails.

The test procedure should be executed as follows:

- The vehicle must circulate in autonomous driving mode, at a constant speed, maintaining a straight path.
- The operator shall not exercise any type of control or contact over the vehicle controls during the approach phase.
- At a distance before the object, following the control strategy declared by the applicant, the emergency disconnection should be performed.

And it is considered as passed if:

- The vehicle's powertrain stops accelerating and the autonomous driving system turns off after emergency disconnection.
- The vehicle did not brake to prevent impact with the object. Unless another emergency braking logic has been declared (e.g. AEB system activation).

It shall be performed for each of the declared possibilities, e.g.:

- By on-board safety operator.
- By remote safety operator.
- By other passengers in the vehicle.

6.4.5 Recognition and compliance tests with traffic signs

To guarantee the carrying out of tests of vehicles with autonomous functionalities on roads open to traffic in general and sharing the road with other users, it is essential to guarantee that these vehicles, in autonomous mode, are capable of recognizing and respecting traffic signs, both vertical and horizontal signage.

The recognition and compliance with traffic signs can rely on different systems.

- Homologated according to R(EU) 2021/1958 ISA[10]: a documental assessment of the system integration into the ADS shall be performed.
- Not homologated according to R(EU) 2021/1958 ISA: for computer/AI vision systems a closed-circuit test with physical vertical and horizontal signage must be performed. If the system also relies on HD maps, the applicant must demonstrate that they have a permanently updated digitized map of the test area and with reliable information during the period of testing on public roads and how both methodologies are integrated.

If the applicant can guarantee the identification and compliance with road signs using another system described above, the safety validator may develop a test methodology to guarantee compliance with general traffic regulations.

Funded by the European Union

6.4.6 Failure test

The behaviour of the system shall be checked under failure conditions by applying corresponding output signals to electrical units or mechanical elements in order to simulate the effects of internal failure within the unit. The failure shall be indicated to safety operator(s) and the system shall stop the vehicle in a safe way following the strategies declared by the applicant.

Funded by
the European Union

7 Mutual recognition

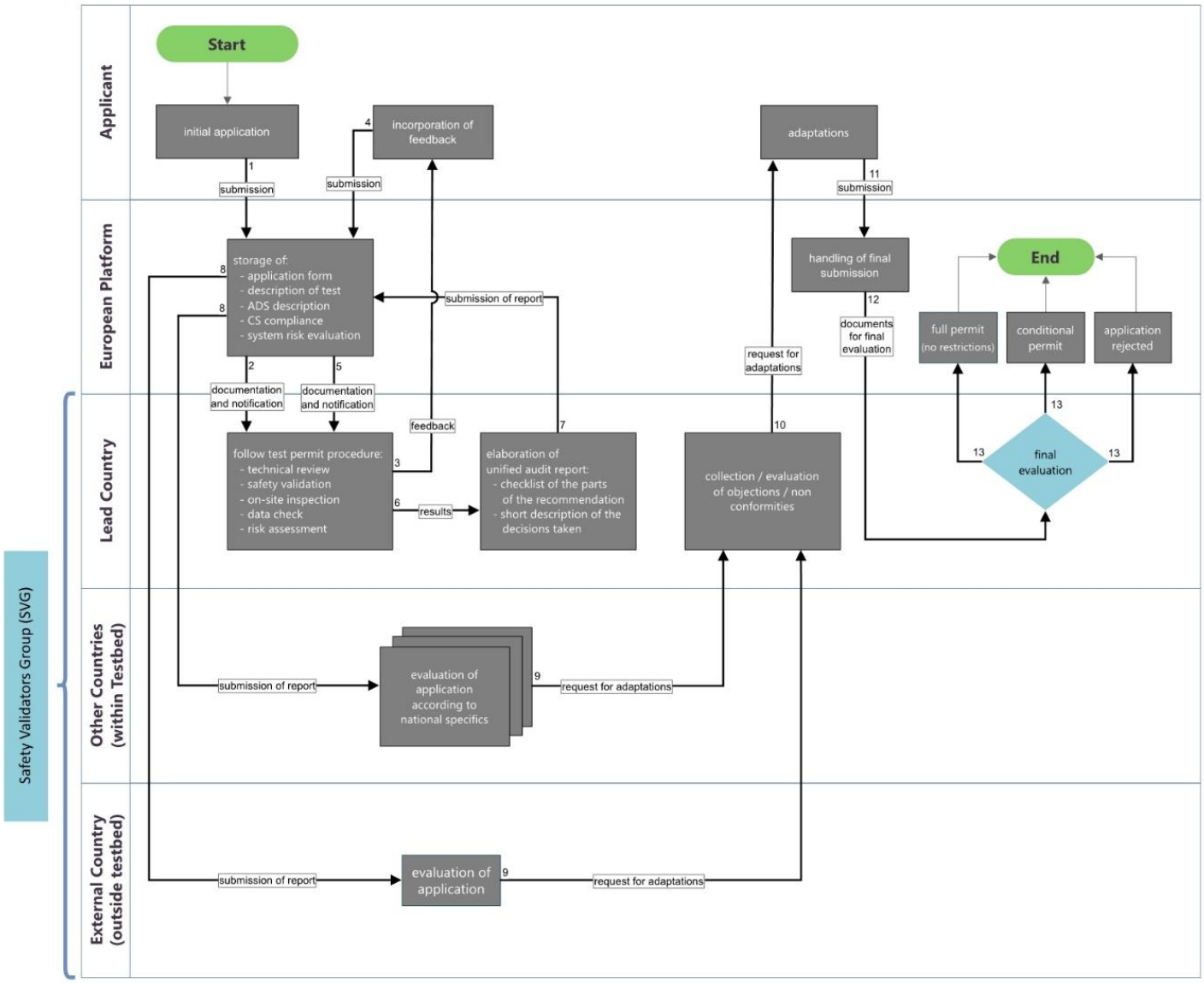


Figure 8: Flow diagram for mutual recognition

Mutual recognition of a license granted by a member state by others is a key aspect to facilitate the deployment of prototypes with testing aims [11]. In this chapter we propose a European mutual recognition process for AV testing on public roads. There are two central functions that will facilitate the process: the Safety Validators Group, and the European platform for public road testing.

Safety Validators Group (SVG)

Each member state shall appoint (a) cross-border/mutual recognition safety validator(s). This position could be established as part of the approval authority or the designated third-party assessor (e.g. technical service). These designated representatives from multiple member states would form the Safety Validators Group (SVG) in charge of performing the audits of AV tests.

Funded by the European Union

European platform for public road testing

This platform shall act as an online application exchange space where countries agree to recognise the test permit procedure described in chapter 5 of this document. A central European body, such as the European Commission's Directorate-General for Mobility and Transport (DG MOVE), should coordinate the platform. Member states opt into the platform, agreeing to adopt the harmonized framework for AV testing on public roads.

It will be necessary to involve the member states and relevant EC bodies at an early stage to elaborate together concrete opportunities for the implementation of such a group and such a platform.

7.1 Mutual recognition process

The following chapter provides an idea on how a mutual recognition process could be established. It is important to note that this is no final suggestion, and it is necessary to agree on details with the responsible and involved stakeholders, like EC bodies and the member states.

When a test is planned in multiple countries, the SVG members of those countries will be automatically notified by the European exchange Platform for public road AV testing and will have access to the documentation submitted by the applicant through that platform. However, only one designated country, lead member state from now on, shall be responsible for certifying the test following the Test permit procedure described in chapter 5.

Similar to the current discussions in the GRVA forum this mutual recognition process involves the evaluation and acceptance of all the contracting parties or member states. At the 6th GRVA Workshop on ADS of March 2025 [12] the following requirements for type approval are being drafted.

- *The approval authority concerned shall notify the other approval authorities applying the UN Regulation of the issue and of their proposed solution for the interpretation, including any supporting information from the manufacturer. As a general rule, this should be done via electronic media.*
- *Approvals should not be granted unless comments have been 'taken into account'*
  (b) If it is not possible to take a decision according to the comments received, the approval authority shall seek further clarification
- *After having considered the potential impact on vehicle safety, […] Contracting Parties may prohibit the sale and use of such wheeled vehicles, equipment or parts in their territory until this non-conformity is rectified.*
- *In this case the granting Approval Authority shall ensure that the territory of the Contracting Party concerned is excluded from the ODD of the ADS feature(s) concerned and shall not include that Contracting Party*

This lead Member State could be determined based on the following indicators. The recommended indicators for selecting the lead Member State for cross-border AV testing are based on Commission Implementing Decision (EU) 2025/264[13] key performance indicators, aligning with the European Commission's ITS framework. Nonetheless it is important to elaborate a process which ensures that not only the "big countries" get assigned as the lead member state.

- Technical Expertise
    - Number of AV tests previously overseen
    - National AV regulation (none, testing, deployment)
- Infrastructure
    - Cooperative & Connected Mobility Readiness of the route
        - Percentage of test roads covered by PDI services
        - Availability of real-time traffic information
        - Percentage of road network equipped with incident detection systems
    - Availability of dedicated AV testing facilities (e.g. proving ground facilities)
    - Variety of road types to test in their territory (urban, rural, highway)
    - Total kms driven
- Resource Availability
    - Number of staff (full time equivalence) dedicated to AV testing oversight
    - Annual public investment allocated to AV testing and infrastructure
- Track Record
    - Successful completion rate of previous AV tests
    - Average time to process AV test applications

To facilitate trust in validations from other countries, the short report template included in Annex V – Model of report for recognition of permits granted by a different authority is expected to be elaborated by the lead Member State, including:

- Statement of the lead member state affirming that the submitted application is in line with the present recommendations for the listed parts.
- Checklist of the parts of the recommendations that have been followed.
- Short description of decisions taken in favour of granting the permit, taking into account the information provided by applicant (e.g., inclusion/exemption of requirements, testing area agreed, reporting or monitoring decisions…).

This report is then forwarded to the European platform which sends it to the SVG members of the other included countries, implied the request for review. The other SVG members validate the application for their country and can request adaptations by the applicant. In the process of mutual recognition review, each additional jurisdiction performs a thorough gap analysis, comparing their specific requirements for AV testing against the report issued by the lead member state. To accommodate these varying needs across different territories, the applicant shall adapt its ADS as required.

These adaptations should allow the ADS to adjust its operational parameters as it traverses different jurisdictions. That could be minor changes, involving small adjustments such as modifications to speed limits or sensor configurations. Alternatively, the changes could be significant, requiring additional

Funded by the European Union

testing or imposing major operational restrictions, such as limiting the vehicle's functionality in complex urban environments or during adverse weather conditions.

Only after positive review by all participating SVG members, a mutually recognised permit for AV testing can be issued.

This would allow innovative testing to operate across borders with a single, streamlined set of rules. In the meantime, it reduces administrative duplication, ensuring that tests are approved efficiently by all members involved and maintaining rigorous safety and technical standards across borders.

There have been precedent cases of European platforms to exchange documentation and support mutual recognition such as ETAES and DETA[12]. Germany, the country hosting the Database for the Exchange of Type Approval documentation (DETA) and its representative, chair of the Informal Working Group (IWG) on the Database have acknowledged the value of DETA as a good platform for exchange of information. He mentioned GRVA activities in the context of exchange of scenarios. In addition, he explained that this workstream started recently and considered centralized and decentralized ways to share information and last and most important reflected the availability for other compliance certifications widening the scope of DETA for activities such as software updates (e.g. Over The Air), storage of software version numbers and storage of validation models for Automated Driving.

In its 51st session held in September 2024, the IWG of DETA was working on an initial draft on Guidelines for the use of DETA with regards to the exchange of information on Cyber Security.[15] Its procedure is “The Approval Authority of a country hereby notifies the other Approval Authorities of the Contracting Parties applying UN Regulation No. 155[16] about the method and criteria taken as a basis to assess the appropriateness of the measures taken in accordance with UN Regulation No. 155 […] Please refer to the type approval No. […] for the details”. This procedure would be similar to these guidelines for public road testing.

Moreover, this procedure is also proposed for Driver Control Assistance Systems (DCAS) short-term reporting of safety-critical occurrences. “The Type Approval Authority shall upload this information in English language to the secure database "DETA", established by the United Nations Economic Commission for Europe, without undue delay after the manufacturer has informed the Type Approval Authority to communicate this information to all Type Approval Authorities. The information shall be sufficient to understand the cause for and the remedial action itself.”

7.1.1 Case study: Multi site

Mutual recognition establishes a flexible framework ensuring that the AV can operate safely and in compliance with local regulations across diverse countries. By adjusting the vehicle to the specific requirements of each jurisdiction, it facilitates efficient cross-border testing while maintaining rigorous safety standards and regulatory compliance throughout all territories.

For instance, lets imagine an applicant applies for AV testing at country A (lead country in the permission process), country B and C.

- Country A (Urban Environment, Highways): In charge of AV test permit procedure.
  Testing in urban areas with high traffic density and highways. Speed limit up to 120 km/h, complex intersections navigations, pedestrian interactions.

- Country B (Rural Highways): Recognizes Country A's test assessment and evaluation after reviewing information and requests further information.
    - Additional Requirements: Evidence of lane-keeping function on narrow lanes without wayside.
- Country C (Mixed Environment): Recognizes Country A's test assessment with significant adaptations.
    - Additional Requirements: Testing in mountainous terrain. Adverse weather condition handling (e.g., snow, fog). Specific rules for small town traversal.

7.1.2 Partial mutual recognition

When the operational domain or specific manoeuvres of a test activity differ between countries, or when certain actions conflict with a country's laws, mutual recognition may not be possible. In such cases, if the applicant cannot resolve these discrepancies or non-conformities, a Safety validator from a particular country may choose to partially agree to issue the test permit. This partial recognition consists of allowing the test to proceed under specific conditions, which must be clearly stated by the country in question. This approach ensures that while full mutual recognition might not be achievable, testing can still proceed in a controlled manner that respects each country's regulatory requirements and safety standards.

Not only internationally but this can also be seen at national level where different municipalities may have different traffic rules regarding AVs.

- International Cross-Border Testing: countries may present different operational domains referring to the general conditions and environments in which a system or vehicle is designed to operate. These can be e.g. traffic laws, traffic signs, speed ranges, infrastructure, or environmental conditions which can vary significantly across borders.
- National Inter-Regional Testing: Within a country, different regions or municipalities may have distinct AV regulations. Individual cities might impose specific rules for AV testing within their boundaries.

7.2 AV test corridors: A Standardized Approach to Cross-Border Testing

AV test corridors with pre-certified infrastructure pave the way for mutual recognition and cross border testing. These corridors across Europe have predefined conditions where road infrastructure, communication systems, and safety protocols are aligned in advance for AV testing, ensuring a standardized and predictable testing environment, therefore providing seamless testing environments for AV testing.

AV developers and testers can use these corridors focusing on the AV systems without worrying about differing road regulations, data exchange protocols, or infrastructure issues. Countries involved maintain the infrastructure and ensure that it meets predefined conditions. Therefore, when a mutual recognition application is submitted for these areas, member states can easily grant the permit.

Some examples of these corridors are:

- France, Germany and Luxembourg, the cross-border digital testbed for autonomous and connected driving. It connects the south of Luxembourg with Metz in France and Merzig in Germany, 215 km in total. It offers developers of technologies for automated and connected

driving as well as of related mobility services the opportunity to conduct tests in real-life traffic environment. A wide range of testing conditions includes high-speed zones, tunnels, tolls, border crossings, road works, road marking, traffic density, navigation, uninterrupted cellular networks, navigation and road safety. [17]

- Bizkaia Connected Corridor places at the disposal of the Basque industrial and research network the 1,200 km of roads in Bizkaia with all their associated infrastructures: tunnels, viaducts, embankments, service roads, control centres, etc., to be used as a testing laboratory for CCAM technologies and Smart and Digital Infrastructures, for both physical technologies, linked to Materials, Resilience, Sustainability, etc., as well as digital initiatives, linked to Artificial Intelligence, Cybersecurity, Advanced Communications, Software Technologies, etc. [18]

It is important to note that while these corridors provide valuable controlled environments for initial cross-border validation, comprehensive AV deployment will ultimately require addressing the complexities of testing across diverse regulatory frameworks, infrastructure conditions, and operational domains outside of these standardized settings. Test corridors should be viewed as complementary to broader testing strategies that progressively tackle the challenges of varying traffic regulations and infrastructure disparities. The standardization achieved in these corridors provides useful frameworks that can inform future harmonization efforts for the wider European road network.

8 Risk Assessment

In order to ensure that the process of testing the ADS on public roads does not pose a severe risk to other road users, a risk assessment procedure is established. This is performed prior to the testing permit submission. The methodology recommended consists of an initial system risk evaluation and a test-specific risk evaluation.

8.1 System risk evaluation

This evaluation shall be performed by the applicant and shall be provided in the first documentation stage. See chapter 5.1.5

8.2 Test-specific risk evaluation

After each documental submission stage, an evaluation of the general activity shall be performed by the safety validation responsible. Given that risk assessment is inherently tied to the test activity itself, this evaluation must account for all relevant test specific risk aspects. In case that the safety validation responsible is the applicant, by means of self-validation, activity risk evaluation should be performed jointly with the approval authority.

The following aspects are inspired by the basic driving situations from the situation catalogue of VDA 702 E-parameter table[19]. If the safety validator considers that the risk of the activity is too high to be deployed, it could request action to be taken to reduce the evaluated risk.

- Human Population
- Impact on Human Safety
- Impact on Pedestrian Traffic
- Variety of Operational Domain
- Impact of Test Route Complexity
- PDI Reliability and Coverage
- Compliance with Traffic Regulation
- Impact of Traffic Density
- Remote or On-board Safety Operator
- Impact of Safety Operator Experience
- Applicant's Previous Experience in public road testing
- Novelty/Innovation of Technologies
- Impact of Emergency Procedures (within the AV)
- Car with Steering Wheel, Pedals, Override System
- Impact of Environment (weather, road conditions)

If considered by the safety validator, further aspects could be added to the following list.

Funded by the European Union

Table 15. Activity risk assessment table

Activity aspect	Low	Minor	Moderate	Significant	Critical
Human Population	No human interaction (isolated areas)	Low population density (rural areas)	Moderate density (suburbs, small towns)	High population density (urban, city areas)	Extremely high density (city centres, event areas)
Impact on Human Safety	No impact	Minimal discomfort	Higher discomfort	Minor injury	Major injury/ Loss of life
Impact on Pedestrian Traffic	No pedestrian activity	Minimal interaction	Moderate interaction	High interaction	Critical danger to pedestrians
Variety of the Operational Domain	Small-scale testing (limited area or routes)	Large scale (multiple test areas with large routes)	City-wide scale testing	National level testing (intercity)	Cross-border level testing (varying road markings, different traffic rules)
Impact of Test Route Complexity	Simple (e.g., highway driving straightforward one way lane, multiple lanes, wide lanes, physical separation, no pedestrian and bicycles)	Moderately complex (e.g., interurban road, no physical separation, change of course, poor visibility)	Complex scenarios (e.g., urban driving, intersections, turnings, zebra crossing, traffic signal compliance (yield, stops, traffic lights, etc.))	Highly complex (e.g., multi-modal environments (rural, highway, urban), highway incorporations and exits, roundabouts and complex road geometries)	Extremely complex (e.g., urban driving with dense pedestrian traffic, narrow lanes, objects and cars parked, poor traffic signalling and lack of lane markings)
PDI Reliability and Coverage	Stable and reliable PDI with full coverage across the test route. No anticipated failures.	Minor coverage gaps or occasional signal losses, but with effective fallback mechanisms ensuring continued	Moderate reliability issues, requiring frequent fallback mechanisms or temporary	Significant coverage limitations, leading to potential safety risks or operational failures.	Frequent or prolonged PDI failures, preventing safe AV operation and leading to potential critical incidents.

Funded by the European Union

Activity aspect	Low	Minor	Moderate	Significant	Critical
		safe operation.	operational pauses.		
Compliance with traffic regulation	Fully compliant	Minor local discrepancies			Moderate or significant violation of legal requirements
Impact of Traffic Density	Low traffic density (isolated area)	Minor traffic density	Moderate traffic density	High traffic density (urban)	Very high traffic density (congestion)
Remote or On-board Safety Operator	On-board operator with full control	On-board operator with limited control capability (e.g. activating MRM, emergency protocol)	Fully remote with full control and direct vision	Fully remote with full control no direct vision	Fully remote with limited control capability no direct vision (e.g. activating MRM, emergency protocol)
Impact of Safety Operator Experience	Experienced professional and highly trained safety operator	Experienced professional with minor training gaps	Novel Safety operator (few previous experiences) but highly trained	Experienced safety operator insufficiently trained (less than xx hours)	Safety operator with no previous experience and insufficient training (less than xx hours)
Applicant's Previous Experience in public road testing	Extensive experience in AV testing on public roads	Moderate experience in AV testing on public roads	Limited experience in AV testing on public roads, some tests conducted	Inexperienced in AV testing on public roads with minimal previous experience in track testing)	No relevant experience

Funded by the European Union

Activity aspect	Low	Minor	Moderate	Significant	Critical
Novelty/Innovation of Technologies	Well-established technology with minimal new elements	Minor innovations or improvements	Moderate innovation with some untested elements	Highly innovative, requiring new systems or integration	Groundbreaking, never-before-seen technology or methodologies
Impact of Emergency Procedures (within the AV)	Full emergency procedures in place	Minor gaps in procedures	Moderate procedural issues	Significant gaps in emergency handling	No emergency protocols in place
Car with Steering Wheel, Pedals, Override System	Full direct manual override with steering, pedals, brakes			Limited manual control (e.g. no steering, or braking only emergency stop or MRM activation)	No manual controls, fully autonomous without override
Impact of Environment (weather, road conditions)	No adverse	Minor impact (e.g. light rain)	Snow or fog impacts test	Heavy rain/snow impairs data	Severe conditions, e.g., black ice

Funded by the European Union

9 Inspection of test vehicle(s)

After validating that the system is safe enough to perform the tests described by the applicant and prior to the testing activity start, the safety validator must conduct an in-person verification before the testing activity begins. This involves confirming that the physical vehicle(s) match the specifications provided in the documentation submitted by the applicant. Any discrepancies between the approved documentation and the actual vehicle could compromise the validity of the test and introduce unforeseen risks.

The inspection includes, but is not limited to:

- Exterior safety checks: Ensuring that there are no sharp projections or modifications that could pose a danger to pedestrians or other vehicles.
- Interior safety checks: Verifying that the interior provides appropriate space and ergonomic considerations for the operators or passengers involved in the test.
- Condition of wheels and tires: Ensuring proper tire pressure, tread depth, and structural integrity to maintain stability and control during testing.
- Mounting of instrumentation and ballast (if applicable): Confirming that all added equipment is securely installed to prevent unexpected vehicle behaviour or hazards during operation.

The safety validator must also review and confirm the qualifications of the personnel responsible for overseeing and operating the test vehicle. This involves collecting and verifying the following information:

- Identity and role: Name and job position of each safety operator involved in testing activities.
- Certifications or training: Confirmation that operators have undergone any necessary safety training, including but not limited to:
    - Familiarity with specific vehicle systems
    - AV operation protocols
    - Emergency intervention techniques and procedures
    - Local traffic laws applicable to AV testing.

Upon completion of the above inspections, the safety validator will issue the permit for the public road test to commence. If any discrepancies or safety concerns are identified, corrective measures must be taken before the test begins. This process guarantees that all testing is conducted in a controlled and risk-mitigated environment.

Funded by the European Union

10 Cybersecurity management plan

In addition to declaration of compliance, a cybersecurity management plan may be requested by the safety validator detailing how cybersecurity risks are managed throughout the vehicle's development, covering the roles, responsibilities, and processes that ensure security.

- Threat Analysis and Risk Assessment (TARA): This identifies potential attack vectors and classifies risks based on their potential impact and likelihood. TARA will help define the cybersecurity goals and controls implemented in the vehicle.
  - The applicant shall identify the critical elements of the vehicle and perform an exhaustive risk assessment and shall treat/manage the identified risks appropriately. The mitigations implemented shall include but are not limited to all mitigations referred to in Annex IV – Cybersecurity vulnerabilities and threats. These are based in Part B and C of Annex 5 of the UN regulation 155.[16] However, if a mitigation referred to in Annex 5, Part B or C, is not relevant or not sufficient for the risk identified, the applicant shall ensure that another appropriate mitigation is implemented.
  - The risk assessment shall consider the individual elements of the vehicle type and their interactions.
  - The risk assessment shall further consider interactions with any external systems. While assessing the risks, the applicant shall consider the risks related to all the threats.
- Cybersecurity Requirements and Controls: evidence of the specific cybersecurity requirements derived from TARA and the corresponding technical and organizational controls implemented. This includes data encryption, secure communication protocols, and protection against unauthorized access.
- Test Results and Validation Reports: Provide the results of internal penetration testing, fuzz testing, and other validation methods used to ensure the vehicle's cybersecurity measures are functioning as intended.

The applicant shall inform the safety validator of any cybersecurity change that will affect the relevance of the tests. After consultation with the applicant, the safety validator shall decide whether new checks are necessary.

Funded by the European Union

11 Monitoring process and reporting

The monitoring and reporting process focuses on two topics: traffic safety and effects evaluation. Safety is of the highest priority. This means that in case of an occurrence, this must be reported immediately to the authority responsible for the testing permit.

The ADS regulation EU 2022/1426[20] defines different levels of occurrences:

Table 16. Definitions of different types of occurrences

Occurrence	A safety related situation involving a vehicle equipped with an automated driving system
Non-critical occurrence	An occurrence involving an operational interruption, defect, fault or other circumstance that has or may have influenced ADS safety and that has not resulted in an accident or serious incident. This category includes for example minor incidents, safety degradation not preventing normal operation, emergency/complex manoeuvres to prevent a collision, and more generally all occurrences relevant to the safety performance of the ADS on-road (like interaction with remote operator, etc.).
Critical occurrence	a collision event and because of which: (a) at least one person suffers an injury that requires medical assistance as a result of being in the vehicle or being involved in the event. (b) the fully automated vehicle, other vehicles or stationary objects sustain a physical damage that exceeds a certain threshold or any vehicle involved in the event experiences an airbag deployment.

11.1 Occurrence reporting process

In the case of a critical occurrence, the organization holding the permit must put the test on hold and notify the territory authority with no delay. An initial report shall be sent to the authority within three days including a safety assessment to determine if the test can continue or halt. Based on this report, the authority can decide to further pause the test and mandate a more elaborated report to be submitted within 30 days including documentation that the test is safe to re-start. The authority conducts a safety assessment based on this material. If declined, the testing is stopped and permit revoked.

- Notification to the territory authority responsible for the permit with no delay and put tests on hold until clarification with the authority.
- Day 3: initial report to be shared with the territory authority responsible for the permit.
- Day 30: in case of a severe accident, an elaborated report shall be provided to the territory authority responsible for the permit.
- Decision by the authority on continuing the test or not, based on the safety assessment.

11.2 Periodic reporting process

To monitor ongoing testing activities, a report shall be submitted every 6 months to the authority that issued the permit, as required under the safety validator mandate. The report covers the number of occurrences (as per the definition above), a set of common indicators, and (potentially) a number of specific metrics as decided by the permit.

Any provided information shall be grouped by driving mode (AD or manual), and the ERTAC [21] domain (motorway, urban, rural, (and confined areas)).

- Distance and duration
- Number of trips
- Number of occurrences, non-critical occurrences, and critical occurrences
- Number of passengers (if applicable)
- Average speed

The report shall include a descriptive part on the progress and developments of the test. There shall be descriptive part reasoning on the occurrences. The report shall contain no information that cannot be made public.

The authority can mandate the organization running the test to collect specific indicators per permit. These could cover e.g., the effect on congestion, user experience of the driver or passenger, or experience from other traffic participants, or effects on travel modes.

11.3 National database for accident reports

There is today only one European country storing accident reports from AV testing in national repository: Switzerland. There are plans for such databases in other countries (Denmark, Poland, Slovakia). In case of an accident, the organization responsible for the test must store raw data for future accident analysis. This is implemented in the UK.

11.4 Software version traceability

The applicant shall declare the software version(s) of the system(s) or single ECUs with the connection to the relevant functions of the automated vehicle to be tested. The test permit shall be given just to these specific software versions of the system.

In the event that, during application or testing, updates are applied the applicant shall determine by self-assessment if changes affect the functional and/or operational safety. Two primary scenarios are possible:

- Updates that do not affect the functional and operational safety:
  The applicant shall declare that these changes are free of unreasonable safety risks to vehicle occupants and other road users.
- Updates that do affect the functional and/or operational safety

Regardless of the update type, the applicant must maintain comprehensive traceability of the updates, ensuring that when an occurrence happens, the software version of the function(s) involved, or the multiple software versions, are clearly identifiable, indicating the precise software present when the event occurred.

Purpose of the update	System(s) or function(s) affected	Which are type approved (if any)	SW update confirmation free from unreasonable risks

When updates potentially compromise system safety, the applicant must submit detailed documentation to the safety validator that the software update has undergone and successfully passed verification and validation procedures. This documentation should describe the system changes and provide evidence demonstrating continued compliance with the initially defined requirements. Following document review and consultation with the applicant, the safety validator retains the authority to request additional requirements and update the risk evaluation accordingly.

11.5 Safety maintenance

The data and insights gathered through these monitoring and reporting processes feed directly into the ongoing safety maintenance of the AV testing program. Safety case documents, which form the foundation of the testing permit, are not static but are required to be updated regularly based on the information collected during testing.

This dynamic approach to safety maintenance ensures that risk assessments and safety measures evolve in response to real-world testing experiences. For instance, if periodic reports indicate a recurring issue in certain traffic scenarios, the safety case can be promptly updated to include additional precautions or modified testing parameters.

Furthermore, the continuous updating of safety documentation creates a valuable knowledge base that can inform future testing protocols and contribute to the overall advancement of AV technology. It allows for the identification of trends, the refinement of risk assessment methodologies, and the development of best practices in AV testing.

Funded by the European Union

12 Data requirements during and after AV testing

The purpose for collecting data during tests of AV on public roads is first and foremost to ensure the vehicles are safe to the passengers or operators, as well as other traffic participants. In addition, the organisation collecting the data has interest in performance, efficiency, quality of service etc. The authority issuing the permit to conduct the tests has interest in the potential of the technology and its societal impact, but also in monitoring the tests (e.g., duration and distance driven, or incidents / accidents, impact on traffic, feedback of citizens, etc.). This chapter is limited to only cover the interest of the authority issuing the permit.

As in other technology areas, it is important to distinguish between test and deployment. Note that testing refers to the process of evaluating a system or service to make sure that it works as expected or to identify issues or aspects of improvement. This typically happens in controlled environments before the system is released, although in the context of AV, the focus is on public roads. Deployment, on the other hand, is a process where the system or service is made available for the end users or mass market, by installing or making it available on servers or vehicles, after the testing is complete.

The recommendations for requirements on data logging described in this chapter are set for testing AVs on public roads. However, the requirements are, and could further be, affected by future developments in legislation related to the deployment of AV on public roads.

12.1 Legal landscape for testing AV on public roads

Currently, there are today no common requirements at the European level on data logging during testing automated vehicles on public roads. The requirements from different countries examined in FAME D5.1 [22], range from no mandatory data to be collected, to quite ambitious requirements or recommendations (e.g., in Latvia and in the UK). Out of 22 countries allowing AV testing on public roads, 15 require a minimum set of data recording while the vehicle is in AD mode. Only Austria requires an EDR system to be in place, however other countries like France, Lithuania, Greece, Italy and Germany, put requirements similar to having an EDR. Therefore, these recommendations collect these provisions under a general approach at chapter 5.2.2.

In the UK, the "Code of practise: automated vehicle trialling"[9] has formulated requirements on logging data at 10 Hz from vehicle dynamics (acceleration, speed), commands and activation (steering or braking), location, connectivity, signage (lights and horn), external traffic participants (as objects), remote commands (if applicable), and intervention by safety driver or operator. In addition, this code of practice suggests recording video footage (both external and interior) as part of the trial, however not as a mean to replace the mandatory data elements mentioned before. In case of an accident (definition similar to the definition of critical occurrence in chapter 11), it is recommended to record the data at a minimum of 50 Hz (15 seconds before, and 30 seconds after the course of the impact). Recording at this higher frequency shall be possible after an impact through a buffering system that continuously records data with a dual-channel buffering approach, where data is recorded at the default frequency to disk for general monitoring. Simultaneously, a higher-frequency channel (e.g., 50

[9] https://www.gov.uk/government/publications/trialling-automated-vehicle-technologies-in-public/code-of-practice-automated-vehicle-trialling?utm_source=chatgpt.com

Hz) captures data in a rolling buffer, discarding information older than 15 seconds, except in the case of an impact, extending the recording period another 30 seconds.

Research projects involved in testing CCAM solutions, have the requirement to make data available for further research, however it is not formalized in-detail which data.

12.2 Legal landscape for deployment and type approval

In the EU, the current EU ADS Regulation 2022/1426 [20] includes requirements on data collection built on the EDR regulation (UN R160), but adding DSSAD elements (actuations, take-over requests, interventions, minimum risk manoeuvres, and lane changes).

The EDR directive is built on the UN Regulation No. 160 - Event Data Recorder (EDR)[23]. In annex 4 of the regulation, the data elements are stated and defined. The data elements for DSSAD are stated in UN Regulation No. 157[24].

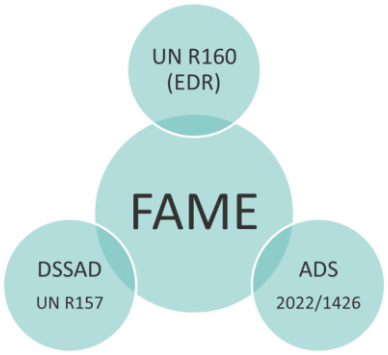


Figure 9: FAME flexible approach to testing based on the type approval regulation UN R160, 2022/1426 and UN R157

12.3 Data requirements for monitoring and reporting

Monitoring and reporting include two main areas:

1) Occurrences
2) Overall performance of testing activities.

In case of an occurrence (Table 16. Definitions of different types of occurrences), the organization holding the permit to execute the test must have the capacity to understand the cause and determine if it is safe to continue the testing activities or not. In case of second stage application, the use of a data logger shall be assessed. The requirements are outlined in chapter 5.2.2 However, any organization testing AV on public roads should evaluate the data elements suggested by ADS regulation 2022/1426 and add on logging of traffic participants around the vehicle (i.e., objects), infrastructure (e.g., guard rails or poles), position (including data elements describing the context of the road segment). Forward video is also recommended and additional video view(s) to be considered.

Regarding the monitoring of the test, continuous data shall be collected to produce indicators, possibly to be detailed per ODD. The indicators are described in chapter 11.2.

12.3.1 Recommendations on data handling and transfer

The data collected during testing activities, must be protected in all phases considered its value (intellectual property) and the potential risks associated with disclosing personal data. Personal data, as defined by GDPR, includes any information that can directly or indirectly identify an individual, such

as location data, biometric vectors, or any other data that relates to an identifiable person interacting or using a vehicle. The protection of data from testing activities is covered in the CCAM Data Sharing Framework (DSF)[25], as well as legal implication of handling this data. Under chapter 13, the ethical aspects of handling data are also covered. The following recommendations should be implemented by testing organizations to ensure data integrity, traceability, and compliance throughout the data lifecycle.

It is important that raw data from data logger remain intact and secure, ensuring it cannot be tampered with at any point. Tampering refers to any unauthorised modification, deletion or corruption of the data, which could compromise its validity and reliability, particularly if the data is to be used as digital evidence or for safety-related reports.

To protect the integrity of the data, checksums for relevant sections must be calculated (a cryptographic value that is generated based on the content of the data, so it serves as a guarantee that any deletion or modification can be detected). Since data is likely to be processed in many stages, from initial collection, conversion, compression, transmission (including from the vehicle to the back-office, using physical or network interfaces), processing and storage, these processing steps must be documented in case there is need to step back in the process. This documentation should include details on the specific actions performed on the data, such as transformations, anonymization, summarization, along with timestamps and authors or software version used for each processing step. This ensures full traceability and transparency of the data handling process. In case errors or problems are found in a later stage, having a clear record of the pipeline of data processing steps facilitates the investigation and helps developers and integrators to identify the problem and fix it. Also, this documentation is especially relevant when data is used for regulatory compliance, safety assessments or other legal proceedings. Frameworks, like ITIL[26], ISO 27001[27], can support the access control process, to some extent also documented in CCAM DSF.

12.3.2 Recommendations on data elements

For testing activities on public roads, we recommend implementing balanced data collection practices that are proportionate to the testing scope while still providing sufficient information for safety analysis. Unlike type approval processes, testing activities should maintain flexibility in data collection requirements.

During the Second documental submission stage, the safety validator should assess the use of data loggers. While ADS regulation 2022/1426 and UN regulation 160 (EDR) provide comprehensive reference points for data elements, testing activities may adopt a more tailored approach better suited to development phases.

For safety monitoring purposes, applicants should consider recording relevant data categories based on the specific testing objectives and risk assessment. In cases where accident analysis capabilities are deemed necessary, a reasonable sampling rate (typically 10 Hz, with an option for 50 Hz in specialized scenarios) may be considered for key parameters. This allows for meaningful data collection while avoiding the excessive costs and capacity challenges associated with full homologation requirements.

The data elements selected should be proportional to the testing scope, complexity of the system being tested, and the ODD. Test applicants and safety validators should collaboratively determine the

appropriate level of data collection that balances safety oversight with practical implementation constraints.

Table 17. Data elements from type approval regulations that the safety validator may consider.

Data elements	
Software version	ADS Actuations
Date (resolution: yyyy/mm/dd)	Remote interventions (if applicable)
Failure(s) & disengagement(s) of the ADS	Position (GPS coordinates)
Steering, braking, throttle	Timestamp
Emergency operation, minimal risk manoeuvre	Lane changes or crossings
Vehicle dynamics (longitudinal and lateral acceleration, speed, roll angle)	Collision detection / EDR trigger input
Airbag deployment, seat belt usage + pretensioner, seat track position	Systems activation (ABS, ESC)

Table 18. Additional data elements recommendations by FAME to be considered by the safety validator

Data category	Data elements
External objects	Object size, class (e.g., pedestrian, car, motorbike), ID (as a temporal identifier over time), distance and position according to the ego vehicle coordinate system, relative speed, and heading.
External sensing	Video (forward). Additional video views if necessary. LIDAR, if applicable.

Funded by the European Union

13 Coordinated ethical public involvement in CCAM testing

13.1 Introduction

To ensure a uniform, harmonized approach to the ethical testing of connected and automated vehicles, some specific obligations and regulations are already laid down in European legislation. These include, for example, sensitive access to personal data and other data of the persons involved or ensuring sufficient information. These legal and ethical aspects, mentioned in the following chapter, are directly related to the previous project deliverable, which addressed an overall, fundamental view of ethics. [22] Now, we will try to translate these basic ethical principles into clear and highly usable rules, that should be followed when designing CCAM test scenarios.

Given the complexity of the issue, we propose designating a person within the project team responsible for ethical issues, who will conduct ethical assessments for the purpose of preparing and ensuring the smooth running of the tests. This chapter, along with the Ethical Checklist in Annex VI, is dedicated to this ethical advisor. The checklist summarizes areas with ethical dimensions that need to be addressed during test preparation and discusses points related to public involvement.

This chapter discusses mainly personal data, user consent, AI act, and proposes documenting safe and ethical operation concepts. The Ethical Checklist highlights also additional aspects such as rigorous safety testing and ethical development of algorithms, which are mainly addressed by other chapters of this document. In addition, the checklist provides notes on transparent and wide evaluation from EU-CEM[28] and FESTA handbooks[29], security (see also CCAM Data Sharing Framework), accessibility targets, and marketing communications. These topics are introduced at the end of this chapter.

13.2 Privacy

Loss of privacy is one of the potential threats associated with the use or testing of connected and autonomous vehicles. Passengers may not always be sufficiently informed about how data is processed in or through a connected vehicle. Therefore, there is a significant risk that cars may request a significant amount of personal data without the persons concerned being able to exercise their data protection and privacy rights.

Connected and automated vehicles generate increasing amounts of data that can potentially identify passengers or drivers. Even if the data collected by a data-connected vehicle is not directly linked to the names of the passengers (or the driver, if he is still present) but to the technical aspects and functions of the vehicle, it concerns all the passengers in the vehicle and, if it can be used to identify them, it is personal data.

It is therefore important to provide those involved in testing with basic information on protecting consumer data and privacy, and to guide companies in approaching these issues responsibly.

13.2.1 Data protection laws

The most relevant privacy laws for the processing of personal data by AVs are:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation -

GDPR): Applies in all cases where data processing in relation to AVs involves the processing of personal data of natural persons.

- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ('the ePrivacy Directive'): A specific standard for all entities wishing to store or access information stored on a subscriber's or user's terminal equipment in the European Economic Area (EEA).

- The national legislation of the country in which the testing is to take place concerning the processing of personal data, or the Civil Code or other related legal acts.

13.2.2 The main principles arising from current European legislation

1. An AV and the device connected to it can be considered a so-called "terminal device" (like a smartphone, for example) according to the current interpretation of the law. An end-device is a device directly or indirectly connected to the interface of a public telecommunications network for the purpose of transmitting, processing or receiving information.
2. Prior consent of the person is required (with specific exceptions) to store information or gain access to information already stored on a subscriber's or user's terminal equipment.
3. The controller must inform the data subject of all the purposes of the processing before obtaining consent to store or access the information.
4. Informed consent should constitute the legal basis both for storing and accessing information already stored and for subsequent processing of personal data. However, it is not excluded that there will be other legal titles for the processing of personal data, in particular that the processing will be necessary to comply with a legal obligation to which the controller will be subject.
5. The GDPR is a comprehensive set of rules protecting the personal data of EU citizens. It applies to any person in the EU (legal or natural) who collects or processes personal data of individuals, including those based outside the EU who operate in the European market. Therefore, the protection provided by the GDPR extends to specific situations related to the protection of personal data of AV users. The scope of this document focuses in particular on the processing of personal data in relation to the non-professional use of connected vehicles by data subjects: e.g. drivers, passengers, vehicle owners or other road users. More specifically, it deals with personal data:
   a) processed inside the vehicle
   b) exchanged between the vehicle and personal devices connected to it (e.g. the user's smartphone)
   c) collected locally within the vehicle and exported to external entities (e.g. vehicle manufacturers, insurance companies, car repairers) for further processing
   d) collected externally, in particular by the infrastructure manager or AV service and application providers.

13.3 Handling of personal data within the operation of the AV

As mentioned in the chapter on the GDPR purpose for processing data in the AV above, personal data may be processed by multiple entities within the AV's operations and may be processed by both internal AV systems and external systems related to the infrastructure and services provided. These entities may process personal data in the following roles:

a) a controller, who alone or jointly with others determines the purposes and means of the processing of personal data
b) a processor who processes personal data for the controller.

Each role then has specific responsibilities for the security of the personal data processed.

13.3.1 Protection of the data subject

In accordance with the GDPR, AV drivers and passengers have the right to the protection of their personal data during processing. The data controller is required to implement appropriate technical and organizational measures to ensure compliance with the GDPR, with these measures being reviewed and updated as necessary.

Considering the state of the art, the cost of implementation, the nature, scope, context, and purposes of the processing, as well as the varying risks to the rights and freedoms of individuals posed by the processing, the controller must adopt suitable technical and organizational safeguards. These measures, such as pseudonymization, should be applied both when determining the means of processing and during the processing itself. They must effectively uphold data protection principles, including data minimization, and integrate necessary safeguards to meet the GDPR requirements while protecting the rights of data subjects.

13.3.2 Dealing with GDPR

To facilitate orientation, brief explanations of the basic terms used are provided:

Personal data

Personal data is any information about an identified or identifiable natural person (so-called data subject). An identifiable natural person is a natural person who can be identified, directly or indirectly, in particular by reference to an identifier (name, identification number, ...) or to one or more specific elements of the identity of that natural person (e.g. physical, physiological, genetic, psychological or cultural elements).

What is the processing of personal data?

Processing of personal data is any operation or set of operations which the controller or processor systematically carries out on personal data, whether by automated means or by other means. Processing of personal data means, for example, collection, storage on a medium, disclosure, adaptation or alteration, retrieval, use, transmission, dissemination, disclosure or storage.

Who is the data subject?

The data subject is the natural person to whom the personal data relates. In the case of AV users, this may be drivers or passengers.

What personal data appear in the AV?

As mentioned in the introduction, most data associated with AVs is considered personal data to the extent that it can be linked to one or more identifiable persons on board the vehicle. This may include, for example, in specific cases, technical data relating to the movement of the vehicle (e.g. speed or distance travelled) as well as data on the condition of the vehicle (e.g. coolant temperature, battery charge, tyre pressure).

Some data generated by AVs may also require special attention due to their sensitivity and/or potential impact on the rights and interests of data subjects. Currently, two categories of personal data have been identified as deserving special attention by vehicle and equipment manufacturers, service providers and other data controllers:

Location data

Location data is particularly indicative of the data subjects' living habits, and its collection and evaluation may interfere with fundamental rights other than the right to privacy. Journeys made are very characteristic in that they can be used to infer the place of work and residence as well as the driver's centres of interest in leisure time, and may potentially reveal sensitive information such as religious affiliation (e.g. through the place of worship) or sexual orientation or political affiliation through the places visited.

Additionally, localization data, which involves determining and tracking the precise location of the vehicle and its occupants, falls under the broader category of location data. This includes:

1. Tracking the places where an individual has travelled.
2. Locations that can reveal personal attributes, such as religious or political affiliations.
3. Locations where criminal or traffic offenses may have occurred.

Biometric data

In the context of connected vehicles, biometric data used for the purpose of uniquely identifying a natural person may be processed within the scope of Article 9 of the GDPR and national exemptions, inter alia, to allow access to the vehicle, to authenticate the driver/owner and/or to allow access to the driver's profile settings and preferences. When considering the use of biometric data, guaranteeing full control of the data subject over his/her data involves:

- Ensuring the existence of a non-biometric alternative (e.g. the use of a physical key or code) without further restrictions (i.e. the use of biometrics should not be mandatory)
- Storing and matching the biometric template in encrypted form only at local level, while the biometric data should not be processed by an external reading and matching terminal.

Purposes of processing

Personal data may be processed in the context of an AV for a variety of purposes, including the safety of both the driver (if present in the vehicle) and the AV passengers and other road users, insurance, efficient transport or information services. In accordance with Article 5 of the GDPR, data controllers must ensure that the purposes for which personal data are processed are always specific, explicit and legitimate, that personal data are not further processed in a way that is incompatible with those purposes, and that there is a valid legal basis for the processing.

Relevance and data minimisation

In order to comply with the data minimisation principle, vehicle and equipment manufacturers, AV service providers and other data controllers should pay particular attention to the categories of data processed in the operation of AVs, as they should only collect personal data that are relevant and necessary for the processing to achieve legitimate purposes. For example, location data is particularly intrusive and can reveal many of the data subjects' lifestyle habits.

Funded by the European Union

Data Processing Policy

In general, users should be able to control how their data is collected and processed in the vehicle.

- Information on processing must be provided in the driver's language (manual, settings, etc.).
- By default, only data strictly necessary for the functioning of the vehicle and its safety should be processed. Data subjects should be able to activate or deactivate the processing for each additional purpose and controller/processor and be able to delete the data concerned, taking into account the purpose and legal basis of the data processing.
- The data should not be transferred to third parties (i.e. access to the data is limited to the user and to the processor to whom the user has given consent to the processing or who processes the data to fulfil his/her legal obligations).
- The data should be kept only for the time necessary for the provision of the service or otherwise required by Union or Member State law.
- Data subjects should have the possibility to permanently delete all personal data except for the total mileage of vehicles before the AVs are put up for sale.
- Also, data subjects should, where possible, have direct access to data generated by applications related to the operation of AVs.

There are circumstances where the obligations for GDPR for academic and research purposes may be relaxed, as stated in Regulation (EU) 2016/679. Since it also depends on member states laws, the data protection authority, where the research organisation is based, is recommended to be contacted because it will be able to provide specific guidance on derogations relevant to that jurisdiction. In general, a relaxation of some of the obligations may apply where:

- Complying with the obligation would prevent or seriously impair the likelihood of successfully achieving the research purposes (if the purposes are for public research or research in the public interest).
- The processing is not likely to damage or distress an individual.
- The project continues to employ organisational and technical measures to protect the data.
- The project carefully documents the decision not to comply, specifically explaining the circumstances and reasons.

13.4 Guidelines for persons involved in AV testing

As an AV passenger or tester, individuals have the right to:

- Know certain technical details of the AV, including the level in relation to information and advice on potential risks (i.e. not information protected by, for example, trade secrets or otherwise)
- Privacy rights
- Know what information about the AV is communicated to other road users.

13.4.1 Provision of information

Before processing personal data, the data subject must be informed of the identity of the data controller (e.g. vehicle and equipment manufacturer or service provider), the purpose of the processing, the recipients of the data, the period for which the data will be kept and the data subject's rights under the GDPR.

In addition, the vehicle and equipment manufacturer, service provider or other data controller should also provide the following information to the data subject in a clear, simple and easily accessible manner:

- contact details of the Data Protection Officer
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing
- an explicit indication of the legitimate interests of the data controller or of the third party, where those legitimate interests constitute the legal basis for the processing
- the recipients or categories of recipients of the personal data, if any
- the period for which the personal data will be retained or, if that is not possible, the criteria used to determine that period
- the existence of the right to request access to and rectification or erasure of personal data or restriction of processing concerning the data subject from the controller or to object to processing, as well as the right to data portability
- the existence of the right to withdraw consent at any time, without prejudice to the lawfulness of processing based on consent prior to its withdrawal, where the processing is based on consent
- where applicable, information on the fact that the controller intends to transfer the personal data to a third country or an international organisation and on the safeguards applied to the transfer
- information on whether the provision of personal data is a legal or contractual requirement or a requirement necessary for entering into a contract, as well as on whether the data subject is obliged to provide personal data and the possible consequences of not providing such data; the existence of automated decision-making, including profiling, which has legal effects on the data subject or similarly significantly affects the data subject, and meaningful information on the logic used, as well as on the significance and foreseeable consequences of such processing for the data subject. This should apply in particular in the context of the provision of insurance to individuals on a usage basis
- the right to lodge a complaint with a supervisory authority
- information on further processing
- in the case of joint data management, clear and complete information on the responsibilities of each data controller.

The information addressed to data subjects can be provided in layers, i.e. by separating two levels of information: on the one hand, the first level information that is most relevant to data subjects and, on the other hand, information that is likely to be of interest at a later stage.

In addition to the identity of the data controller, the first level of basic information includes the purpose of the processing and a description of the data subject's rights, as well as any additional information on the processing that has the greatest impact on the data subject and on the processing that might surprise the data subject.

Data subjects may be informed by means of concise and easily understandable clauses in the vehicle purchase contract, in the service contract and/or in any written medium, through distinct documents (e.g. vehicle maintenance record book or manual) or on-board computer.

13.5 Consent for AV

If the processing of data is based on consent, all the elements of valid consent must be met, which means that the consent must be free, specific and informed and must constitute an unambiguous expression of the data subject's will.

Data controllers must pay careful attention to the means of obtaining valid consent from the different actors involved, such as car owners or users. Such consent must be given separately, for specific purposes and must not be linked to a contract for the purchase or lease of a new car. Consent must be as easy to withdraw as to grant.

The same should apply where consent is required to comply with the requirements of the ePrivacy Directive, for example where information is stored or accessed already stored in the vehicle, as required in certain cases by Article 5(3) of the ePrivacy Directive.

Where data are collected on the basis of consent as required by Article 5(3) of the ePrivacy Directive or under one of the exemptions under Article 5(3) and subsequently processed in accordance with Article 6 of the GDPR, they may only be further processed if the controller requests additional consent for that additional purpose or if the controller can demonstrate that it is necessary under Union or Member State law to ensure the purposes referred to in Article 23(1) of the GDPR.

Initial consent never authorizes further processing, as consent must be informed and specific to be valid. For example, telemetric data collected during the use of a vehicle for maintenance purposes may not be disclosed to motor insurance companies without the consent of the users in order to create driver profiles for the purpose of offering insurance policies based on driver behaviour.

13.5.1 Consent forms – additional tips for researchers

In the context of testing connected and automated vehicles (AVs), based on past experience in testing autonomous systems, we can summarize the main problematic points that often arise when designing test scenarios involving the general public. They should be kept in mind when creating consent forms for test scenarios. These include:

- Treat video recordings as separate data: Video recordings captured during testing may be more sensitive than other data and stored separately, raising privacy concerns and requiring specific consent. Participants should be clearly informed about the purpose of video recording, how the recordings will be used (e.g., additional consent sought for publishing any short sample), and who will have access to them.
- Reusing of data in new research projects: Data collected during AV testing may be reused in future research projects. This broader sharing could exceed what was initially agreed upon in the basic consent form, unless the wording defines this possibility. Clear communication is necessary about the possibility of data being used in subsequent studies, including sharing with new research partners not originally involved in data collection. Consent forms should address the potential for sharing collected data with academic institutions or universities that were not initially part of the project, ensuring transparency and respecting participants' rights to know who might have access to their data.
- Data retention period: Clearly stating the period for which data will be retained and the criteria used to determine that period is crucial for transparency and compliance with legal requirements.

- Insurance and liability issues: Participants need to be informed about how risks associated with the research will be managed, including insurance coverage for any potential harm or accidents during testing. This includes outlining the research risks and the measures in place to mitigate them.
- GDPR exemptions for research: GDPR provides certain exemptions for research activities, such as not requiring the deletion of data if it would cause disproportionate effort. Participants should be made aware of these exemptions and how they might affect their rights, including the retention and use of their data. See “Dealing with GDPR” chapter.
- Right to withdraw consent: Clear instructions should be provided on how participants can withdraw their consent at any time and the implications this will have on their data, particularly concerning data that has already been used in research.
- Data anonymization and pseudonymization: Information on how personal data will be anonymized or pseudonymized to protect privacy should be included. Participants should understand the measures taken to safeguard their identity.
- Data security measures: Details about the technical and organizational measures in place to ensure data security should be clearly communicated to participants, reassuring them that their data is protected against unauthorized access and breaches.

Including these details in consent forms can help mitigate common concerns and ensure that participants are fully informed about how their data will be handled throughout the research process. The general principle for creating consent forms is to keep the scope reasonable; try to be concise and to the point when describing each measure. This is particularly important in cases where passengers involved in the test process read and sign the consent form directly at the test site before the test drive begins.

13.6 AI Act

The Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending certain Union legislation in the field of artificial intelligence [30] was approved in March 2024. It will be applied gradually over the next 6–24 months after its promulgation. It is one of the first comprehensive AI regulations in the world.

The regulation sets four levels of risk:

1. prohibited systems (e.g. covert manipulation of behaviour and emotions or social credit scoring, certain biometric identification)
2. high risk systems ("HRAIS" for high-risk AI systems, e.g. biometric identification in general, uses with direct impact on humans, such as certain social policies, HR, healthcare, etc.)
3. low-risk systems (used for human interaction or artificially generated content) should meet minimum transparency standards, e.g. systems must inform the user that he is interacting with AI
4. systems with minimal risk (most systems in use, such as chatbots).

Within the European Union, the following regulations are now primarily relevant in relation to (partially) autonomous vehicles, or their development and approval for use:

- Regulation (EU) 2018/858[31] of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems,

components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and No 595/2009 and repealing Directive 2007/46/EC ("TAFR" for Type-Approval Framework Regulation).

- Regulation (EU) 2019/2144[32] of the European Parliament and of the Council of 27 November 2019 concerning type-approval requirements for the protection of motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, with regard to general safety and the protection of vehicle occupants and vulnerable road users ("GSR" for General Safety Regulation).

As stated in Recital 29 of the AI Act, in respect of high risk AI systems which are safety features of products or systems, or which are themselves products or systems falling within the scope of enumerated EU legislation including the above Regulations, it is appropriate to amend these acts to ensure that the specificities of each sector are taken into account and without prejudice to the existing management, conformity assessment and enforcement mechanisms under these specific regulations.

Although many of the AI systems used in AVs are likely to fall into the high-risk category, the AI Act recognises that AVs are already regulated by other Union legislation, such as TAFR and GSR. As such, the AI Act seeks to ensure that the management of these systems is consistent with existing vehicle regulatory rules by not directly imposing rules or requirements for them, but merely bridging the various industry specifics and general requirements for high-risk systems. Therefore, although these systems will be classified as high risk, they will be primarily governed by their sector-specific legislation and the standard regime of requirements or obligations under the AI Act will not apply to these systems. For the remaining systems used in AVs that are not subject to specific regulation, the standard approach to determining the level of risk will apply, which means that it is necessary to examine whether the system falls within high-risk use cases (Annex III) or whether it operates in a manner that is subject to specific transparency requirements (Article 52 of the AI Act).

So, what are the requirements for AI systems contained in AVs covered by Union harmonisation legislation? Article 2.2 of the AI Act lists the provisions relevant to HRAIS that are covered by specific Union harmonisation legislation, including the EA. Accordingly, AVs assessed as HRAIS will also be subject to Articles 84 (assessment and review by the Commission) and 53 (regarding regulatory sandboxes or AI regulatory sandboxes). The AI Act also anticipates the implementation of specific amendments to the TAFR and GSR under Articles 81 and 82, which specify that the requirements for HRAIS should be taken into account in future legislative acts. In other words, the AI Act's provisions relating to HRAIS, including the requirements and obligations, will not apply to AVs.

13.7 Safe and Ethical Operational Concept Documentation

Adopting a Safe and Ethical Operational Concept (SEOC) [33] model as public documentation for automated vehicles in Europe could bring clarity and transparency to AV operations. Drawing inspiration from the UK's SEOC approach, an EU-wide SEOC-type documentation could detail an AV's safety, accessibility, and data privacy practices, offering insights beyond vague high-level testing statements like "thousands of kilometres tested." This documentation would ideally provide practical descriptions, such as AV responses to emergencies (both before and after a collision), pedestrian safety protocols, overtaking, and remote control capabilities, contributing to public trust.

A simple SEOC document template, with structured but flexible fields, could support companies in communicating essential information while respecting national regulatory nuances. Similar to online

data processing or GDPR statements by companies, made available for testers and general public, this document would reassure the public by making safety and ethical behaviours clear.

This is particularly important when deploying pilot operations with passengers, which will inevitably attract a lot of interest not only from the public but also from the media. With a well-crafted SEOC, it is very easy to answer frequently asked questions regarding the intended behaviour of an autonomous vehicle in critical or otherwise significant situations. It is clear that without significant openness to the public, the deployment of such ground-breaking technologies as automated driving systems for road vehicles will be very difficult.

As an initial step, we propose that organisations publish a short online description of how their AV avoid accidents and handle emergencies. This description could be used together with a similar page describing data collection and privacy aspects. Such online documentation would be easy to link passengers to.

13.8 Additional Ethical Considerations in CCAM Testing

While previous sections have focused on critical aspects such as privacy and legal compliance, there are additional ethical considerations essential to the responsible development and testing of CCAM technologies. Addressing these considerations ensures that the deployment of CCAM systems aligns with societal values and promotes public trust. This chapter discusses ethical decision-making in algorithms, security, accessibility and inclusivity, comprehensive impact assessment, and effective public engagement.

13.8.1 Safety Assurance

While safety aspects are discussed in detail elsewhere in this document, it is important to highlight additional ethical considerations related to safety in the context of CCAM testing. Ensuring the safety of all road users is paramount, and developers have an ethical responsibility to conduct rigorous testing of automated driving systems under various conditions.

Adopting a phased approach to testing enhances safety by allowing issues to be identified and addressed progressively. Beginning with simulations and closed test tracks before advancing to public road tests reduces risks during early development stages.

For larger tests, involving independent evaluators to systematically analyse key aspects of vehicle safety can provide valuable insights and enhance credibility. For smaller tests involving a single vehicle with an onboard safety driver, comprehensive company documentation and safety plans are essential.

The presence of a safety operator or driver during testing, especially in critical areas such as school zones, adds an additional layer of protection. Their role may also include engaging with passengers, overseeing onboard safety, assisting with consent forms, and aiding passengers with disabilities.

Continuous monitoring for malfunctions or unexpected behaviours allows for immediate response to potential issues. Developing comprehensive test plans, documenting safety considerations, and establishing clear procedures for handling incidents or accidents contribute to a proactive safety culture.

Funded by
the European Union

13.8.2 Ethical Decision-Making in Algorithms

Developers should be mindful of potential biases in the data used to train automated systems and neural networks, as biases can lead to discriminatory behaviours or unfair treatment of certain groups. To mitigate such risks, algorithms should be trained on diverse and representative datasets that encompass a wide range of scenarios and user profiles. Regular audits and evaluations of algorithmic performance can help identify and correct any unintended biases or ethical concerns.

Involving ethicists and legal experts in the development process can provide valuable perspectives on ethical considerations and assist in aligning technological capabilities with societal expectations.

Transparency in algorithmic decision-making is also important. While the complexity of machine learning models may make it challenging to explain every decision, providing stakeholders with understandable principles about how decisions are made can enhance trust.

13.8.3 Security

Security is a fundamental aspect of CCAM systems, given the potential risks associated with unauthorized access or malicious attacks. Ensuring the cybersecurity of automated vehicles protects not only data but also the safety of passengers and other road users. Developers should implement robust security measures to safeguard against hacking, data breaches, and other security threats.

This involves adopting best practices in cybersecurity, such as encrypting sensitive data, using secure communication protocols, and regularly updating systems to address vulnerabilities. Conducting security assessments and penetration testing can help identify weaknesses before they are exploited.

Physical safety measures are equally important. Implementing video monitoring can enhance security by deterring unauthorized activities and assisting in incident investigations. Equipping vehicles with emergency buttons allows passengers to request immediate assistance in case of emergencies. Remote door control systems enable authorized personnel to manage access to the vehicle, providing additional security during critical situations. Preparing for such scenarios ensures the safety and well-being of passengers and contributes to overall system security.

13.8.4 Accessibility and Inclusivity

The advancement of CCAM technologies offers an opportunity to enhance mobility for all segments of the population. To maximize these benefits, it is important to design systems that are accessible and inclusive, considering the needs of individuals with disabilities, the elderly, and others who may face barriers to mobility. While prototype vehicles aren't required to fulfil all accessibility standards, it is good practice to collect feedback from diverse users during system design to improve prototypes toward market-ready products.

User-friendly interfaces and audible and visual alerts can make automated vehicles more accessible. Engaging with diverse user groups during the design and testing phases helps identify specific needs and preferences, leading to solutions that are more universally beneficial. Additionally, efforts should be made to address socio-economic barriers that may limit access to these technologies, ensuring that the benefits of CCAM are equitably distributed.

Funded by
the European Union

13.8.5 Wide and Transparent Impact Assessment

Understanding the broader impacts of CCAM deployment is essential for responsible innovation. Testing projects, when resources allow, should strive to conduct comprehensive evaluations rather than focusing solely on technological development. This means assessing how automated vehicles affect safety, traffic efficiency, the environment, employment, and social dynamics.

Transparency in these assessments is crucial. Methodologies, assumptions, and findings should be openly shared with stakeholders to enable replication and further improvement by others. For instance, clearly documenting the assumptions about how certain percentages of specific types of accidents are expected to be reduced by the new technology allows future researchers and developers to verify, challenge, or refine these calculations.

By considering both the positive and negative implications, developers and policymakers can make informed decisions that enhance benefits and mitigate adverse effects. Engaging independent evaluators can provide unbiased insights and strengthen the credibility of the assessments. Utilizing established frameworks, such as the FESTA and EU-CEM handbooks, ensures that evaluations are conducted using standardized methodologies and best practices.

13.8.6 Marketing, Communications, and Public Engagement

Effective communication and public engagement are crucial for the successful integration of CCAM technologies into society. Transparent and honest communication about the capabilities and limitations of automated vehicles helps build public trust and sets realistic expectations. Marketing efforts should avoid overstating the technology's readiness or downplaying potential risks.

User engagement is essential not only for creating trust but also for learning and continuous improvement of CCAM systems. Actively involving users through surveys, community meetings, test drives, and collaborative projects allows developers to attract test participants and gather valuable feedback. This engagement fosters a culture of openness regarding how vehicles behave, how they avoid accidents, and how they accommodate different user needs.

Funded by
the European Union

14 Conclusions

The analysis of the current legislative basis for AV testing across EU countries reveals a diverse landscape, ranging from dedicated laws to adaptations of existing frameworks. This diversity underscores the urgent need for harmonization to facilitate cross-border testing and development. The proposed framework addresses this challenge by offering flexibility in safety validation responsibilities, allowing for self-assessment, authority validation, or third-party assessment. This adaptability is crucial in accommodating different national capabilities and test complexities.

Central to the framework is the expanded role of safety operators, including the possibility of remote operation, reflecting the evolving nature of AV technology. This emphasis on safety extends to the comprehensive two-stage documental submission process for test permits, which ensures thorough vetting of safety and compliance measures. The inclusion of proving ground pre-tests as a critical safety checkpoint before public-road testing further reinforces this safety-first approach.

A significant step towards harmonization is the proposed Safety Validators Group (SVG) and European platform for public road testing. These initiatives aim to streamline the mutual recognition process across member states while maintaining rigorous safety standards. The framework also introduces a robust approach to risk assessment, covering both system and activity-related risks, providing a solid foundation for safe AV testing.

Recognizing the growing importance of cybersecurity in AV systems, the framework includes a comprehensive cybersecurity management plan. This proactive approach is essential in maintaining the integrity and safety of AV systems in an increasingly connected environment. Similarly, the established processes for accident reporting and periodic test reporting not only ensure continuous safety monitoring but also contribute valuable data for ongoing improvements in AV technology and testing procedures.

The framework places a strong emphasis on ethical considerations, offering practical advice for addressing ethical challenges in AV testing. It recommends assigning a person responsible for ethical oversight, using a provided checklist as a guide. Drawing inspiration from the UK's Safe and Ethical Operational Concept (SEOC), the document also proposes publishing an online safety principles document that details how vehicles avoid accidents and manage emergency situations, thereby enhancing transparency and public trust.

Looking forward, the implementation of this framework should be accompanied by a pilot program in selected EU member states to test its effectiveness in real-world scenarios. Establishing a dedicated working group to monitor this implementation and gather feedback will be crucial for future refinements. Additionally, developing comprehensive training programs for safety validators and operators will ensure consistent application of the framework across different jurisdictions.

To streamline the process further, creating a European platform for test permit applications and processing public road testing should be a priority. This would not only increase efficiency but also provide a centralized system for data collection and analysis, benefiting future research and policymaking in the field of AV testing.

As the field of autonomous driving continues to evolve rapidly, this framework should be viewed as a living document. Annual reviews and updates will be necessary to incorporate technological

Funded by
the European Union

advancements, regulatory changes, and lessons learned from practical applications. Special attention should be given to emerging technologies such as AI-driven decision-making systems and advanced V2X communications. Furthermore, aligning this framework with evolving EU policies on transportation, data protection, and environmental sustainability will ensure its continued relevance and effectiveness.

In conclusion, this framework represents a significant step towards creating a unified, safe, and ethically sound environment for AV testing across Europe. By addressing key challenges in harmonization, safety, data protection, and ethical considerations, it lays the groundwork for responsible innovation in autonomous vehicle technology. The success of this framework will depend on continued collaboration between regulators, industry stakeholders, and researchers, as well as its ability to adapt to the rapidly changing landscape of automated driving technology.

Funded by
the European Union

15 References

[1] SAE J3016, "SAE Levels of Driving Automation™ Refined for Clarity and International Audience," May 2021, Accessed: Jun. 03, 2024. [Online]. Available: https://www.sae.org/blog/sae-j3016-update#:~:text=With%20a%20taxonomy%20for%20SAE%E2%80%99s%20six%20levels%20of,of%20motor%20vehicles%20and%20their%20operation%20on%20roadways.

[2] European Commission, *REGULATION (EU) 2022/1426*. 2022.

[3] European Commission, "GUIDELINE ON A UNIFORM EU-WIDE PROCEDURE FOR THE SUBJECTS OF PRE-TYPE APPROVAL ASSISTED (ADAS) AND AUTOMATED VEHICLE (ADS) TESTING AND RECOGNITION OF TESTING APPROVALS AMONG MEMBER STATES." Accessed: Feb. 18, 2025. [Online]. Available: https://circabc.europa.eu/ui/group/4273d650-b8a9-4093-ac03-18854fbba4b5/library/0f6b3136-df1c-426e-b17a-e1109dafaa1a/details

[4] Dirección General de Tráfico, "VEH-2022-07," 2022.

[5] ISO, "ISO 26262-3:2018. Road vehicles functional safety. Part 3: Concept phase," 2018.

[6] "Regulation - 2016/679 - EN - gdpr - EUR-Lex." Accessed: Jun. 30, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[7] "Einride Approved by NHTSA - Einride Press." Accessed: Feb. 20, 2025. [Online]. Available: https://www.einride.tech/press/einride-gets-nhtsa-approval

[8] UNECE, "UN R79. Uniform provisions concerning the approval of vehicles with regard to steering equipment," 2024.

[9] UNECE, "UN R152. Uniform provisions concerning the approval of motor vehicles with regard to the Advanced Emergency Braking System (AEBS) for M1 and N1 vehicles," Sep. 2023.

[10] European Commission, "REGULATION (EU) 2021/1958," no. Rules concerning the specific test procedures and technical requirements for the type-approval of motor vehicles with regard to their intelligent speed assistance systems and for the type-approval of those systems as separate technical units, Nov. 2021.

[11] UNECE GRVA, "Information sharing, peer review and mutual recognition of ADS approvals," 2024.

[12] UNECE GRVA, "6th GRVA Workshop on ADS - Information sharing, peer review and mutual recognition of ADS approvals," Mar. 2025.

[13] European Commission, "Implementing decision - EU - 2025/264 - EN - EUR-Lex." Accessed: Mar. 03, 2025. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32025D0264

[14] UNECE - IWG on DETA, "Status DETA Ways forward," 2017.

[15] UNECE - IWG on DETA, “IWG on DETA document 39-03e INITIAL DRAFT-Guidelines for the use of DETA with regard to the exchange of information on Cyber Security,” 2024.

[16] “UN Regulation No 155.” Accessed: Feb. 05, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2021/387/oj/eng

[17] “Discover the cross-border digital testbed for autonomous and connected driving.” Accessed: Dec. 10, 2024. [Online]. Available: https://www.infogreen.lu/discover-the-cross-border-digital-testbed-for-autonomous-and-connected-driving.html

[18] “HOME - Bizkaia Connected Corridor.” Accessed: Dec. 10, 2024. [Online]. Available: https://bizkaiaconnectedcorridor.biz/en

[19] Association of the Automotive Industry (VDA), “VDA 702_2015,” 2015.

[20] European Commission, “COMMISSION IMPLEMENTING REGULATION (EU) 2022/1426,” 2022.

[21] “Connected, Cooperative and Automated Mobility Roadmap Update of Chapter 2 ‘Agenda 2030’ on Innovation Use Cases”, Accessed: Feb. 05, 2025. [Online]. Available: www.ertrac.org

[22] J. Kremenović, “FAME D5.1 Analysis of testing procedures and administrative framework conditions on CCAM testing,” MD, 2024.

[23] UNECE, “UN R.160 - 02 series,” 2024.

[24] UNECE, “UN R157 on ALKS,” 2023.

[25] “CCAM Data Sharing Framework - Connected Automated Driving.” Accessed: Jun. 30, 2025. [Online]. Available: https://www.connectedautomateddriving.eu/data-sharing/ccam-data-sharing-framework/

[26] A. Limited, “ITIL ® Foundation ITIL 4 Edition 2,” 2019, Accessed: Jun. 30, 2025. [Online]. Available: https://www.axelos.com

[27] “ISO/IEC 27001:2022 - Information security management systems.” Accessed: Jun. 30, 2025. [Online]. Available: https://www.iso.org/es/norma/27001

[28] “European Common Evaluation Methodology for CCAM - Connected Automated Driving.” Accessed: Jun. 30, 2025. [Online]. Available: https://www.connectedautomateddriving.eu/methodology/common-evaluation-methodology/

[29] FESTA Project, “FESTA-Handbook-Version-8-FINAL-Version-20-09,” Sep. 2021, Accessed: Dec. 18, 2024. [Online]. Available: https://www.connectedautomateddriving.eu/wp-content/uploads/2024/07/FESTA-Handbook-Version-8-FINAL-Version-20-09.pdf

Funded by the European Union

[30] European Union, “Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence,” Jun. 2024. [Online]. Available: http://data.europa.eu/eli/reg/2024/1689/oj

[31] “Regulation - 2018/858 - EN - EUR-Lex.” Accessed: Jun. 30, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2018/858/oj/eng

[32] “Reglamento - 2019/2144 - EN - EUR-Lex.” Accessed: Jun. 30, 2025. [Online]. Available: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:32019R2144

[33] UK Centre for Data Ethics and Innovation, “Responsible Innovation in Self-Driving Vehicles.” Accessed: Nov. 18, 2024. [Online]. Available: https://www.gov.uk/government/publications/responsible-innovation-in-self-driving-vehicles/responsible-innovation-in-self-driving-vehicles#annex-a-safe-and-ethical-operational-concept-and-safety-management-systems

Funded by
the European Union

Annex I – Application form content example

1. DATA REGARDING THE ORGANIZATION SUBMITTING THE APPLICATION	
Company/organization name	
Company identification number	
Registered Office	
Telephone Number	
E-mail	

2. DATA REGARDING THE PERSON SUBMITTING THE APPLICATION	
Name	
Surname	
ID or Passport number	
Telephone Number	
E-mail	

Funded by
the European Union

Annex II – Template for test vehicle data

DATA REGARDING THE TEST VEHICLE SUBMITTING THE APPLICATION	
BASIC DATA	
Data	
Applicant	
Vehicle manufacturer	
Vehicle category	
Vehicle identification number(s) (e.g., VIN)	
Location of the vehicle identification number(s)	
Base vehicle	
Base type approval number (if applicable) (including the corresponding extension):	
GENERAL VEHICLE STRUCTURE	
Nº of axles and Tyres	
Powered axles (nº, location and interconnection):	
MASSES AND DIMENSIONS	
Wheelbase	
Axle tracks	
Vehicle length	
Vehicle width	
Vehicle height	
Mass in running order	
Minimum permissible mass	
Maximum technically permissible mass	
POWER UNIT	
Engine manufacturer	
Engine code assigned by the manufacturer	

Funded by the European Union

Internal combustion engine (yes/no)	
Electric engine (yes/no)	
Hybrid engine (yes/no)	
Operating principle	
Type of fuel or energy source	
Maximum net power (kW)	
TRANSMISSION	
Type (mechanical/hydraulic/electric/ etc.)	
Gear box (type)	
Number of gears	
SUSPENSION	
Brief description of front and rear suspension types	
Tyres and wheels (main characteristics)	
STEERING	
Steering, type of assistance	
BRAKING	
Brief description of the braking system **ABS: yes/no**	

Annex III – Compliance with cyber security template

Applicant's declaration of compliance with appropriate cybersecurity levels

Applicant Name: .....

Applicant Address: .....

(Applicant Name) attests that the necessary processes to comply with the requirements for Cyber Security are installed and will be maintained.

Done at: (place) .....

Date: .....

Name of the signatory: .....

Function of the signatory: .....

(Stamp and signature of the applicant 's representative)

Funded by the European Union

Annex IV – Cybersecurity vulnerabilities and threats

Threats to "External connectivity and connections"	Mitigation
Manipulation of functions designed to remotely operate vehicle systems, such as remote key, immobiliser, and charging pile	Security controls shall be applied to systems that have remote access
Manipulation of vehicle telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)	
Interference with short range wireless systems or sensors	
Corrupted applications, or those with poor software security, used as a method to attack vehicle systems	Software shall be security assessed, authenticated and integrity protected. Security controls shall be applied to minimise the risk from third party software that is intended or foreseeable to be hosted on the vehicle
External interfaces such as USB or other ports used as a point of attack, for example through code injection	Security controls shall be applied to external interfaces
Media infected with viruses connected to the vehicle	
Diagnostic access (e.g. dongles in OBD port) used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly)	Security controls shall be applied to external interfaces

Funded by the European Union

Threats to "Potential targets of, or motivations for, an attack"	Mitigation
Extraction of copyright or proprietary software from vehicle systems (product piracy / stolen software)	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP
Unauthorized access to the owner's privacy information such as personal identity, payment account information, address book information, location information, vehicle's electronic ID, etc.	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Examples of Security Controls can be found in OWASP
Extraction of cryptographic keys	Security controls shall be implemented for storing cryptographic keys e.g. Security Modules
Illegal/unauthorised changes to vehicle's electronic ID	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP
Identity fraud. For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend	
Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP. Data manipulation attacks on sensors or transmitted data could be mitigated by correlating the data from different sources of information
Data manipulation to falsify vehicle's driving data (e.g. mileage, driving speed, driving directions, etc.)	
Unauthorised changes to system diagnostic data	
Unauthorized deletion/manipulation of system event logs	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP.
Introduce malicious software or malicious software activity	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP.
Fabrication of software of the vehicle control system or information system	

Funded by the European Union

Denial of service, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging	Measures to detect and recover from a denial of service attack shall be employed
Unauthorized access to falsify configuration parameters of vehicle's key functions, such as brake data, airbag deployed threshold, etc.	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP
Unauthorized access to falsify charging parameters, such as charging voltage, charging power, battery temperature, etc.	

Annex V – Model of report for recognition of permits granted by a different authority

1. Identification data of the original test permit application

a. **Authority granting the permission.**
   In this chapter the authority known as lead member state shall identify itself
b. **Applicant information.**
   In this chapter, the authority shall identify the applicant of the test permit application.
c. **Vehicle/s identification**
   In this chapter, the vehicle, or vehicles object of the test pilot shall be identified.
d. **Description of the original activity**
   In this chapter, a description of the activity and safety assessment conclusions by the lead member state authority shall be included.

2. Use of FAME's Recommendation during the original authorisation process

The Authority reviewing the permission hereby declares that the following items of the FAME recommendations have been taken into consideration in order to grant the permission for the test pilot identified in chapter 1:

a. **Safety validation responsible:**

Safety validator	Comments
Authority / Third party / Applicant	

b. **First documental submission stage:**

Term		Recommendations followed? (Y/N)	Comments
Description of testing activity			
System documentation package	Function name		
	SW version		
	Scope of the function		
	Override implementation		
	Emergency disconnection implementation		
	Cybersecurity		
	Compliance with traffic regulation		

Funded by the European Union

c. Second documental submission stage:

Item	Recommendations followed? (Y/N)	Comments
Successful pre-test on proving ground		
Use of EDR and/or DSSAD		
Use of remote safety operator		
other		

d. Risk Assessment:

Item	Recommendations followed? (Y/N)	Comments
System risk evaluation		
Activity risk evaluation		
Safety maintenance		

e. Test vehicle(s) inspection:

Recommendations followed? (Y/N)	Comments

f. Safety operator:

Item	Recommendations followed? (Y/N)	Comments
Safety operator(s) responsibility		
Safety operator(s) training		
Safety operator(s) driving license		

Funded by the European Union

g. Proving ground pre-tests:

Item	Recommendations followed? (Y/N)	Comments
Manual driving tests		
Override		
Emergency disconnection		
Longitudinal control tests		
Lateral control tests		
Recognition and compliance with traffic signs		
Other		

h. Software version traceability:

Recommendations followed? (Y/N)	Comments

i. Data requirements during and after CCAM testing:

Item	Recommendations followed? (Y/N)	Comments
Short-term reporting		
Long-term reporting		
Monitoring requirements		
KPIs defined		

j. Ethical recommendations:

Recommendations followed? (Y/N)	Comments

3. Additional comments

Funded by the European Union

Annex VI – Ethical checklist for Connected, Cooperative, and Automated Mobility (CCAM) tests

This checklist targets research and development activities within CCAM, such as those for automated driving. It highlights ethical aspects to consider during development and testing, helping projects prepare comprehensively. This checklist aims to cover critical ethical considerations for CCAM tests, but it should be continually revised and updated to reflect new challenges and advancements in the field.

1. Safety Assurance

- Ensure rigorous testing of automated driving systems under various conditions.

  Test scenarios and selection of areas should be based as much as possible on the regulatory framework within the World Forum for the harmonization of vehicle regulations (WP.29), which has been developing very dynamically in the field of CCAM in recent years, including the issue of testing using AI. Due to the deployment of new automated technologies, it is necessary to cover as wide a range of operational situations as possible when creating test scenarios, i.e. testing in different weather conditions, at night, at different traffic volumes, testing the behaviour of systems when interacting with integrated rescue system vehicles and so on.
- Adopt a stepwise approach to testing: begin with simulations and closed test tracks, gradually progressing to public road tests.
- Employ an independent evaluator to systematically analyse key aspects of vehicle safety, e.g. carry out test scenarios at a proving ground.

  For large tests, independent evaluation is recommended. For smaller tests involving a single vehicle with an onboard safety driver, company documentation and safety plans are likely sufficient.
- Implement robust fail-safe mechanisms that default to a safe state in emergencies.
- Ensure the presence of a safety operator/driver for emergency situations when operating/testing automated vehicles in critical areas such as schools.

  The safety operator should preferably remain out of sight to prevent interference with the testing process. Visible drivers can lead to unintended eye contact with other road users, disrupting the automation test. While teleoperation is the future, safety drivers should not be removed prematurely to maintain safety during development. Consider also the role of the safety person onboard in pilot deployments, which may involve several other aspects, such as being able to introduce the ongoing test and its broader ecosystem meaning to the public during the ride, overseeing safety onboard, collecting and helping to fill out consent forms if needed, or, for example, assisting people with disabilities.
- Continuously monitor for malfunctions or unexpected behaviours.
- Document safety considerations and test plans; establish procedures for accidents.
- Ensure AV doesn't obstruct first responders.
- Develop an insurance model.

Funded by the European Union

2. Ethical Decision-Making in Algorithms

- Avoid algorithmic bias and discrimination.

  Ensure that algorithms are trained on diverse datasets to minimize bias. Regularly review and update the algorithms to detect and correct any discriminatory patterns.
- Incorporate ethical guidelines in decision-making, consulting ethicists, legal experts, and the public.

  Refer to established frameworks such as the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems for guidance on integrating ethical considerations into technology development. Regarding the proper ethics of the decision-making processes of the AI-based systems, the Ethics guidelines for Trustworthy AI (2019) or the later JRC reports Trustworthy autonomous vehicles (2021) and Toward explainable, robust and fair AI in automated and autonomous vehicles (2023), based on expert workshops, are also good guides.
- Ensure transparency in the decision-making process of automated systems.

  Stakeholders should understand the basis on which final decisions are made by the system, even if every single decision cannot be fully predicted.
- Clearly define responsibility and accountability for decisions made by these systems, whether it lies with the manufacturer, the software developer, or another party.

  The so-called "handover period", during which responsibility passes from one entity to another, is risky. Pay attention to its clear definition, good training of the test drivers as well as the acquisition of a reliable record in case of possible litigation.
- Create a public document detailing accident-avoidance methods with specific details rather than just general safety processes.

  Promote an openness concept for safety details and approaches, similar to the UK Safe and Ethical Operating Concept (SEOC)
- Drive cautiously, especially near vulnerable groups (children, elderly, disabled, inebriated), as required by law.

  Carefully select test routes and locations to minimize risks to vulnerable groups. Ensure that the vehicle drives at a safe speed, assuming all pedestrians are potentially unpredictable if the vehicle cannot classify them. It is important for machine learning systems to capture as many different scenarios as possible, so take extra care in these particular cases.
- Conduct regular audits of algorithms to identify and rectify potential ethical issues.

3. Data Privacy

- Collect data only for specified, explicit, and legitimate purposes; avoid unnecessary data collection.
- Comply with data protection laws (e.g., GDPR), including documenting data processing activities, management processes, and deletion schedules.
- Be transparent about data collection and usage; user briefings, posted signs and web pages, agreements etc.
- Apply anonymization techniques wherever possible, store only relevant and necessary data.
- Ensure that data collected from vehicles/users is stored securely and used ethically. Data analysis and research reports should focus on behaviour of groups instead of individuals.

Funded by the European Union

4. Security

- Conduct security audit/review to identify potential vulnerabilities.
- Implement robust surveillance systems to monitor vehicle operations and data access, ensuring compliance with security protocols.
- Utilize automated safety features to enhance user safety and prevent unauthorized access. These features should include continuous monitoring with video cameras, emergency buttons for passenger use, and advanced door control mechanisms to ensure security.
- Establish protocols for emergency situations, ensuring quick and effective responses.
- Prevent misuse and ensure robust cybersecurity measures.

  Conduct simulated cyber-attacks to test and strengthen the system's defenses against potential threats.

5. User Consent and Control

- Obtain clear user consent for data collection and usage. Provide a real opportunity to read through and understand agreements. Agreements should be clearly written and contain e.g. responsibilities.
- Provide users with control over their data and participation.
- Educate users on the capabilities and limitations of automated systems, also from safety and responsibility aspects.

6. Accessibility and Inclusivity

- Ensure technology and infrastructure cater to diverse users, including those with disabilities.
- Address socio-economic access barriers.
- Design user-friendly and inclusive interfaces. Test their acceptance on different target-groups.
- Engage diverse stakeholders, including underrepresented groups, in design and testing.

7. Legal and Regulatory Compliance

- Adhere to all relevant laws and regulations.
- Collaborate with regulatory bodies for ongoing compliance.
- Stay updated with legislation changes in automated driving.
- Maintain communication with national public research organizations to stay informed about the latest research and best practices in the field.

8. Wide and Transparent Impact Assessment

- Conduct a comprehensive evaluation addressing topics such as safety, traffic flow, efficiency, environmental impact, economic factors, workforce effects, and inclusivity.
- Maintain transparency in assumptions and analyses.
- Refer to the FESTA Handbook for comprehensive guidelines on conducting field operational tests.
- Utilize the EU-CEM Handbook for guidance on setting up and carrying out evaluations of direct and indirect socio-economic impacts on different user groups. This handbook is part of the European framework for testing CCAM on public roads.

Funded by
the European Union

9. Marketing, Communications and Public Engagement

- Engage the public to understand their concerns and expectations through surveys, forums, and groups.
- Be transparent about the technology's capabilities and limitations.
- Provide clear information on testing processes and outcomes.
- Encourage cross-sector collaboration and stakeholder engagement for comprehensive learning and development.

ANNEX VII – Hi-Drive use case description

Topic	Use Case 1.2.1	Use Case 1.2.2	Use Case 1.2.3
Name	**Demonstrator to Test a AD Functionality on Public Roads - Test are carried out only in one country**	**Demonstrator to Test a AD Functionality on Public Roads - Test are carried out only in one country with ODD extension**	**Demonstrator to Test a AD Functionality on Public Roads - Test are carried out only in one country and demonstration for final event on public roads in a second country**
Description of testing activity			
- Objectives of the activity.	Study the technical capabilities and interaction with other traffic participants in the ODD, such as - sensor performance (missed objects, precision in detection, how man vehicles are detected correctly), - driving performance / comfort (driven speed, lat. and long. acceleration) and - interaction / safety related metrics (distance / time gap / time to collision to other object) - advantages & disadvantages, technical limitations of V2X sensor in traffic light scenarios (e.g. how reliable is the detection) and detection other traffic participants at crossings (e.g. when are traffic participants detect, how precise are the traffic participants detected)		Demonstration at the final event (Driving with visitors; Safety Driver on driver seat)
- Connected/automated features to be deployed.	SAE Level 3 system with V2X communication including redundancy for sensors		
- Description of the scenarios and test procedure to be tested for each feature.	Driving in the city of Wolfsburg: Driving on one lane and two lane per driving directions roads (Speed limit 30 and 50 km/h), Passing Traffic lights, conducting right and left turns (with and without VRUs)	Driving in the city of Wolfsburg and rural road around Wolfsburg: Urban: Driving on one lane and two lane per driving directions roads (Speed limit 30 and 50 km/h), Passing Traffic lights, conducting right and left turns (with and without VRUs) Rural: Driving on one lane per driving directions roads (Speed limit 70 km/h), Passing Traffic lights, conducting right and left turns (with and without VRUs)	Driving in the city of Brussels around the Autoworld: Driving on one lane and two lane per driving directions roads (Speed limit 30 and 50 km/h), Passing Traffic lights, conducting right and left turns (with and without VRUs)
- Identification and detailed description of the area requested to carry out the tests.	City of Wolfsburg	City of Wolfsburg and rural area around the city of Wolfsburg	City of Brussels close to the Autoworld
- Identification of the affected populations.	Surrounding traffic (cars, trucks, busses VRUs)		
- Number and characteristics of vehicle(s):	1 VW Golf		
- Safety operator documentation:	A professional safety driver is required to operate the vehicle. ADF is activated by a two-hand switch and deactivated by intervention of the safety driver. Emergency stop switch is available and reachable by driver and co-driver. The safety driver needs to have a profession training (high dynamics training according to company training classification). AD status and interventions by the safety driver are logged over the test.		

Funded by
the European Union

System documentation package			
	Example Hi-Drive Deliverable D3.3; chapter 3.3.18; Vehicle owner ID18		
Description of the automated driving system to be tested			
1. Name of the function(s).	Hi-Drive Test Function 1		
2. Software version of the function(s).	V1.0.0	V1.1.0	V1.1.1
3. Description of control functions of the system, including:			
- Sensing and perception: input variables such as sensors involved in gathering all real-time data and their involvement in perception.	See Hi-Drive Deliverable AD uses camera, radar and LIDAR next to the other sensors + Driver inputs The use of sensors in different will change during the test to investigate advantages and disadvantages.		Similar as the previous use cases. However, a fixed setting will be run.
- Decision making and planning: based on sensor data how decisions are made.	Detailed information would be in practice available. However, since this example no detailed information is available. In course of the test activities the logic will change as the sensor usage changes. Again the purpose is to investigate pro and cons of different solution.		Similar as the previous use cases. However, a fixed setting will be run.
- Control execution: actions or signals that the system generates to control the vehicle in response to the input data. In other words, how previous decisions are implemented.	Actuators for braking and steering. For this example, it is presumed that the actuators are (at least partly) protype systems. A safe integration according to defined concept is established. The original HMI is changed (cluster display, switches) are changed to activate and operate the system (e.g. inform about system status). HMI is visualized in the upper picture.		
4. Operational Design Domain (ODD)			
- Infrastructure: Road type (highway, urban, rural), curvature and incline, lane markings, for instance.	Urban roads	Urban and rural roads	Urban (rural roads possible, but not required for this demonstration)
- Traffic conditions: Traffic density, behaviour of surrounding vehicles (e.g. lane changing). Roadwork and Obstructions (temporary lane diversions, cones, and roadblocks that alter normal lane patterns)	Operation in all traffic conditions, except: - Construction sides (Roadworks)		
- Environmental conditions: weather (clear, rainy, or snowy conditions), lighting (daytime, nighttime, or low-light conditions)	No operations in adverse weather conditions (heavy rains, ice / snowy roads, any snow fall, any hail), Operation in all light condition (day, night, dusk, dawn) Temperature > 3°C		
- Speed range: range of speeds within which the automated driving function is designed to operate	speed limit up 50 km/h	speed limits up 70 km/h	speed limit up 70 km/h possible. However, roads allow only 50 km/h.
- longitudinal acceleration range: range of accelerations within which the automated driving function is designed to operate	Acceleration up to 5 m/s²; Decelerations up 9.81 m/s²		
5. Boundaries	V2X will be tested in dedicated /stage scenarios at a preselected intersection		No demonstration of V2X

Funded by the European Union

Funded by
the European Union

Hi-Drive

3.3.18 Vehicle owner ID

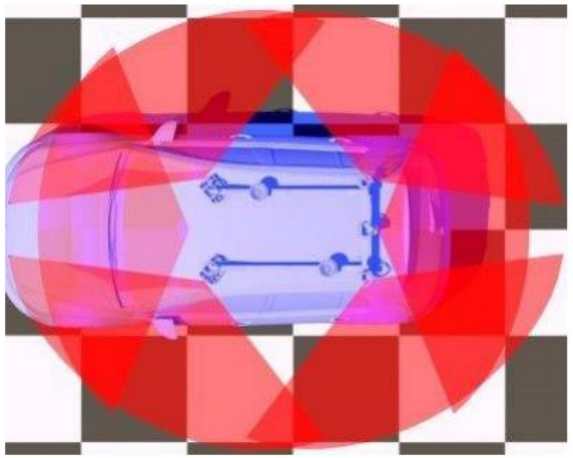
3.3.18.1 Vehicle description

ID	Count	Prototype / Series	Requirements to operate the vehicle with the enabler	Requirements to integrate the enabler inside the vehicle platform	Enabler Tech Solution (E2.x.y, see Table 2-2)	Use case (Urban, Motorway, Rural, Table 2-3)
	1	Modified series vehicle equipped with full sensor setup (cameras, LiDAR, radar) and computer HW	A professional safety driver is required to operate the vehicle. ADF can be activated by a two-hand switch and deactivated by intervention of the safety driver.	Sufficient network capacity and computer HW (GPUs) to transfer video streams and perform data processing with neural networks.	E.2.6.2	Urban

3.3.18.2 Sensors for AD function(s)

Technology	Function	Hor. field of view	Interface
Outside camera	Depth estimation, object detection	120°	GMSL
Radar	Not used	360°	
LiDAR	Reference measurements (dynamic and static objects)	360°	Ethernet
GPS	Vehicle position	N/A	Ethernet
IMU	Vehicle position	N/A	Ethernet

3.3.18.3 Sensor coverage



3.3.18.4 HMI description

Channel	Device	Main features
Visual	N/A	
Audio	N/A	
Commands	Buttons	Turn on/off AD
MID (Meter)	N/A	
Multimedia	N/A	
HUD	N/A	
Haptic	N/A	

3.3.18.5 Data logger description

Raw data record	Yes
Fusion object level record	Yes
Embedded video labelling	No
Could the driver annotate events	No
Data volume per hour in terabytes	0.24 TB/h

Funded by the European Union